Правила обмена электронными документами по системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

Оглавление

1. Общие положения

1.1. Настоящие Правила обмена электронными документами по системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО) (далее – Правила) устанавливают порядок обслуживания Клиентов с использованием Системы дистанционного банковского обслуживания «Клиент-Банк» (далее – Система «Клиент-Банк»), в целях предоставления услуг по дистанционному банковскому обслуживанию и определяют возникающие в этой связи права, обязанности и ответственность Сторон.

1.2. Правила являются типовым документом Банка и могут быть приняты Клиентом путем присоединения к Правилам в целом в порядке, установленном Правилами.

1.3. Заключение Договора об обслуживании с использованием Системы дистанционного банковского обслуживания (далее – **Договор**) осуществляется Клиентом в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

1.4. Клиент, имеющий в Банке открытый расчетный счет, не подключенный к Системам дистанционного банковского обслуживания (далее – ДБО), в целях заключения Договора предоставляет в Банк Заявление о присоединении к Правилам обмена электронными документами по Системе дистанционного банковского обслуживания и подключении Системы на бумажном носителе, составленное по форме Приложения №1 к настоящим Правилам или по иной форме, установленной Банком (далее – **Заявление о присоединении**), с проставлением отметки о приеме уполномоченным сотрудником Банка на Заявлении. Заявление о присоединении является офертой Клиента Банку заключить Договор о дистанционном банковском обслуживании с использованием Системы «Клиент-Банк».

1.5. Заключение Договора при открытии первого расчетного счета Клиента в Банке и подключение Системы «Клиент-Банк» производится на основании Заявления о присоединении по форме Банка, предоставленного Клиентом в Банк на бумажном носителе в составе комплекта документов для открытия расчетного счета и документов, указанных в настоящих Правил.

1.6. Уполномоченное лицо Клиента, ранее заключившее с Банком двухсторонний «Договор о применении системы дистанционного банковского обслуживания "БАН К-КЛИЕНТ"» по форме Банка, вправе присоединиться к настоящим Правилам в их действующей редакции путем предоставления в Банк надлежаще оформленного Заявления о присоединении к настоящим Правилам, в электронном виде, посредством действующей системы ДБО "БАНК-КЛИЕНТ" ЭКСИ-Банк (АО), подписанное действующей электронной подписью Уполномоченного лица. С дальнейшим предоставлением оригинала Заявления о присоединении на бумажном носителе в отделение Банка, в срок не более одного календарного месяца, с даты направления Заявления посредством действующей системы ДБО "БАНК-КЛИЕНТ" ЭКСИ-Банк (АО).

1.7. Банк с целью ознакомления Клиента с условиями настоящих Правил размещает Правила путем их опубликования в порядке, предусмотренном разделом 9 настоящих Правил.

1.8. Дистанционное банковское обслуживание Клиента с использованием Системы «Клиент-Банк» осуществляется в соответствии с законодательством Российской Федерации и Правилами. В случае изменения законодательства Российской Федерации Правила, до момента их изменения Банком, применяются в части, не противоречащей требованиям законодательства Российской Федерации.

2. Термины, определения и сокращения, используемые в Правилах

2.1. **Авторизация** – подтверждение полномочий (предоставление прав доступа) Клиента/ его Уполномоченного представителя, успешно прошедшего Аутентификацию входа, на получение услуг Банка.

2.2. **Авторство документа** – принадлежность документа одной из Сторон по Договору. Авторство электронного документа определяется принадлежностью электронной подписи конкретному пользователю Системы.

2.3. **Администратор (Оператор) Удостоверяющего центра** – должностное лицо, ответственное за решение комплекса задач по организации и обеспечению защиты информации с использованием СКЗИ, в том числе обеспечение функционирования СКЗИ Клиентов Системы.

2.4. **Аутентификация –** проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности**.**

2.5. **Аутентификация информации –** установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена. Любые преднамеренные и случайные попытки искажений информации обнаруживаются с соответствующей вероятностью.

2.6. Акт признания ключа проверки ЭП – электронный документ, подтверждающий принадлежность Ключа проверки ЭП PayControl владельцу,.

2.7. Активация – процедура персонализации Мобильного приложения PayControl, состоящая из следующих шагов:

- успешный ввод/передача в Мобильное приложение PayControl QR-кода/ключа инициализации;
- формирование в Мобильном приложении PayControl и регистрации на сервере PayControl набора уникальных признаков Мобильного устройства Клиента;
- создание Ключей ЭП в Мобильном приложении PayControl;
- регистрация Ключа проверки ЭП на сервере PayControl с целью дальнейшей проверки ЭП Клиента;
- создание Клиентом Пароля/TouchID/FaceID для дальнейшего использования в качестве аутентификационных данных для доступа к Ключу ЭП в Мобильном приложении PayControl.

2.8. Аутентификационные данные – Пароль/TouchID/FaceID, используемый для доступа к Ключу ЭП PayControl. Создание и установка аутентификационных данных является обязательным.

2.9. Аутентификация входа PayControl – процедура проверки соответствия предъявленных Аутентификационных данных Аутентификационым данным, установленным при активации Мобильного приложения PayControl.

2.10. Безопасность информации (информационная безопасность):

- состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.;
- состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

2.11. Бланк сертификата открытого ключа – документ на бумажном носителе, являющийся дубликатом сертификата ключа проверки УНЭП в Системе «Клиент-Банк», заверенный администратором УЦ и печатью.

2.12. Владелец сертификата ключа проверки УНЭП – физическое лицо (ответственный сотрудник Банка или Клиента), на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи, и которое владеет соответствующим ключом УНЭП, позволяющим с помощью средств УНЭП создавать УНЭП в электронных документах (подписывать электронные документы). Владельцами сертификатов ключей проверки УНЭП являются уполномоченные лица Сторон, имеющие право подписывать электронные документы своей ЭП от имени Стороны в Системе «Клиент-Банк».

2.13. Документ в электронной форме (электронный документ – ЭД) – документ, представленный в электронной форме в виде файла или записи базы данных, заверенный ЭП уполномоченного лица Клиента или Банка, подготовленный и переданный с помощью программного обеспечения Системы «Клиент-Банк» в соответствии со всеми процедурами защиты информации. Электронный документ, содержащий распоряжение Клиента, должен соответствовать требованиям нормативных актов Банка России и внутренних нормативных актов Банка, определяющих порядок оформления распоряжений и выполнения процедур приема к исполнению и исполнения распоряжений.

2.14. Зарегистрированный номер – номер телефона сотовой связи Уполномоченного лица Клиента/Пользователя Системы «Клиент-Банк», указанный в Договоре / Заявке ПЭП и используемый в целях подписания ПЭП Акта признания ключа проверки ЭП в Системе «Клиент-Банк».

2.15. Заявление на изготовление сертификата пользователя УЦ (сертификата ключа проверки УНЭП) – Документ на бумажном носителе, содержащий идентификационные данные Пользователя Системы «Клиент-Банк», параметры и области использования ключа, заверенный собственноручной подписью владельца сертификата ключа УНЭП и печатью организации (при ее наличии).

2.16. Защита информации – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации**.**

2.17. Иностранная валюта - официальная денежная единица иностранного государства (группы государств), являющаяся законным средством платежа на территории соответствующего иностранного государства (группы иностранных государств), операции с которой могут осуществляться уполномоченными банками Российской Федерации.

2.18. **Идентификатор пользователя** – уникальная последовательность, присваиваемая Клиенту в рамках работы со Средством ЭП PayControl.

2.19. **Тарифы на услуги** - оказываемые клиентам ЭКСИ-Банк (АО) для клиентов – юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой.

2.20. **Клиент** - юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающиеся в установленном законодательством РФ порядке, частной практикой, имеющий открытый расчетный счет в ЭКСИ-Банк (АО).

2.21. **Ключ УНЭП (и шифрования) – (закрытый ключ) –** уникальная последовательность символов, предназначенная для создания в ЭД ЭП, а также преобразования полученной закрытой информации в открытую с использованием сертифицированных средств криптографической защиты информации в Системе «Клиент-Банк».

2.22. **Ключ проверки УНЭП – (Открытый ключ)** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи, а также преобразования передаваемой открытой информации в закрытую в Системе «Клиент-Банк».

2.23. **Ключевой носитель** – USB-Token или иное аппаратное устройство для хранения закрытого ключа электронной подписи для Системы «Клиент-Банк».

2.24. **Ключи инициализации** – уникальные ключи, выпускаемые Банком для каждой учетной записи Клиента – владельца Средства ЭП PayControl. Направляются Банком каждой учетной записи Клиента в закодированном виде двумя частями (QR-код + SMS).

2.25. **Ключ ЭП** – уникальная последовательность данных, используемая для формирования ЭП документа Клиентом. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом проверки ЭП с использованием Средства ЭП PayControl при выполнении процедуры Активации, а также при плановой смене ключей ЭП. Однозначно соответствует Ключу проверки ЭП. Хранится на Мобильном устройстве Клиента и защищается средствами Мобильного приложения PayControl, средствами операционной системы и аппаратными средствами Мобильного устройства.

2.26. **Ключ проверки ЭП** – уникальная последовательность данных, служащая для проверки значения ЭП документа. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом ЭП с использованием Средства ЭП PayControl при выполнении процедуры Активации, а также при проведении плановой смены ключей ЭП. Однозначно соответствует Ключу ЭП. Хранится на Мобильном устройстве Клиента, а также передаётся на сервер PayControl, для целей обеспечения процедуры проверки ЭП.

2.27. **Код подтверждения** – уникальный код проверки целостности информации, позволяющий гарантировать то, что данные, не были изменены посторонними лицами.

2.28. **Компрометация ключей ЭП** – событие, в результате которого Ключ ЭП или его часть становятся известны или доступны постороннему лицу, либо подозрение, что такое событие могло произойти. К событиям, связанным с компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- Потеря Мобильного устройства Клиента, на котором выполнена процедура Активации.
- Потеря Мобильного устройства Клиента, на котором выполнена процедура Активации, с последующим обнаружением в местах, где к устройству могли получить доступ третьи лица.
- Увольнение сотрудников, имевших доступ к Мобильному устройству Клиента, на котором выполнена процедура Активации.
- Возникновение подозрений на утечку ключевой информации или ее искажение.
- Случаи, когда нельзя достоверно установить, что произошло с Мобильным устройством Клиента, на котором выполнена процедура Активации (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).

2.29. **Компрометация закрытого ключа УНЭП (и шифрования), пароля доступа к Системе «Клиент-Банк» –** событие, в результате которого возникает возможность ознакомления неуполномоченных лиц с закрытым ключом УНЭП (и шифрования), паролем доступа к Системе «Клиент-Банк». К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, относятся следующие:

- безвозвратная утрата носителей закрытого ключа;

– утрата носителей закрытого ключа с последующим обнаружением;
– увольнение работников, имевших доступ к носителям закрытого ключа и паролю для доступа к Системе «Клиент-Банк»;
– нарушение правил хранения и уничтожения (после окончания срока действия) носителей закрытого ключа;
– возникновение подозрений на утечку информации или её искажение в Системе «Клиент-Банк»;
– нарушение печати на сейфе или пенале (контейнере) с носителями закрытого ключа;
– случаи, когда невозможно достоверно установить, что произошло с носителями закрытого ключа, в том числе случаи, когда носители закрытого ключа вышли из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника.

2.30. Компрометация одноразового кода – ситуация, при которой есть достаточные основания полагать, что доверие к одноразовому коду в виде SMS сообщения, направленному для использования в качестве кода для подтверждения факта формирования ПЭП от имени Уполномоченного лица, утрачено. К событиям, связанным с Компрометацией одноразового кода, относятся, включая, но, не ограничиваясь, следующие события:
– утеря/кража/изъятие телефона/SIM-карты с Зарегистрированным номером, в том числе с последующим обнаружением;
– несанкционированное использование Зарегистрированного номера, технических, программных и коммуникационных ресурсов, используемых для доступа в Систему;
– возникновение подозрений о доступе к информации в Системе неуполномоченных лиц или об ее искажении в Системе, когда нельзя достоверно установить, что произошло с техническими, программными, коммуникационными ресурсами, используемыми для доступа в Систему (в том числе, выход из строя, когда доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц).

2.31. Конверсионная сделка - сделка купли-продажи суммы в одной Валюте за сумму в другой Валюте по Курсу Банка, доступному Клиенту в сервисе «Онлайн конверсия», заключаемая между Сторонами на условиях настоящих Правил, с осуществлением Сторонами расчетов в Дату валютирования.

2.32. Курс Банка - курс, по которому Банк осуществляет Конверсионную сделку на основании Поручения на конверсию валюты Клиента в сервисе «Онлайн-конверсия», сформированный на основании рыночного соотношения спроса и предложения на валютные и рублевые ресурсы на момент заключения Конверсионной сделки.

2.33. Лицензия в области защиты информации – оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

2.34. Мобильное приложение PayControl – мобильное приложение для операционных систем iOS и Android, разработанное ООО «СэйфТек» (SafeTech LTD), предназначенное для формирования ЭП.

2.35. Мобильное устройство – смартфоны, мобильные телефоны, планшеты и прочие устройства, имеющие доступ к сети Интернет, на которых установлено Мобильное приложение PayControl.

2.36. Мероприятия по защите информации – совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

2.37. Обработка информации – передача, прием, хранение, преобразование и отображение информации.

2.38. Плановая смена ключей – процедура смены Ключей в Системе «Клиент-Банк» в связи с окончанием срока их действия, не вызванная компрометацией ключей.

2.39. Подтверждение подлинности УНЭП в электронном документе – положительный результат проверки средствами ЭП с использованием сертификата ключа подписи принадлежности ЭП в ЭД владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной ЭП ЭД в Системе «Клиент-Банк».

2.40. Пользователь Системы (Пользователь) – физическое лицо, наделенное Клиентом полномочиями (правами) доступа в Систему и уполномоченное Клиентом просматривать информацию в Системе и/или давать Банку распоряжения о совершении операций по Счетам Клиента с использованием Системы и наделенное правом подписания ЭД ЭП. Права просмотра информации в Системе и/или формирования ЭП подписанта, формирования и отправки в Банк сообщений в опции «Документы свободного формата» соответствуют полномочиям, которыми Пользователь наделен Клиентом в соответствии с предоставленными в Банк документами (Доверенностью / Приказом) и заявками для подключения к Системе, предусмотренными настоящими Правилами.

2.41. Поручение на конверсию валюты - электронный документ, формализованный в Системе «Клиент-Банк», содержащий распоряжение Клиента на исполнение операций покупки / продажи соответствующей валюты по Курсу Банка, выбранному Клиентом в сервисе «Онлайн конверсия» в режиме реального времени.

2.42. Правила открытия и ведения счетов[1] - Правила открытия и ведения счетов юридических лиц – резидентов/ нерезидентов (кроме кредитных организаций), индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в ЭКСИ-Банк (АО).

2.43. Проверка электронной подписи (УНЭП) документа – проверка соотношения, связывающего хеш-функцию документа, подпись под этим документом и открытый ключ подписавшего абонента в Системе «Клиент-Банк». Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ – подлинным, в противном случае документ считается измененным, а подпись под ним – недействительной.

2.44. Проверка ЭП – процедура проверки соответствия предъявленной ЭП данным документа, времени формирования ЭП и набору уникальных признаков Мобильного устройства, выполняемая с использованием Ключа проверки ЭП на сервере PayControl.

2.45. Простая Электронная подпись (ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Пользователем или Уполномоченным лицом Клиента в Системе. В рамках настоящих Правил Простой электронной подписью является одноразовый код, формируемый Банком и направляемый на Зарегистрированный номер Пользователя / Уполномоченного лица Клиента для однократного использования при передаче кода для подписания Акта признания ключа проверки ЭП в Системе «Клиент-Банк».

2.46. Реестр Сертификатов – набор документов в электронной и/или бумажной форме, включающий следующую информацию для Системы «Клиент-Банк»:

– запросы на регистрацию в Удостоверяющем Центре;
– список пользователей Удостоверяющего Центра;
– запросы на изготовление сертификатов ключей подписи;
– запросы на аннулирование (отзыв) сертификатов ключей подписи;
– запросы на приостановление/возобновление действия сертификатов ключей подписи;
– сертификаты ключей подписи;
– списки отозванных сертификатов.

2.47. Сервер PayControl — преднастроенный сервер, реализующий проверку сформированной ЭП и хранение Ключа проверки ЭП.

2.48. Сервис «Онлайн Конверсия» — раздел системы «Клиент-Банк», предназначенный для дистанционного совершения Конверсионных сделок в режиме реального времени по Курсу Банка, обеспечивающий Клиенту техническую возможность на основании предоставляемой Банком информации о курсах конвертации валюты дистанционно заключать Конверсионные сделки по Курсу Банка, выбранному Клиентом в режиме реального времени на сумму, доступную в Сервисе «Онлайн конверсия». Выбранное Клиентом значение курса в Сервисе «Онлайн-Конверсия» используется для расчета суммы Валюты, получаемой в результате исполнения Конверсионной сделки.

Сервис «Онлайн конверсия» подключается Банком автоматически Клиенту, подключенному к Системе «Клиент-Банк» при открытии первого расчетного счета в Иностранной валюте.

Банк оказывает услугу проведения конверсионных операций по Курсу Банка, сформированному в сервисе «Онлайн конверсия», в Иностранных валютах, указанных Клиентом в Поручении на конверсию валюты при наличии в Банке открытых расчетных счетов Клиента в заявленных Иностранных валютах.
Сервис «Онлайн Конверсия» предоставляется, при наличии технической возможности.

2.49. Сертификат ключа проверки УНЭП (сертификат ключа подписи) – ЭД с ЭП уполномоченного лица Удостоверяющего Центра, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи, изготовленный в соответствии с заявлением Пользователя Системой «Клиент-Банк».

[1] Размещены на корпоративном Интернет-сайте Банка https://www.exibank.ru

2.50. Система «Клиент-Банк» (Система) – системы дистанционного банковского обслуживания производства ООО «Банк Софт Системс» (Компания BSS): Традиционный «Клиент-Банк», Интернет «Клиент-Банк», которые позволяют осуществлять формирование, передачу и хранение документов в электронном виде. Система «Клиент-Банк» предназначена для повышения качества обслуживания Клиента, а также для ускорения выполнения расчетных операций Клиента за счет замены бумажного документооборота между Банком и Клиентом на документооборот с использованием ЭД, передаваемых для исполнения в Банк по техническим каналам связи.

2.51. Симметричный ключ – уникальный ключ, используемый в симметричных криптографических алгоритмах. Передается Клиенту доверенным каналом и используется для выработки и проверки кодов подтверждения.

2.52. Средства ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП для Системы «Клиент-Банк»**.**

2.53. Средство ЭП PayControl – программный комплекс, предназначенный для подтверждения уполномоченным лицом Клиента операций в Системе Клиент-Банк».

2.54. Удостоверяющий Центр (УЦ) – юридическое лицо ООО «АйтиКом», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2.55. Уполномоченное лицо -

- для подписания Акта признания ключа проверки ЭП ПЭП в Системе «Клиент-Банк» - индивидуальный предприниматель, физическое лицо, занимающиеся в установленном законодательством РФ порядке частной практикой, единоличный исполнительный орган ЮЛ или Руководитель ЮЛ, который вправе действовать от имени ЮЛ без доверенности;
- для подписания документов УНЭП в Системе «Клиент-Банк» - Владелец сертификата ключа проверки УНЭП.
- для подписания документов Средством ЭП PayControl в Системе «Клиент-Банк» - Владелец сертификата ключа проверки ЭП.

2.56. Усиленная неквалифицированная электронная подпись (далее – УНЭП) – электронная подпись, полученная в результате криптографического преобразования информации, позволяющая определить лицо, подписавшее Электронный документ, а также обеспечивающая возможность контроля целостности и подтверждения подлинности Электронных документов, исходящих от каждой из Сторон в Системе «Клиент-Банк».

2.57. Формирование ЭП – процедура вычисления ЭП Клиента в Мобильном приложении PayControl на основе данных операции, времени формирования и набора уникальных признаков Мобильного устройства, выполняемая путем математических преобразований с использованием Ключа ЭП.

2.58. Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.59. Шифр – совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей в Системе «Клиент-Банк».

2.60. Шифрование – способ преобразования открытой информации в закрытую и обратно, для хранения в ненадёжных источниках или передачи её по незащищённым каналам связи.

2.61. Шифровальные средства (средства криптографической защиты информации или СКЗИ) – Программно-техническое средство «КриптоПро CSP», осуществляющее криптографическое преобразование информации для обеспечения неизменности содержания и установления Авторства электронных документов, а также конфиденциальности и контроля целостности информации в Системе «Клиент-Банк».

2.62. Электронная подпись (далее – 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. Для целей настоящих Правил предусмотрена возможность использования ПЭП, УНЭП и/или Средство ЭП PayControl.

2.63. SMS- сформированная Банком уникальная последовательность символов, направленная в виде сообщения на Зарегистрированный номер и предназначенная для однократного использования Клиентом в качестве кода для подтверждения факта формирования ПЭП Уполномоченным лицом Клиента.

2.64. USB-Token – персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с сертификатами и УНЭП.

2.65. PayControl — программный комплекс, предназначенный для подтверждения пользователем операций в Системе «Клиент-Банк» и/или формирования подписи в Системе «Клиент-Банк». Это решение для электронной подписи в мобильном устройстве, которое позволяет Клиентам подтверждать свои операции, создаваемые в Системе «Клиент-банк». Работает в виде отдельного приложения для мобильного устройства.

2.66. PUSH-сообщение – электронное сообщение, направляемое Банком Клиенту через сервисы, предоставляемые компаниями Apple или Google, поступает на Мобильное устройство Клиента исключительно при наличии доступа Мобильного устройства к сети Интернет.

2.67. QR-код – оптическая метка, содержащая Ключ инициализации в закодированном виде.

2.68. Документы валютного контроля – документы, формализованные в Системе «Клиент-Банк», связанные с проведением валютных операций, в том числе:

– «**Ведомость банковского контроля**» – документ, который формируется и ведется в электронном виде, в отношении контрактов, принятых на учет уполномоченным банком;
– «**Формы учета по валютным операциям**» – справка о подтверждающих документах Клиента, а также иные документы, предусмотренные действующим законодательством Российской Федерации и нормативными документами Банка России по валютному контролю.

2.69. Ответственное лицо Банка по ВК – сотрудник Банка, уполномоченный на основании распорядительного документа по Банку осуществлять от имени Банка действия по валютному контролю, предусмотренные действующим законодательством Российской Федерации.

2.70. Аналог собственноручной подписи ответственного лица Банка (АСП) – персональный идентификатор Банка, являющийся контрольным параметром правильности составления всех реквизитов документов и неизменности их содержания.

2.71. Служебно-информационные документы[2] - электронные документы, формализованные в Системе «Клиент-Банк», направляемые в Банк Клиентом или Банком Клиенту в виде сообщения, подписанного действующей ЭП, в том числе, содержащие распоряжение Банку на совершение операций по счету Клиента. В качестве Служебно-информационных документов могут выступать распоряжения по счету, документы валютного контроля и иные документы.

2.72. Документы свободного формата[7] – электронные Служебно-информационные документы, направляемые по Системе в виде сообщения, подписанного в Системе «Клиент-Банк» действующей УНЭП или Средством ЭП PayControl Уполномоченного лица Клиента или Пользователя с соответствующими полномочиями (правами) в Системе, в том числе содержащего как сформированные в электронном виде документы, так и созданные с использованием сканирующих устройств изображения документов, оформленных на бумажном носителе.

Клиент и Банк могут обмениваться сообщениями в Системе «Клиент-Банк», подписанными УНЭП или Средством ЭП PayControl с вложением Документов свободного формата следующих типов: Документы валютного контроля, письма в Банк, файлы, содержащие реестры к платежным поручениям на общую сумму зачислений на банковские счета, файлы с вложением выставленных платежных требований, Запросы на отзыв документов, Запросы на предоставление информации по счету, Заявления об акцепте / отказе от акцепта, заявления на заключение с Банком договора, Договоры, дополнительные соглашения к заключенному с Банком договору, иные Заявления, договоры с контрагентами на поставку товаров / оказание услуг, иные договоры и документы.

3. Права и обязанности Сторон

3.1. Банк обязуется:

3.1.1. Обеспечить функционирование Системы в круглосуточном режиме с возможностью проведения регламентных работ (технологических перерывов) в нерабочие дни или в будни в период с 20:00 до 02:00 по московскому времени не более 3 (Трех) раз в месяц. В иное время при возникновении сбоев в срок не более 1,5 часов

[2] Максимальный объем вложения для служебно-информационных документов и для Документов свободного формата 10мб. Рекомендованные настойки для качественного сканирования документов больших объемов: качество 150 Dpi, монохромное сканирование.

обеспечить работоспособность Системы. При этом прием документов осуществляется в режиме, указанном в настоящих Правилах.

3.1.2. Обеспечить Клиента после подписания настоящего Договора комплексом программных средств, обеспечивающих функционирование Системы, необходимой нормативно-технической документацией, а также документацией на используемую систему защиты информации.

3.1.3. Консультировать представителей Клиента по работе в Системе в период операционного обслуживания Клиентов, указанный в Тарифах на услуги.

3.1.4. Принимать полученные по Системе электронные документы (пакеты электронных документов), оформленные в соответствии с настоящими Правилами.

3.1.5. Обеспечивать защиту информации в Системе от несанкционированного доступа. В этих целях:

3.1.5.1. Сохранять конфиденциальность и подлинность используемых ключей ЭП (и шифрования), паролей и одноразовых кодов;

3.1.5.2. Протоколировать все случаи и попытки нарушения безопасности Системы. При возникновении таких случаев принимать все возможные меры для предотвращения и ликвидации их последствий вплоть до приостановления функционирования Системы;

3.1.5.3. В случае получения информации о компрометации ключей ЭП (и шифрования) и/или одноразового кода и/или выявления несанкционированных платежей Клиента заблокировать работу Клиента в Системе до завершения внеплановой смены ключей ЭП (и шифрования) и/или замены логина / пароля на основании полученным Банком новым Заявлением о присоединении по форме Приложений №1 к настоящим Правилам;

3.1.5.4. Обеспечивать сохранность и конфиденциальность информации, доверенной ему Клиентом в ходе практической деятельности в рамках настоящего Договора, в соответствии с действующим законодательством.

3.1.5.5. Своевременно информировать Клиента об изменениях порядка осуществления приема/передачи ЭД и другой информации по Системе. Оказывать консультационные услуги Клиенту по вопросам функционирования Системы и использования СКЗИ.

3.1.5.6. Принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Клиентом Средства ЭП PayControl. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Российской Федерации.

3.1.5.7. В случаях, когда использование Средства ЭП PayControl предполагает передачу Клиенту либо хранение Банком какой-либо конфиденциальной информации, Банк обязуется принять все необходимые меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Клиенту, а также во время ее хранения Банком.

3.1.6. Соблюдать положения законодательных документов Российской Федерации, нормативных документов Банка России, регламентирующих функционирование Системы, а также настоящих Правил.

3.1.7. Предоставлять Клиенту выписки о проведении операций по счетам Клиента по Системе в соответствии с п.п.13.20. настоящих Правил.

3.1.8. Предоставлять Клиенту новые версии программного обеспечения Системы в случае их замены без дополнительной оплаты, а также консультировать Клиента по телефону в случаях сбоев установленной у Клиента Системы в целях устранения последствий сбоев и восстановления нормального функционирования Системы.

3.1.9. При подключении Системы «Клиент-Банк»:

3.1.9.2. Предоставить доступ к Системе Уполномоченному лицу Клиента в рамках предоставленных им полномочий (прав) в срок не позднее следующего рабочего дня после получения Заявления о присоединении, оформленной и предоставленной в Банк в порядке, указанном в настоящих Правил.

3.1.9.4. При использовании Клиентом УНЭП, предоставить зарегистрированным уполномоченным лицам Клиента права доступа к Системе в соответствии с данными Заявок о выпуске сертификата, не позднее следующего рабочего дня после получения от Клиента заверенных владельцем Заявления на изготовление сертификата пользователя УЦ (Приложение №2 к Правилам) и в случае выдачи USB-Token «Акта приема-передачи».

3.1.9.4. При использовании Клиентом Средства ЭП PayControl, осуществить подключение и предоставить доступ к Системе Уполномоченному лицу Клиента и Пользователям Системы в рамках предоставленных им

полномочий (прав) к Средству ЭП PayControl в срок не позднее следующего рабочего дня после получения Заявления о присоединении, оформленной и предоставленной в Банк в порядке, указанном в настоящих Правил.

3.1.11. При получении от Клиента письменной информации об ошибочном, в том числе в результате несанкционированного доступа к банковскому счету Клиента, списании со Счета Клиента в Банке незамедлительно информировать банк-корреспондент о списании денежных средств Клиента (по его информации) в результате несанкционированного доступа к банковскому счету указанного Клиента с предложением (просьбой) оказать содействие по возврату денежных средств (как ошибочно перечисленных, необоснованно списанных при несанкционированном доступе к счету).

3.1.12. В установленном в Банке порядке провести служебное расследование ставшего известным факта несанкционированного доступа к счету Клиента, в том числе в результате компрометации одноразового кода, с привлечением Клиента, проинформировать Клиента о результатах расследования.

3.2. Банк вправе:

3.2.1. Вносить изменения в Тарифы на услуги в части размера комиссий, уплачиваемых Клиентом Банку за обслуживание в Системе «Клиент-Банк», срока и порядка оплаты указанных комиссий, в порядке, указанном в разделе 8 настоящих Правил.

3.2.2. Отказать Клиенту в совершении операций по счету с использованием ЭД в случае отрицательного результата процедур приема к исполнению ЭД, предусмотренных Правилами.

3.2.3. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию Системы, в одностороннем порядке приостановить работу с Клиентом через Систему до момента устранения неисправностей. Все платежные документы в этом случае должны передаваться в Банк и Клиенту на бумажных носителях в установленном порядке. Действие данного пункта не должно противоречить п.3.1.1. настоящих Правил.

3.2.4. При наличии у Банка сомнений в подлинности (аутентичности) платежного документа, поступившего с использованием Системы, направить письменный запрос Клиенту (с курьером/ посредством факсимильной связи/ по Системе) или провести переговоры с Клиентом по телефону о подтверждении подлинности документа. В случае подтверждения Клиентом подлинности платежного документа, Банк выполняет операцию по нему не позднее банковского дня, следующего за днем получения Банком платежного документа.

3.2.5. Отключить Клиента от Системы в случаях выявления фактов допуска Клиентом к Системе третьих лиц.

3.2.6. Временно блокировать доступ Клиента к Системе в случае поступления информации о зачислении на банковский счет Клиента денежных средств, списанных в результате несанкционированного доступа к счетам третьих лиц (в Банке или в других кредитных организациях).

3.2.7. Расторгнуть Договор, заключенный в соответствии с настоящими Правилами, в одностороннем порядке в случае неисполнения Клиентом обязательств по оплате услуг Банка по сопровождению и обслуживанию Системы в соответствии с Тарифами на услуги путем направления Клиенту письменного уведомления в порядке, предусмотренном в разделе 10 настоящих Правил. Решение о способе отправки уведомления (почтовым отправлением или по Системе «Клиент-Банк») принимается Банком.

3.2.8. В целях исполнения требований законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма в качестве мер предупредительного характера отказать Клиенту в предоставлении услуг с использованием Системы.

3.2.9. При выявлении подозрительных операций, осуществляемых Клиентом по счету, а также в случае отказа Клиента от предоставления Банку запрашиваемых документов в соответствии с п. 3.2.10 настоящих Правил (в случае не предоставления таких документов), после предварительного предупреждения Клиента отказать ему в приеме распоряжений на проведение операций по банковскому счету, направленных в Банк с использованием Системы. В этом случае Клиент вправе направлять в Банк надлежащим образом оформленные расчетные документы, на бумажном носителе.

3.2.10. Требовать от Клиента в рамках мероприятий по реализации положений Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» предоставления в срок, указанный Банком, документов, связанных с проведением Клиентом банковских операций и подтверждающих их действительность и экономическую обоснованность (в т.ч. заверенные надлежащим образом копии договоров, на основании которых производится зачисление/списание денежных средств, счетов-фактур, спецификаций и др.), а также копий документов, заверенных надлежащим образом,

содержащих сведения о выгодоприобретателях и бенефициарных владельцах Клиента.

3.2.11. Отказать в выполнении распоряжения Клиента о совершении операции, по которой не представлены документы, необходимые для фиксирования информации в соответствии с требованиями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также в случае, если у работников Банка возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

3.2.12. Расторгнуть Договор об обслуживании с использованием Системы, заключенный в соответствии с настоящими Правилами, в случае принятия в течение календарного года двух и более решений об отказе в выполнении распоряжения Клиента о совершении операции по основаниям, указанным в п.3.2.11. настоящих Правил.

3.2.13. Расторгнуть Договор об обслуживании с использованием Системы, заключенный в соответствии с настоящими Правилами, в одностороннем порядке или отключить Систему «Клиент-Банк» в случае неисполнения Клиентом обязательств по плановой перегенерации и замене Ключей УНЭП (и шифрования) в течение 2 (Двух) месяцев и более при условии отсутствия иных действующих сертификатов ключа проверки ЭП.

3.2.14. В соответствии с требованиями Федерального закона от 26.10.2002г. № 127-ФЗ «О несостоятельности (банкротстве)»:

3.2.14.1 Блокировать доступ Клиента к Системе не позднее рабочего дня, следующего за днём поступления в Банк документов/сведений о признании Клиента Банкротом и инициировании в отношении него процедур банкротства:

- для юридического лица - «Внешнее управление» или «Конкурсное производство»;
- для индивидуального предпринимателя – «Реструктуризация долгов индивидуального предпринимателя» или «Реализация имущества индивидуального предпринимателя».

3.2.14.2. Восстановить доступ Клиента к Системе по Заявлению Клиента после прекращения производства по делу о банкротстве или по Заявлению/Согласию финансового управляющего в ходе реализации процедур банкротства.

3.2.15. Банк не несет ответственности за убытки, понесенные Клиентом в связи с указанием Уполномоченным лицом / Пользователем Системы неверных реквизитов при оформлении Заявления о присоединении, либо в связи с исполнением Банком ЭД, направленных с Мобильного устройства, который более не принадлежит Уполномоченному лицу / Пользователю Системы, как следствие неисполнения или ненадлежащего исполнения Клиентом обязанности, предусмотренной настоящими Правилами в части несвоевременного предоставления информации об изменении реквизитов доступа в соответствии с Приложением №1 к настоящим Правилам.

3.2.16. Без предварительного уведомления Клиента временно приостановить или ограничить доступ Клиента к Средству ЭП PayControl, при наличии у Банка достаточных оснований считать, что по используемому Клиентом каналу доступа возможна попытка несанкционированного доступа от имени Клиента или в иных случаях по усмотрению Банка. О временном приостановлении или ограничении доступа Банк оповещает Клиента путем направления письменного уведомления (заказным почтовым отправлением с уведомлением о вручении или по Системе «Клиент-Банк»).

3.2.17. Осуществлять сбор информации о Мобильном устройстве для целей противодействия угрозам, возникающим при использовании Средства ЭП PayControl, такой как:

- геолокация;
- информация об устройстве;
- информация о подключении к сети;
- события, происходящие в Мобильном приложении PayControl;
- обнаруженное потенциально вредоносное ПО.

3.3. Клиент обязуется:

3.3.1. Представить Банку материалы и информацию, необходимые для подключения к Системе.

3.3.2. Назначить лиц, имеющих право работать с Системой.

3.3.3. Для использования подсистемы Интернет-Клиент Системы «Клиент-Банк» оборудовать за свой счет автоматизированное рабочее место – АРМ «Клиент-Банк», в составе персонального компьютера с доступом к сети Интернет с операционной системой Microsoft Windows 7 и выше[3], а также следующими характеристиками:

[3] При условии совместимости соответствующей версии ОС с сертифицированной версией СКЗИ

- объем доступной памяти на жестком диске не менее 3 ГБ,
- наличие свободного USB-порта;
- программное обеспечение MS Internet Explorer версии 9.0 или выше;
- установленное и работающее лицензионное антивирусное ПО.

3.3.4. Для работы с подсистемой Интернет-Клиент Системы «Клиент-Банк» с использованием УНЭП назначить лиц, ответственных за сохранность ключей ЭП (и шифрования), подать Заявления на изготовление сертификата ключа проверки электронной подписи в Удостоверяющем центре (Приложение №2 к Правилам), произвести генерацию ключей в соответствии с руководством пользователя Системы (предоставленную Банком УЦ).

3.3.5. Для работы с использованием УНЭП предоставить в Банк Заявления на изготовление сертификата ключа проверки электронной подписи (Приложение №2 к Правилам), заверенные подписями зарегистрированных в Удостоверяющем центре лиц (владельцев сертификатов) и печатью Клиента (при ее наличии) и с отметкой УЦ о выпуске сертификатов.

3.3.6. Строго соблюдать предусмотренные настоящими Правилами требования к подготовке и передаче ЭД.

3.3.7. Обеспечивать защиту Системы «Клиент-Банк» от несанкционированного доступа с использованием средств криптографической защиты информации, сертифицированных ФСБ России. Для этого выполнять требования, перечисленные в разделе 4 настоящих Правил, а также в Правилах на использование СКЗИ "КриптоПро CSP", передаваемых Клиенту Банком.

3.3.8. Незамедлительно извещать Банк обо всех случаях компрометации ключей ЭП (и шифрования), выхода из строя носителей ключей ЭП Клиента, изменения регистрационных данных в сертификате, смене Уполномоченных лиц Клиента/Пользователей, уполномоченных подписывать электронные документы предоставив письмо о прекращении права доступа в Систему «Клиент-Банк» сертификата ключа подписи Пользователя (Приложение № 3 к Правилам) в соответствии со временем работы офисов Банка. В случае компрометации или изменении состава Уполномоченных лиц Клиента/ Пользователей Системы - незамедлительно известить об этом Банк, предоставив Заявку на отключение использования простой электронной подписи/ Средством электронной подписи PayControl для удостоверения документов в Электронной системе «Клиент-Банк» (Приложение № 7 к Правилам) в офис Банка или в электронном виде, путем вложения в сообщение сканированных копий документов в опции «Документы свободного формата».

3.3.9. Немедленно сообщать службе техподдержки Банка на номер телефона, указанный на сайте Б**анка** о случаях несанкционированного доступа к счету, списания денежных средств и о фактах компрометации.

3.3.10. При смене Мобильного устройства и/или Номера телефона Клиент обязан обратиться в Банк для получения новых Ключей инициализации для Средства ЭП PayControl.

3.3.11. По первому требованию Банка представлять информацию, подтверждающую подлинность (аутентичность) платежного документа, направленного с использованием Системы (в том числе, предоставлять платежный документ, направленный с использованием Системы, на бумажном носителе с подписями лиц, уполномоченных распоряжаться счетом, и оттиском печати Клиента (при наличии)).

3.3.12. Соблюдать конфиденциальность информации, касающейся Системы, в том числе конфиденциальность используемых паролей и одноразовых кодов.

3.3.13. Использовать предоставленные Банком средства Системы «Клиент-Банк» только для целей, определенных настоящими Правилами.

3.3.14. Клиент обязуется использовать предоставленные шифровальные (криптографические) средства (СКЗИ) только на территории Российской Федерации, без права их продажи или передачи каким-либо другим способом третьим лицам.

3.3.15. В случае уведомления Банком Клиента о смене программного обеспечения и/или смене сертификатов ключей обеспечить меры для их своевременного получения и установки в соответствии с Правилами.

3.3.16. Обеспечивать на Счете сумму денежных средств в размере, необходимом для своевременного списания Банком комиссий за сопровождение и обслуживание Системы в соответствии с Тарифами на услуги.

3.3.17. Своевременно вносить абонентскую плату за сопровождение и обслуживание Системы в соответствии с Тарифами на услуги.

3.3.18. Не позднее одного рабочего дня с момента передачи бланков Заявлений на изготовление сертификата пользователя УЦ в Системе «Клиент-Банк» (Приложение № 2 к Правилам) и в случае выдачи USB-Token подписать со своей стороны «Акт приема-передачи» и передать в Банк.

3.3.19. В целях использования Средства ЭП PayControl в Системе «Клиент-Банк» подписать со своей стороны «Акт признания ключа проверки ЭП» действующей ПЭП в Системе «Клиент-Банк».

3.3.20. Производить смену ключей шифрования и ЭП/Ключей ЭП лиц, ответственных за работу с электронными документами в Системе «Клиент-Банк», не менее 1 (Одного) раза в год, и предоставлять в Банк и/или УЦ бланки новых Заявлений (Приложения № 2 к Правилам).

3.3.21. В случае изменения данных владельца сертификата (ФИО, наименования организации, юридического адреса), Клиент должен предоставить в Банк новую Заявку на подключение к Системе «Клиент-Банк», оформленную согласно Приложению № 5 к Правилам:

- подать Заявления на изготовление сертификата ключа проверки электронной подписи (Приложение №2 к Правилам);
- предоставить Заявление об отзыве сертификатов ключей проверки ЭП лиц, у которых меняются данные, с указанием причины отзыва (изменение регистрационных данных).

3.3.22. В случае изменения полномочий или состава лиц, уполномоченных подписывать электронные документы, а так же в случае изменения наименования организации Клиент должен предоставить в Банк новую Заявку на подключение к Системе, оформленную согласно Приложению № 5 к Правилам:

- подать Заявления на изготовление сертификата ключа проверки электронной подписи (Приложение №2 к Правилам);
- предоставить Заявление на прекращение права доступа в Систему «Клиент-Банк» сертификата ключа подписи Пользователя Удостоверяющего Центра, в отношении которых прекращены полномочия подписывать ЭД (Приложение №3 к Правилам).

3.3.23. Предоставлять информацию, необходимую для исполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», включая информацию о своих выгодоприобретателях и бенефициарных владельцах.

3.3.24. Клиент обязуется обеспечить сохранность Мобильных устройств с установленным Мобильным приложением PayControl, а также Мобильных устройств, номера которых зарегистрированы в Банке для целей получения одноразового кода в виде SMS сообщения (Зарегистрированный номер). В случае утери мобильного устройства с установленным Мобильным приложением PayControl/Зарегистрированным номером, или осуществления операций по счетам Клиента посредством ПЭП/Средством ЭП PayControl без согласия Клиента незамедлительно, в момент обнаружения факта утраты или осуществления несанкционированных операций, проинформировать службу поддержки Банка по номеру телефона, указанному на сайте Банка. Для своей идентификации Клиент при уведомлении Банка через службу поддержки должен по телефону сообщить данные, включая паспортные, указанные в Заявлении о присоединении. При обращении Клиента в службу поддержки с устным сообщением об утрате мобильного устройства с установленным Мобильным приложением PayControl/Зарегистрированным номером Банк блокирует доступ Клиента в подсистему Интернет-Клиент Системы «Клиент-Банк». В случае осуществления операций по счетам Клиента посредством ПЭП/Средством ЭП PayControl без согласия Клиента, Клиент обязан направить в Банк письменное уведомление заказной почтой (с уведомлением о вручении и описью вложений), курьерской службой или в любой офис Банка.

3.3.25. Клиент обязуется не допускать переполнение памяти мобильных устройств с установленным Мобильным приложением PayControl/Зарегистрированными номерами, что может стать препятствием для приема QR-кода, кода активации, SMS-сообщений с одноразовыми кодами.

3.3.26. Не передавать третьим лицам и сохранять конфиденциальность информации, направленной Банком на Зарегистрированный номер телефона до момента ее применения.

3.3.27. Не предоставлять телефон с Зарегистрированным номером третьим лицам и незамедлительно сообщать в ЭКСИ-Банк (АО) при утере/изменении номера телефона или при нарушении конфиденциальности, направленной Банком на указанный номер телефона информации.

3.4. Клиент вправе:

3.4.2. В случае возникновения у Клиента технических неисправностей или других обстоятельств, препятствующих использованию ЭД, обратиться в Банк с письмом, содержащим мотивированную просьбу о приостановлении его работы в Системе на определенный срок. Все документы в этом случае должны передаваться в Банк и Клиенту на бумажных носителях в установленном порядке. Изменение порядка передачи документов вступает в силу с момента получения Банком уведомления Клиента.

3.4.3. Взаимодействовать с Банком в ходе расследования факта несанкционированного доступа к счету Клиента, получать от Банка информацию о результатах расследования.

3.4.4. Использовать Мобильное приложение PayControl для электронного обмена документами в соответствии с настоящими Правилами.

4. Передача прав

4.1. Ни одна из Сторон не может передавать свои права и обязательства по Договору, заключенному в соответствии с настоящими Правилами, третьим лицам.

5. Порядок расчетов

5.1. Клиент оплачивает услуги Банка за обслуживание в Системе в размере и сроки, указанные в Тарифах на услуги, и в соответствии с настоящими Правилами.

5.2. В случае неисполнения Клиентом обязательств по оплате Банку услуг и внесению абонентской платы Банк имеет право без дополнительного распоряжения Клиента списать с расчетного счета, а при невозможности списания с расчетного счета - с любого банковского счета Клиента, открытого в Банке, сумму денежных средств в размере стоимости услуг/абонентской платы.

6. Порядок хранения и уничтожения электронных документов и сертификатов ключей

6.1. Банк и Клиент осуществляют хранение и защиту электронных документов, подписанных ЭП, соответствующих сертификатов ключей в электронной форме в течение 5 (Пяти) лет.

6.2. Банк и Клиент обязаны обеспечить защиту архивов ЭД и сертификатов ключей от несанкционированного доступа в соответствии с требованиями, перечисленным в Разделе 14 настоящих Правил.

6.3. По истечении срока хранения ЭД и сертификатов ключей Банк и Клиент самостоятельно производят их уничтожение.

7. Ответственность Сторон

7.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Банк не несет ответственности за неисполнение или ненадлежащее исполнение поручений Клиента в случаях, указанных в п.3.2.3 настоящих Правил, из-за нарушения Клиентом положений настоящих Правил, а также в случаях, предусмотренных законодательством Российской Федерации.

7.3. Банк не несет ответственности за списание средств со счета Клиента в случае, если по причинам, не зависящим от Банка, электронные платежные документы были отправлены в Банк лицами, не несущими ответственность за сохранность ключей ЭП (и шифрования), не имеющими право работать с Системой, при условии, что электронные платежные документы были составлены правильно и соответствовали требованиям системы защиты от несанкционированного доступа и содержали правильные ЭП, а также, если Банк не был своевременно информирован об обстоятельствах, предусмотренных пунктами 3.3.8., 3.3.22 и 3.4.2. настоящих Правил.

7.4. Банк не несет ответственности за невыполнение обязательств, предусмотренных настоящими Правилами в случае сбоев, возникших по причинам, независящим от Сторон.

7.5. Банк не несет ответственности за ущерб, возникший:

- вследствие несанкционированного доступа третьих лиц к Мобильному устройству Клиента, Ключа ЭП, Аутентификационым данным и их использования третьими лицами;
- вследствие нарушения Клиентом требований технической защиты Мобильного устройства;
- в случае нарушения Клиентом настоящих Правил;
- вследствие принятия высшими органами законодательной и исполнительной власти Российской Федерации решений, которые делают невозможным для Банка выполнение своих обязательств по предоставлению Услуги;
- вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора и/или оператора доступа к сети Интернет;
- Банк не несет ответственность за качество линий связи;
- Банк не несет ответственности за любые убытки, понесенные Клиентом в результате действия или бездействия оператора сотовой связи либо иного третьего лица. Иск может быть предъявлен фактическому виновнику убытков, исключая Банк.

7.6. Ответственность за правильность оформления первичных документов несет Клиент. Банк несет ответственность за сохранность электронных документов и своевременное исполнение платежных документов.

7.7. Клиент поставлен в известность и в полной мере осознает, что использование Мобильного приложения несет риск несанкционированного доступа от имени Клиента к системе «Клиент-Банк» и конфиденциальной информации Клиента третьих лиц в случае утери или передачи третьим лицам Мобильного устройства и/или компрометации Мобильного приложения. Клиент несет ответственность за несанкционированный доступ третьих лиц к Мобильному устройству и своевременное информирование Банка в соответствии с п.3.3.23. настоящих Правил.

8. Порядок внесения изменений и/или дополнений в Правила и/или Тарифы на услуги

8.1. Банк вправе в одностороннем порядке вносить изменения и/или дополнения в Тарифы на услуги и в настоящие Правила, в том числе утверждать новую редакцию Правил.

8.2. Банк информирует Клиента о внесении изменений/ дополнений в настоящие Правила, в том числе об утверждении новой редакции Правил не менее, чем за 2 (Два) рабочих дня до даты вступления таких изменений/ дополнений/ новой редакции Правил в силу путем направления информационного сообщения по Системе «Клиент-Банк» и/или размещения информации на корпоративном Интернет-сайта Банка https://www.exibank.ru.

8.3. Банк вправе вносить изменения в Тарифы на услуги в части размера комиссий, уплачиваемых Клиентом Банку за обслуживание в Системе «Клиент-Банк», срока и порядка оплаты указанных комиссий, с предварительным уведомлением Клиента об изменениях не менее, чем за 2 (Два) рабочих дня до даты вступления в силу соответствующих изменений следующими способами:

- путем размещения информации в офисах обслуживания Клиентов Банка и на корпоративном Интернет-сайте Банка https://www.exibank.ru;
- путем направления сообщения Клиентам, не подключенным к Системе «Клиент-Банк», на электронный адрес, указанный Клиентом в Заявлении о присоединении;
- по Системе «Клиент-Банк».

8.4. Все изменения /дополнения вступают в силу, начиная со дня, следующего за днем истечения срока направления информационного сообщения в порядке, указанном в п. 8.2. и в п. 8.3. настоящих Правил и размещения на корпоративном Интернет-сайте Банка https://www.exibank.ru

8.5. В случае несогласия Клиента с изменениями/ дополнениями, внесенными Банком в Правила или Тарифы на услуги, новой редакцией Правил, Клиент имеет право расторгнуть Договор в порядке, предусмотренном разделом 9 настоящих Правил.

9. Опубликование информации

9.1. Под опубликованием информации в Правилах понимается размещение Банком информации на корпоративном Интернет-сайте Банка https://www.exibank.ru

9.2. Моментом публикации Правил, планируемых изменений/дополнений Правил/Тарифов на услуги считается момент их первого размещения на корпоративном Интернет-сайте Банка.

9.3. Банк не несет ответственности, если информация об изменении и/или дополнении Правил/ Тарифов на услуги, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.

10. Срок действия и порядок расторжения Договора

10.1. Договор считается заключенным и вступает в силу:

- с даты проставления отметки о приеме уполномоченным сотрудником **Банка** на Заявлении о присоединении, составленном по форме приложений №1 к настоящим Правилам или по иной форме, установленной Банком, представленном Клиентом в Банк на бумажном носителе;
- с даты открытия расчетного счета в случае предоставления в Банк Заявления о присоединении в целях открытия первого расчетного счета

и действует до момента его расторжения по соглашению сторон или в одностороннем порядке одной из Сторон в соответствии с пунктами 10.2.-10.4. настоящих Правил.

10.2. Договор об обслуживании с использованием Системы, заключенный в соответствии с настоящими Правилами, может быть расторгнут в одностороннем порядке по инициативе Банка. Банк уведомляет об этом Клиента не позднее, чем за 15 (Пятнадцать) календарных дней до даты расторжения путем направления письменного уведомления

(заказным почтовым отправлением с уведомлением о вручении или по Системе «Клиент-Банк»). Договор считается расторгнутым с даты, указанной в уведомлении Банка.

10.3. Договор об обслуживании с использованием Системы, заключенный в соответствии с настоящими Правилами, может быть расторгнут по инициативе Клиента. Клиент направляет в Банк письменное заявление о расторжении Договора, составленное по форме Приложения № 6 к настоящим Правилам. Договор считается расторгнутым с даты получения Банком Заявления.

10.4. Договор об обслуживании с использованием Системы, заключенный в соответствии с настоящими Правилами, автоматически прекращает свое действие при расторжении договора(ов) банковского счета Клиента, заключенного(ых) между Банком и Клиентом.

11. Порядок разрешения споров и доказательства принадлежности ЭП при разборе конфликтных ситуаций

11.1. В случае возникновения споров по настоящему Договору или в связи с ним, Банк и Клиент примут все меры к их разрешению на взаимоприемлемой основе путем переговоров и действий в соответствии с законодательством Российской Федерации.

11.2. Разбор конфликтной ситуации выполняется по инициативе любого участника Системы и состоит из:

- предъявления претензии одной из Сторон другой;
- формирования комиссии для рассмотрения конфликтной ситуации;
- разбора конфликтной ситуации.

11.3. Претензии друг к другу рассматриваются Сторонами на основании официально врученных уведомлений в письменном виде.

11.4. Стороны вправе решать возникающие претензии в рабочем порядке. По факту претензии Стороны проводят внутреннее расследование и официально информируют друг друга о его результатах в течение 14 (четырнадцати) календарных дней с даты получения претензии. Сторона, предъявившая претензию, в срок 5 (пять) рабочих дней после получения результатов расследования от другой Стороны, должна рассмотреть достаточность представленных объяснений и направить официальное уведомление о снятии претензии или предложение о создании комиссии по разрешению спорной ситуации.

11.5. В случае если хотя бы одна из Сторон при возникновении спора высказывает недоверие к составу и формату электронных документов, хранящихся в локальном архиве рабочего места Клиента или Банка, или высказывает недоверие к программному обеспечению, функционирующему на данном рабочем месте, или не удовлетворена результатами рассмотрения претензии в рабочем порядке, то Стороны обязаны сформировать комиссию для рассмотрения конфликтной ситуации. Целью работы комиссии является установление правомерности и обоснованности претензии, а также установление, если необходимо, подлинности и Авторства электронного документа.

11.6. В состав комиссии для рассмотрения конфликтной ситуации входит равное количество, но не менее двух, представителей от каждой из Сторон, определяемых Сторонами самостоятельно. При необходимости, по согласованию Сторон, к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, а также (если конфликтная ситуация возникла при проведении расчетов по Системе «Клиент-Банк») эксперт – представитель Разработчика СКЗИ «КриптоПро CSP» / эксперт – представитель Разработчика PayControl / эксперт – представитель Удостоверяющего Центра ООО «АйтиКом». Оплата участия в работе комиссии представителя Разработчика производится Банком за счет Стороны, предъявляющей претензию. Право представлять соответствующую Сторону в комиссии должно подтверждаться доверенностью, выданной каждому представителю на согласованный Сторонами срок работы комиссии.

11.7. Комиссия определяет, включая, но, не ограничиваясь, следующее:

- предмет разногласий на основании письма Стороны-инициатора разбирательства и разъяснений Сторон;
- правомерность предъявления претензии на основании текста заключенного Договора (настоящих Правил и Приложений к ним);
- документы в электронной форме, относящиеся к предмету разногласий;
- идентичность открытых ключей Клиента или Банка (в случае оспаривания ЭД, подписанного УНЭП в Системе «Клиент-Банк»);
- идентичность ключей Клиента (в случае оспаривания ЭД, подписанного Средством ЭП PayControl в Системе «Клиент-Банк»);
- идентичность электронного документа документу на бумажном носителе, сформированному в Банке;
- истинность электронной подписи электронного документа;

- наличие и содержание подтверждения по электронному документу;
- даты и время поступления, отправки электронного документа и подтверждения по нему;
- исправность используемых ключевых носителей в случае оспаривания ЭД, подписанного УНЭП в Системе «Клиент-Банк».

11.8. Стороны договариваются, что для разбора конфликтных ситуаций комиссия принимает на рассмотрение электронные документы и подтверждения по ним и обязана использовать следующие, признаваемые сторонами, эталонные данные:

- данные электронного архива принятых, отправленных документов;
- данные базы данных регистрационных записей (журнал регистрации приема и отправки электронных документов);
- подписанные Клиентом оригиналы бланков заявлений на изготовление сертификатов пользователей УЦ при подключении Системы «Клиент-Банк»;
- хранимое у Банка программное обеспечение Системы.

11.9. Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов экспертной комиссии.

11.10. Действия комиссии при использовании ПЭП Клиентом в Системе «Клиент-Банк».

Комиссия осуществляет подтверждение подлинности оспариваемого ЭД путем проверки факта:

- идентификации и Аутентификации клиента в Системе «Клиент-Банк»;
- направления Банком SMS-сообщения с одноразовым кодом на Зарегистрированный номер при подписании Акта признания ключа проверки ЭП;
- ввода корректного одноразового кода;
- того, что введенный одноразовый код прошел проверку на правильность с положительным результатом и время его ввода не истекло;
- совпадения даты в документе, сформированном в Системе «Клиент-Банк», а также даты и времени ввода одноразового кода.

11.11. Действия комиссии при использовании УНЭП Клиентом в Системе «Клиент-Банк».

11.11.1. Экспертиза осуществляется в три этапа:

Этап 1. Подготовка оборудования и программного обеспечения и тестирование их работоспособности.

Этап 2. Контроль целостности оспариваемого электронного документа путем проверки ЭП при помощи Сертификата открытого ключа ЭП, представленного Банком.

Этап 3. Аутентификация отправителя оспариваемого электронного документа путем проверки принадлежности, актуальности и целостности Сертификата, использованного комиссией для проверки ЭП.

11.11.2. Подготовка и проверка работоспособности оборудования и программного обеспечения проводятся в следующем порядке:

- производится конфигурирование операционной системы, осуществляется проверка предоставленного Банком персонального компьютера на предмет отсутствия вирусов и программных закладок;
- производится установка эталонного программного обеспечения СКЗИ «КриптоПро CSP». Для установки эталонного программного обеспечения СКЗИ «КриптоПро CSP» используется дистрибутив, представленный Разработчиком;
- членам экспертной комиссии предоставляется возможность убедиться в работоспособности, установленного программного обеспечения путем проведения тестов, в порядке, предусмотренном документацией на СКЗИ «КриптоПро CSP».

11.11.3. Контроль целостности оспариваемого электронного документа производится посредством стандартной процедуры проверки ЭП, предусмотренной СКЗИ «КриптоПро CSP». Проверка осуществляется на Сертификате ЭП, файл которого предъявляется Банком комиссии на защищенном носителе.

11.11.4. Для доказательства подлинности (принадлежности, актуальности и целостности) Сертификата, использованного для проверки ЭП, которой подписан оспариваемый документ, Банк должен предъявить членам комиссии заверенное уполномоченным лицом Клиента заявление на изготовление сертификата пользователя УЦ.

Примечание.
Проверка принадлежности, актуальности и целостности Сертификата, подтвержденного письменным

документом, проводится путем визуальной сверки членами экспертной комиссии распечатки файла Сертификата, записанного на представленном Банком съемном носителе и реквизитов ключа проверки ЭП заявления на изготовление сертификата пользователя УЦ, зафиксированных в бумажном документе.

11.11.5. Подтверждением подлинности оспариваемого электронного поручения является единовременное наличие следующих условий:

- проверка ЭП оспариваемого электронного документа на Сертификате, файл которого предъявлен Банком, дала положительный результат;
- подтверждена принадлежность, актуальность и целостность Сертификата открытого ключа Клиента с помощью которого проводится проверка ЭП оспариваемого электронного поручения.

11.12. Действия комиссии при использовании Средства ЭП PayControl Клиентом в Системе «Клиент-Банк»

11.12.1. Для проведения технической экспертизы спорного Электронного документа Экспертная комиссия получает:

У Администратора Системы «Клиент-Банк» и Средства ЭП PayControl (после изменения статуса операции на «Подписана» в качестве электронной подписи документа):

- специализированное ПО разработчика Средства ЭП PayControl – ПО АРМ РКС;
- идентификатор пользователя;
- спорная операция (файл спорного электронного документа и/или данные транзакции);
- код подтверждения, выработанный на симметричных ключах;
- ЭП, выработанная на ассиметричных ключах (при оффлайн-подтверждении отсутствует);
- время выработки ЭП.

Из карточки Юридического досье Клиента:

- Акт признания ключа проверки ЭП (достоверность и работоспособность которого установлена на время совершения спорной Операции).

11.12.2. Проведение технической экспертизы спорного Электронного документа включает в себя выполнение следующих действий:

- загрузку в АРМ РКС:

- идентификатора пользователя;
- спорная операция;
- Код подтверждения, выработанный на симметричных ключах;
- ЭП, выработанная на ассиметричных ключах (при оффлайн-подтверждении отсутствует);
- время выработки ЭП.

- проверку результатов разбора в АРМ РКС;
- печать протокола работы АРМ РКС.

11.12.3. В случае, если:

- ЭП и(или) Код подтверждения для данной спорной операции верны;
- Ключ проверки ЭП, отобранный для разбора конфликтной ситуации, соответствует значению ключа в Акте признания ключа проверки ЭП, считается установленным:

  - что проверяемая спорная операция была подписана Ключом ЭП, соответствующим зарегистрированному Банком Ключу проверки ЭП, использованному при проведении технической экспертизы и(или) предоставлен Код подтверждения, выработанный на симметричном ключе, владельцем которого является Клиент, зарегистрированный Банком;
  - владельцем Ключа ЭП и Ключа проверки ЭП является Представитель Клиента, зарегистрированный Банком.

  спор решается в пользу Банка.

11.12.4. В случае, если:

- ЭП и(или) Код подтверждения для данной спорной операции не верны;
- Ключ проверки ЭП, отобранный для разбора конфликтной ситуации, не соответствует значению ключа в Акте признания ключа проверки ЭП (достоверность и работоспособность которого однозначно установлена на время совершения спорной операции) считается установленным:

  - что проверяемая спорная операция не была подписана Ключом ЭП, соответствующим зарегистрированному Банком Ключу проверки ЭП, использованному при проведении технической экспертизы и(или) Код

подтверждения выработан на симметричном ключе, владельцем которого не является Клиент, зарегистрированный Банком;

- владельцем Ключа ЭП и Ключа проверки ЭП не является Представитель Клиента, зарегистрированный Банком.

спор решается в пользу Клиента.

11.13. Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения всех этапов экспертизы. В Акте фиксируются результаты всех этапов проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного поручения. Акт составляется в двух экземплярах - по одному для представителей Банка и Клиента. Акт комиссии является окончательным и пересмотру не подлежит.

11.14. Подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ имеет юридическую силу и является законным основанием для осуществленных Банком операций по счету Клиента. Не подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ не имеет юридической силы и не является законным основанием для осуществленных Банком операций по счету Клиента.

11.15. Акт, составленный экспертной комиссией, являются доказательством при дальнейшем разбирательстве спора в судебных органах.

11.16. При возникновении конфликтов, связанных с признанием правомочности ЭД, Стороны примут все меры к разрешению их путем переговоров.

11.17. При невозможности разрешения споров и разногласий путем переговоров они разрешаются в Арбитражном суде города Москвы.

12. Порядок подключения Клиента к Системе «Клиент-Банк»

12.1. Для подключения Клиента к Системе «Клиент-Банк» с использованием УНЭП в Банк представляются на бумажном носителе: Заявка на подключение к Электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» (Приложение №5 к Правилам), Заявление на изготовление сертификата ключа проверки электронной подписи (Приложение №2 к Правилам), заверенные подписями зарегистрированных в Удостоверяющем центре лиц (владельцев сертификатов) и печатью Клиента (при ее наличии), с отметкой УЦ о выпуске сертификатов, Заявка на установление ограничения на подключение к электронной системе «Клиент-Банк» по сетевым адресам (Приложение №4 к Правилам), в случае если Клиент ограничения установил.

12.2. Банк предоставляет Клиенту логин для доступа к системе «Клиент-Банк» после заключения Договора (присоединения к Правилам). По заявлению Клиента логин может быть направлен Клиенту по электронной почте. После подключения Клиента к Системе, Клиент получает на Зарегистрированный номер телефона SMS сообщение с одноразовым паролем для первичного входа в Систему «Клиент-Банк». Клиент обязан использовать одноразовый пароль для первичного входа в Систему «Клиент-Банк» в течении 3 (Трех) календарных дней с даты получения SMS с одноразовым паролем.

12.3. Для подключения Клиенту подключенному к Системе «Клиент-Банк» с использованием Средства ЭП PayControl возможности подписания электронных документов Средством ЭП PayControl в Банк представляется соответствующее оформленное Заявление о присоединении по форме Приложения №1 к Правилам или по иной форме, установленной Банком, в бумажном виде или в электронном виде по Системе «Клиент-Банк» путем вложения оформленного Заявления в сообщение в опции Документы свободного формата и подписания его усиленной электронной подписью.

12.5. Если Клиенту подключена Система «Клиент-Банк» с использованием УНЭП, доступ к подсистеме Интернет-Клиент Системы «Клиент-Банк» с момента активации Ключа УНЭП (и шифрования) осуществляется как с использованием УНЭП, так и с использованием Средства ЭП PayControl.

12.9. Для идентификации Банком лиц-владельцев ключей электронной подписи (и шифрования), указанных в Заявлении о присоединении / Заявке на подключение к Электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» и/или сотрудника Клиента, уполномоченного подписывать ЭД Средством ЭП PayControl, Клиент представляет в Банк документы, удостоверяющие личности (оригиналы или нотариально заверенные копии), и документы, подтверждающие полномочия указанных лиц на использование аналогов собственноручной подписи (электронной подписи) (оригиналы или заверенные в установленном порядке копии с предоставлением оригиналов для сверки) в случае непредоставления данных документов ранее для открытия/ведения банковских счетов.

12.10. В случае, если между Клиентом и Банком ранее заключен Договор об обслуживании Клиента по электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» на бумажном носителе, Клиент подтверждает согласие (акцепт) на осуществление электронного документооборота на условиях настоящей редакции Правил путем представления в Банк Заявления о присоединении к Правилам обмена электронными документами по Системе дистанционного банковского обслуживания на бумажном носителе, составленного по форме Приложения №1 к настоящим Правилам с проставлением отметки о приеме уполномоченным сотрудником Банка на Заявлении.

13. Порядок взаимодействия участников расчетов по электронной системе «Клиент-Банк»

13.1. Клиент обеспечивает комплектование аппаратного обеспечения для программного комплекса Системы, а также предоставляет каналы связи и помещение согласно требованиям, изложенным в разделе 14 и п. 3.3.3. Правил.

13.2. Формирование ключей шифрования и УНЭП Клиента осуществляется после заключения Договора (присоединения к Правилам), в соответствии с порядком, указанным в настоящем разделе Правил, и регистрации уполномоченного лица Клиента в Удостоверяющем центре.

13.3. Полномочия лиц, осуществляющих формирование ключей УНЭП (и шифрования), определяются на основании Заявки на подключение к Электронной системе «Клиент-Банк» (Приложения №5 к настоящим Правилам).

13.4. При подключении к Системе формирования ключей Клиента и Сертификатов ключей проверки УНЭП осуществляется Клиентом самостоятельно на своем рабочем месте используя Руководство пользователя.

13.5. При генерации ключей УНЭП на своем рабочем месте Клиент отправляет в УЦ запрос на выпуск Сертификата. Перед получением Сертификата ключа проверки УНЭП Клиент обязан заверить Заявление на изготовление сертификата пользователя УЦ (Приложение №2 к Правилам), подписью уполномоченного лица (владельца Сертификата ключа подписи), скрепить оттиском печати (при ее наличии) и передать в Банк.

13.6. Сертификата ключа проверки УНЭП Клиенту подтверждает использование УНЭП электронных документов и их шифрования исключительно данных ключей в период их действия.

13.7. Клиент обязан производить периодическую (плановую) замену используемых ключей УНЭП (и шифрования) в срок, указанный в Сертификате открытого ключа.

13.8. При самостоятельной плановой смене ключей УНЭП на своем рабочем месте Клиент отправляет в УЦ запрос на выпуск Сертификата, подписанный действующей ЭП, и предоставить в Банк Заявление на изготовление сертификата ключа проверки электронной подписи (Приложение №2 к Правилам), заверенные подписями зарегистрированных в Удостоверяющем центре лиц (владельцев сертификатов) и печатью Клиента (при ее наличии), с отметкой УЦ о выпуске сертификатов.

13.9. Если в результате проверки обнаружена неработоспособность (несовместимость) технических или программных средств, или причиной неработоспособности является низкое качество линий связи, Банк/УЦ представляет Клиенту рекомендации по комплектации рабочего места техническими и программными средствами, Клиент следует этим рекомендациям и принимает меры по улучшению качества линий связи. В случае, если Клиент отказывается следовать рекомендациям Банка/УЦ, то Банк оставляет за собой право расторгнуть Договор в порядке, установленном в разделе 10 настоящих Правил.

13.10. Клиент в Системе «Клиент-Банк» подготавливает для Банка ЭД установленной формы. При этом он заполняет соответствующие реквизиты в сформированной электронной форме документа. За правильное заполнение платежных и иных реквизитов документа несет ответственность Клиент.

13.11. После подготовки ЭД Клиентом производится его подписание ЭП, шифрование и отправка в Банк по каналам связи. Порядок подготовки, контроля и отправки электронных документов в Банк подробно описан в документации на программное обеспечение Системы «Клиент-Банк».

13.12. Клиент может отозвать свой ЭД до его исполнения Банком (до наступления безотзывности перевода денежных средств), создав в Системе «Клиент-Банк» электронный документ «Запрос на отзыв документа» и выбрав из списка ЭД для отзыва. Электронный документ «Запрос на отзыв документа» шифруется и подписывается ЭП Клиента. Так же Клиент может направить заявление на отзыв в текстовом сообщении Системы «Клиент-Банк», с указанием реквизитов, необходимых для осуществления отзыва (номер, дата составления, сумма расчетного документа, наименование получателя средств). Текстовое сообщение на отзыв шифруется и подписывается ЭП Клиента.
Банк не позднее рабочего дня, следующего за днем поступления заявления об отзыве, направляет Клиенту уведомление в электронном виде об отзыве с указанием даты, возможности (невозможности в связи с наступлением безотзывности перевода денежных средств) отзыва распоряжения (ЭД). Заявление об отзыве служит основанием для аннулирования Банком распоряжения (ЭД).

13.13. В рамках настоящих Правил осуществляются следующие **процедуры приема ЭД к исполнению**:

13.13.1. *процедура удостоверения права распоряжения денежными средствами (удостоверение права использования электронного средства платежа)* осуществляется автоматически посредством Системы «Клиент-Банк» при сеансе связи при передаче ЭД Клиентом в Банк путем проверки права владельца ЭП на удостоверение права распоряжения денежными средствами;

13.13.2. *процедура контроля целостности распоряжений* осуществляется Системой «Клиент-Банк» в 2 этапа:

13.13.2.1. автоматически перед отправкой Клиентом в Банк ЭД на этапе заполнения ЭД Клиентом, положительный результат контроля целостности подтверждается возможностью проставления ЭП на ЭД;

13.13.2.2. автоматически при получении Банком ЭД путем проверки корректности ЭП, которой подписан ЭД;

13.13.3. *процедура контроля наличия в Акте признания ключа проверки ЭП ПЭП*, обеспечивает наличие в созданном и (или) подписанном Акте признания ключа проверки ЭП информации, указывающей на логин Уполномоченного лица Клиента, указанный в Заявке ПЭП, от имени которого был создан и подписан Акт признания ключа проверки ЭП. Факт формирования ПЭП подтверждается путем ввода Уполномоченным лицом Клиента одноразового кода, направленного на Зарегистрированный номер в виде SMS сообщения. Одноразовый код для подтверждения факта формирования ПЭП генерируется в привязке к Зарегистрированному номеру и самому подтверждаемому Акту признания ключа проверки ЭП. Акт признания ключа проверки ЭП считается подписанным Клиентом в случае, если одновременно выполняются следующие условия:

- установлен факт входа под логином Клиента в подсистему Интернет-Клиент Системы «Клиент-Банк», предшествующий отправке Акта признания ключа проверки ЭП в Банк;
- установлен факт отправления SMS сообщения с одноразовым кодом на Зарегистрированный номер Клиента;
- установлен факт ввода одноразового кода для подтверждения факта формирования ЭП Клиентом;
- отправленный Банком SMS сообщением одноразовый код совпадает с введенным Клиентом в Систему кодом и время ввода не просрочено.

13.13.4. *процедура структурного контроля распоряжений* осуществляется Системой «Клиент-Банк» автоматически путем проверки соответствия ЭД форме, установленной Системой «Клиент-Банк» и наличия заполнения полей формы ЭД необходимым количеством символов и реквизитов;

13.13.5. *процедура контроля значений реквизитов распоряжений* осуществляется Системой «Клиент-Банк» и Автоматизированной банковской системой автоматически путем проверки в ЭД реквизитов, их допустимости и соответствие требованиям законодательства;

13.13.6. *процедура контроля достаточности денежных средств* осуществляется многократно Автоматизированной банковской системой путем автоматической проверки достаточности денежных средств на банковском счете Клиента, исходя из остатка денежных средств, находящихся на банковском счете Клиента на момент приема ЭД с учетом сумм денежных средств, списанных с банковского счета Клиента и зачисленных на его банковский счет до определения достаточности денежных средств на банковском счете Клиента, а также с учетом сумм наличных денег, выданных с банковского счета Клиента и зачисленных на его банковский счет до определения достаточности денежных средств на банковском счете Клиента;

13.14. При положительном результате прохождения всех процедур приема ЭД к исполнению, Банк направляет в день принятия ЭД к исполнению Клиенту уведомление в электронном виде посредством Системы «Клиент-Банк» о приеме данного ЭД к исполнению с указанием даты принятия ЭД к исполнению.

13.15. ЭД, прошедшие все процедуры приема к исполнению, подлежат исполнению не позднее рабочего дня, следующего за днем поступления в Банк, соответствующего ЭД, если иной срок не предусмотрен законом, изданными в соответствии с ним банковскими правилами или Договором, заключенным между Клиентом и Банком.

В тот же срок Банк направляет Клиенту посредством Системы «Клиент-Банк» ЭД, содержащие распоряжения Клиента и иные расчетные документы о списании денежных средств со счета Клиента, содержащие штамп «ПРОВЕДЕНО» (с указанием даты исполнения соответствующего распоряжения/ расчетного документа) и являющиеся подтверждением исполнения Банком распоряжений Клиента.

Ежедневно не позднее рабочего дня, следующего за днем совершения операций, Банк предоставляет посредством Системы «Клиент-Банк» выписку о проведении операций по счету/счетам Клиента (на основании распоряжений, переданных/поступивших в Банк посредством Системы «Клиент-Банк» или на бумажном носителе) и приложений к ней. При этом выписки на бумажном носителе в порядке, предусмотренном соответствующим Договором банковского счета, заключенным между Банком и Клиентом, по мере совершения операций не

предоставляются.

Выписка на бумажном носителе (о совершении операций по счету за любой указанный Клиентом период времени) предоставляется Банком по требованию Клиента в качестве дубликата лицам, указанным в Карточке с образцами подписей и оттиска печати, а также лицам, имеющим доверенность на получение выписок по счету/ счетам Клиента. Плата за предоставление дубликата выписки взимается Банком в соответствии с Тарифами на услуги, и Договором банковского счета.

Выписка на бумажном носителе за последний рабочий день года (по состоянию на 1 января года, следующего за отчетным), а также в иных случаях, предусмотренных законодательством Российской Федерации, предоставляется Банком Клиенту без взимания платы.

В случае помещения ЭД в очередь не исполненных в срок распоряжений, Банк направляет Клиенту уведомление в электронном виде с указанием в нем номера и суммы ЭД, а также даты помещения ЭД в очередь не исполненных в срок распоряжений.

13.16. При отрицательном результате процедур приема к исполнению ЭД Банк не принимает ЭД к исполнению и направляет Клиенту уведомление в электронном виде об аннулировании данного ЭД с указанием информации, позволяющей идентифицировать аннулируемое распоряжение (даты, номера и суммы документа), даты его аннулирования, а также причины аннулирования в виде текстового комментария.

13.17. В рамках Системы «Клиент-Банк» прием платежных и Служебно-информационных документов Клиента осуществляется Банком в автоматическом режиме круглосуточно и ежедневно, за исключением возможных технологических перерывов с 20-00 до 02-00 по московскому времени. Платежные документы по операциям в рублях и в иностранной валюте, принятые Банком, исполняются согласно установленного внутренним Приказом по Банку режима операционного обслуживания Клиентов, но не позднее рабочего дня, следующего за днем поступления в Банк ЭД, если иное не предусмотрено Договором.

13.18. Информация об остатке денежных средств на счете предоставляется Клиенту:

- за предыдущий рабочий день – до 9-30 по московскому времени следующего календарного дня;
- текущая (актуальная) информация об остатке денежных средств по счету Клиента – в течение 20 минут после зачисления\списания денежных средств по счету.
- дополнительная информация об остатке денежных средств по счету предоставляется Клиенту по его запросу, направленному по Системе «Клиент-Банк».

13.19. В процессе сеансов связи Клиент получает информацию об этапах приема, контроля и прохождения ЭД в Банке путем смены статуса ЭД в Системе.

13.20. Клиент посредством Системы «Клиент-Банк» передает в Банк Документы свободного формата, подписанные действующей УНЭП.

В случае если документы, подтверждающие полномочия представителя Клиента - Владельца сертификата ключа проверки УНЭП подписывать направленный им в Банк конкретный вид Документа свободного формата в Банке отсутствуют, то Документ свободного формата должен обязательно содержать вложенный файл (файлы) в формате pdf, включающий всю направляемую в Банк в составе данного документа информацию, на котором проставлена УНЭП Пользователя, обладающего необходимыми полномочиями в соответствии с представленными в Банк документами.

13.23. Получение Банком от Клиента и Клиентом от Банка документов посредством электронной системы «Клиент-Банк», в том числе в порядке, указанном в п.13.22. настоящих Правил, не требует повторного предоставления документов на бумажном носителе.

14. Требования к Клиентам, осуществляющим эксплуатацию сертифицированных ФСБ России средств криптографической защиты информации

14.1. Техническое обслуживание сертифицированных ФСБ России шифровальных средств могут осуществлять только организации, имеющие соответствующие лицензии ФСБ.

14.2. Уполномоченное лицо Клиента назначает ответственных должностных лиц из числа сотрудников Клиента, ответственных за сохранность ключей УНЭП (и шифрования) и имеющих право работать с Системой «Клиент-Банк».

14.3. Специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), должны обеспечивать Безопасность информации, СКЗИ и ключей УНЭП (и шифрования), сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

14.4. Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом

специфики и условий функционирования конкретной структуры Клиента.

14.5. Для хранения защищенных носителей ключей УНЭП (и шифрования), нормативной и эксплуатационной документации, 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 распорядительным документом Клиента.

14.6. Устанавливаемый руководителем Клиента порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

14.7. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

14.8. Системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля за их вскрытием.

14.9. В целях противодействия получению несанкционированного доступа к секретным ключам ЭП (и шифрования), ключи УНЭП (и шифрования) должны находиться только на защищенных носителях (смарт-картах, USB-токенах и т.п.) у ответственных лиц. Размещение ключей в реестре операционной системы не допустимо.

14.10. В случае сохранения ключа на незащищенный носитель (например, в реестр), Клиент обязан выполнить внеплановую смену ключа и отозвать сертификат в УЦ, сохраненный на незащищенный носитель, и направить в Банк Заявление по форме Приложения №3 к Правилам.

14.11. Все защищенные носители с ключами УНЭП (и шифрования) должны учитываться в специально выделенных для этих целей журналах.

14.12. Учет и хранение носителей закрытых ключей УНЭП (и шифрования) осуществляется уполномоченными лицами Клиента, имеющими право подписи электронных платежей. Их не рекомендуется передавать на хранение и использование лицам, не имеющим право подписи электронных платежей.

14.13. Хранение носителей ключей УНЭП (и шифрования) допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

14.14. При пересылке ключей УНЭП (и шифрования), должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.

14.15. В случае отсутствия индивидуального хранилища у лиц, ответственных за использование СКЗИ Клиента, ключи УНЭП (и шифрования) по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

14.16. Клиент обязан не допускать появления в компьютере, на котором установлена Система «Клиент-Банк», компьютерных вирусов, программ-шпионов и других вредоносных программ для исключения несанкционированного перехвата ключевой информации и передачи ее третьим лицам. Для чего не рекомендуется с компьютера, на котором установлена Система «Клиент-Банк», посещать ресурсы интернет и пользоваться электронной почтой.

14.17. Клиент обязан производить перегенерацию и замену ключей УНЭП (и шифрования) не реже 1 (Одного) раза в год, и каждый раз при изменении состава должностных лиц, уполномоченных распоряжаться счетом.

14.18. Каждый пользователь Клиента может иметь только один ключ УНЭП (и шифрования) для работы в системе «Клиент-Банк».

14.19. К работе с СКЗИ допускаются решением (распорядительным документом) руководителя Клиента только сотрудники, знающие правила их эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

14.20. Руководитель Клиента и лица, уполномоченные на осуществление эксплуатации шифровальных средств, должны иметь представление о возможных угрозах утечки секретной информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

15. Обязанности Клиента по хранению носителей ключевой информации и программного обеспечения

15.1. Клиент обязуется обеспечить соблюдение порядка хранения защищенных носителей с ключевой информацией СКЗИ и условия хранения и использования программного обеспечения СКЗИ, исключающие порчу и утрату защищенного носителя, а также их использование любыми другими лицами.

15.2. Клиент, допустивший утрату контроля за носителем с ключевой информацией СКЗИ, независимо от наличия или отсутствия сведений о его несанкционированном использовании, незамедлительно сообщает об этом УЦ и Банку

и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля защищенный носитель с ключевой информацией СКЗИ не подлежит дальнейшему использованию.

16. Порядок электронного документооборота по Документам валютного контроля

16.1. Клиент подписывает документы для валютного контроля, направляемые в Банк посредством Системы «Клиент-Банк», ЭП Клиента.

16.2. Документы для валютного контроля, требование о представлении которых предусмотрено нормативными документами Банка России, Клиент передает в Банк посредством Системы «Клиент-Банк» как сформированные в электронном виде, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

16.3. Датой предоставления Клиентом в Банк документов и информации по валютному контролю является:

- для Форм учета по валютным операциям – дата, указанная в штампе «Получено по системе электронных платежей. Подписи проверены», проставляемом автоматически Системой «Клиент-Банк» на стороне Банка при получении Банком документов;
- для Ведомостей банковского контроля и иных документов, предусмотренных действующим валютным законодательством Российской Федерации – дата, указанная в штампе «Получено по системе электронных платежей. Подписи проверены», автоматически проставляемом Системой «Клиент-Банк» на сопроводительном/произвольном документе, созданном Клиентом в Системе «Клиент-Банк» и содержащем информацию и/или прикрепленный файл (файлы).

16.4. Датой предоставления Клиентом в Банк документов валютного контроля считается день поступления документов в Банк посредством Системы «Клиент-Банк» в период времени операционного обслуживания Клиентов.

16.5. При поступлении документов валютного контроля в Банк после указанного в п.16.4. настоящих правил времени датой предоставления Клиентом в Банк документов будет считаться следующий день операционного обслуживания Клиентов.

16.6. Документы валютного контроля, полученные Банком от Клиента, должны быть четкими, понятными и полными.

16.7. Документы валютного контроля, направляемые Клиенту посредством Системы «Клиент-Банк», подписываются со стороны Банка аналогом собственноручной подписи Ответственного лица Банка по ВК (АСП) в соответствии с внутренними процедурами Банка.

16.8. Датой принятия Банком Форм учета по валютным операциям считается дата проставления окончательного статуса Ответственным лицом Банка по ВК на принятом документе в Системе «Клиент-Банк».

16.9. Датой принятия Банком контракта на учет считается дата направления Клиенту соответствующей информации Ответственным лицом Банка по ВК посредством Системы «Клиент-Банк».

16.10. Банк имеет право отказаться от принятия Документов валютного контроля Клиента в случаях, установленных действующим законодательством Российской Федерации, а также, в случае если Документы валютного контроля не соответствуют требованиям, указанным в пункте 16.6. настоящих Правил.

16.11. Датой возврата Банком Клиенту не принятых Документов валютного контроля является:

- для Форм учета по валютным операциям – дата проставления финального статуса об отказе в принятии Банком документа;
- для внешнеторговых контрактов (договоров займа, кредитных договоров), для Ведомостей банковского контроля и иных документов – автоматически сформированная дата сопроводительного/ произвольного документа, созданного и направленного Клиенту Ответственным лицом Банка по ВК по электронной системе «Клиент-Банк», содержащего информацию и/или прикрепленный файл (файлы) с указанием причины возврата.

16.12. При направлении Клиенту Документов валютного контроля посредством Системы «Клиент-Банк» могут передаваться как документы, сформированные посредством Системы, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

16.13. В случае если Документы валютного контроля содержат приложения в форме вложений, Стороны настоящим признают, что наличие надлежащего аналога собственноручной подписи на Документе валютного контроля означает подписание тем же аналогом собственноручной подписи соответствующей Стороны всех имеющихся приложений в форме вложения к такому Документу валютного контроля.

16.14. В случае если произвольный/сопроводительный документ, созданный в Системе, содержит приложения в форме вложений, Стороны настоящим признают, что наличие надлежащего аналога собственноручной подписи на указанном

произвольном/сопроводительном документе означает подписание тем же аналогом собственноручной подписи соответствующей Стороны всех имеющихся приложений в форме вложения к такому произвольному/ сопроводительному документу.

16.15. Получение Клиентом от Банка Документов валютного контроля посредством электронной системы «Клиент-Банк» исключает повторное предоставление Банком Клиенту Документов валютного контроля на бумажном носителе.

17. Порядок электронного документооборота с использованием Средства ЭП PayControl в Системе «Клиент-Банк»

17.1. Активация Средства ЭП PayControl.

17.1.1. Услуга предоставляется Клиенту после подписания Клиентом и Банком Акта признания ключа проверки ЭП подписанный действующей ПЭП и передачи его работнику Банка в Системе «Клиент-Банк».

17.1.2. Клиент и Банк признают успешно выполненную Банком Проверку ЭП в соответствии с настоящими Условиями равнозначной собственноручной подписи Клиента на документах, составленных на бумажном носителе.

17.1.3. Средство ЭП PayControl является средством простой ЭП. Стороны признают применение средства простой ЭП PayControl в Системе Клиент-Банк» достаточным для обеспечения целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания. Аутентификационные данные используются Клиентом при каждой Авторизации в Мобильном приложении PayControl.

17.2. Требования технической защиты к Мобильному устройству, реализуемые Клиентом.

17.2.1. Перед подключением к Средству ЭП PayControl Клиент должен обеспечить работу Мобильного устройства в следующем режиме:

- на Мобильном устройстве должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение;
- Мобильное устройство не должно быть подвергнуто операциям повышения привилегии/взлома операционной системы устройства (jail-break, rooting);
- Клиент должен использовать процедуру аутентификации доступа к Мобильному устройству.

17.2.2. Банк не контролирует, не проверяет, не дает одобрения и не несет какой-либо ответственности за иные приложения, добавляемые Клиентом на свое Мобильное устройство.

17.3. Организационные меры по Защите информации, реализуемые Клиентом.

17.3.1. Клиент несет ответственность за реализацию следующих мер по Защите информации:

- Клиент никогда и никому не сообщает Ключ ЭП и Пароль для Аутентификации входа в Мобильное приложение PayControl;
- Клиент использует 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;
- Клиент использует на своих рабочих станциях и/или Мобильных устройствах, применяемых для подключения к подсистемам Системы «Клиент-Банк» только лицензионное ПО;
- Клиент соблюдает требования лицензионного соглашения на Средство ЭП PayControl;
- Клиент обязуется устанавливать Мобильное приложение PayControl из официальных репозиториев AppStore и Google Play.

17.4. Выпуск ключей для Средства ЭП PayControl

17.4.1. Перед выпуском рабочих ключей Средства ЭП PayControl Клиенту необходимо выполнить требования технической защиты к Мобильному устройству, включая установку Мобильного приложения PayControl из одного из официальных репозиториев Google Play или App Store.

17.4.2. Ключи инициализации Средства ЭП PayControl выпускается Банком для каждой учетной записи Клиента – владельца Средства ЭП PayControl.

17.4.3. Первая часть Ключей инициализации в виде QR-кода передается Банком каждой учетной записи Клиента по защищенному каналу Системы «Клиент-Банк» через вывод на экран монитора при первом входе в «Клиент-Банк».

17.4.4. Вторая часть Ключей инициализации направляется учетной записи в виде SMS или сообщения на адрес электронный почты Уполномоченного лица.

17.4.5. После сканирования мобильным приложением Клиента первой части Ключей инициализации и ввода в Мобильное приложение PayControl значения второй части из SMS/электронный почты сообщения, Средство ЭП PayControl выполняет автоматическую процедуру выпуска рабочего Ключа ЭП с сохранением его в зашифрованном виде в Мобильном устройстве, отправки в Банк значения Ключа проверки ЭП и инициализации Ключа проверки ЭП в Банке.

17.4.6. Банк средствами Системы «Клиент-Банк» формирует Акт признания ключа проверки ЭП, и направляет его Клиенту средствами Системы «Клиент-Банк» по защищенному каналу Системы «Клиент-Банк»/

17.4.7. Клиент ознакамливается с полученным Акт признания ключа проверки ЭП признания ключа проверки электронной подписи PayControl, сравнивает реквизиты Акт признания ключа проверки ЭП, включая Идентификатор пользователя и значение Ключа проверки ЭП из Мобильного приложения PayControl со значениями в Акт признания ключа проверки ЭП, подписывает Акт признания ключа проверки ЭП в электронном виде в Системе «Клиент-Банк» с помощью действующей ПЭП Системы «Клиент-Банк».

17.5. Порядок подписания Электронных документов Средством ЭП PayControl

17.5.1. ЭД Клиента, подписанный Средством ЭП PayControl, считается подписанным, если он подписан с помощью Ключа ЭП, принадлежащего Клиенту, для которого Банком зарегистрирован Ключ проверки ЭП. И(или) подтвержден при помощи Кода подтверждения, выработанного на симметричных ключах.

17.5.2. Порядок подписания ЭД в Мобильном приложении PayControl:

- Банк на основании указания Клиента формирует и направляет Клиенту Электронное сообщение с шаблоном ЭД из Системы «Клиент-Банк».
- После поступления Клиенту от Банка через Мобильное приложение PayControl Электронного сообщения с шаблоном ЭД на Мобильное устройство Клиента поступает PUSH-сообщение о необходимости подписания ЭД.
- Клиент проходит Аутентификацию входа в Мобильном приложении PayControl.
- В Мобильном приложении PayControl Клиент видит Электронное сообщение Банка с шаблоном ЭД.
- Клиенту предоставляется возможность подписать ЭД Средством ЭП PayControl или отклонить подписание.
- В случае решения Клиента не подписывать ЭД, Клиент нажимает кнопку «Отказаться», в этом случае ЭД не будет подписан ЭП и не будет направлен на исполнение в Банк.
- В случае решения Клиента подписывать ЭД, Клиент нажимает кнопку «Подтвердить», в этом случае с помощью Мобильного приложения PayControl ЭД подписывается ЭП и направляется на исполнение в Банк.
- Банк выполняет проверку ЭП.
- Если Клиент не принял решение подписывать или не подписывать ЭД в течение установленного времени с момента получения соответствующего Электронного сообщения от Банка, такое Электронное сообщение исчезает из списка ЭД в Мобильном приложении PayControl и будет аннулировано на сервере PayControl.

17.6. В случае изменения лица, уполномоченного подписывать ЭД Средством ЭП PayControl и/или Мобильного устройства/Зарегистрированного номера телефона, Клиент предоставляет в Подразделение Банка новое Заявление о присоединении на бумажном носителе или путем направления в электронном виде с ЭП по Системе «Клиент-Банк» (Приложение 1 к настоящим Правилам). Банк исполняет Заявление о присоединении не позднее следующего рабочего дня после ее получения. При наличии всех документов, являющихся основанием для внесения соответствующих изменений.

17.7. Отключение возможности подписания документов Средством ЭП PayControl производится при предоставлении Клиентом в Подразделение Банка Заявки на отключение использования Средством ЭП PayControl для удостоверения документов в Электронной системе «Клиент-Банк» на бумажном носителе или путем направления указанной Заявки в электронном виде по Системе «Клиент-Банк» (Приложение 7 к настоящим Правилам). Банк исполняет Заявку не позднее следующего рабочего дня после ее получения

17.8. Отключение производится без заявления Клиента в случае выявления Банком неактуальности контактных сведений, ранее указанных Клиентом в Заявлении о присоединении. Банк не несет ответственности за возможные неблагоприятные последствия для Клиента в связи с выявлением Банком неактуальности ранее представленных Клиентом контактных сведений, а также несвоевременным сообщением Клиентом Банку актуальных данных.

18. Порядок электронного документооборота с использованием ПЭП в Системе «Клиент-Банк».

18.1. Подписывать Акт признания ключа проверки ЭП ПЭП может только одно Уполномоченное лицо Клиента. ПЭП Клиента является равнозначной (аналогом) его собственноручной подписи. Если иное не установлено Правилами,

Клиент вправе подписать ПЭП только Акт признания ключа проверки ЭП, предусматривающий подпись Клиента. Передача подписанного Заявления о присоединении в Банк подтверждает согласие Клиента на подписание ПЭП Акта признания ключа проверки ЭП в Системе «Клиент-Банк».

18.2. Банк предоставляет Клиенту, услугу подписания Акта признания ключа проверки ЭП ПЭП с использованием одноразовых кодов в виде SMS сообщений, формируемых и направляемых Банком по запросу Клиента на Зарегистрированный номер. Для подтверждения Аутентификации и совершения (подтверждения) операций, Клиент сообщает Банку одноразовый код, содержащийся в SMS -сообщении, правильность которого проверяется Банком.

18.3. Клиент в целях подписания Акта признания ключа проверки ЭП Клиент формирует в соответствующей опции Системы сообщение, к которому прикрепляет сканированную копию оформленного Документа свободного формата и инициирует его отправку. В Системе формируется запрос, в ответ на который Клиент получает от Банка на Зарегистрированный номер телефона SMS сообщение, содержащее одноразовый код/ Клиент обязан ввести в Систему одноразовый код только при условии согласия с проводимой операцией.

18.4. Каждый Клиент может использовать только один Зарегистрированный номер.

18.5. В случае изменения лица, уполномоченного подписывать ЭД ПЭП и/или Зарегистрированного номера телефона, Клиент предоставляет в Подразделение Банка новое Заявление о присоединении на бумажном носителе или путем направления в электронном виде с ЭП по Системе «Клиент-Банк» (Приложение 1 к настоящим Правилам). Банк исполняет Заявление о присоединении не позднее следующего рабочего дня после ее получения. При наличии всех документов, являющихся основанием для внесения соответствующих изменений.

18.6. Банк не несет ответственность за недоставку Платежной системой отправленного Сообщения, за недоставку оператором сотовой связи отправленного Банком SMS-сообщения.

18.7. Риск убытков и иных неблагоприятных последствий вследствие передачи ЭД, подтвержденных ПЭП, несет Клиент.

18.8. Отключение возможности подписания документов ПЭП и производится при предоставлении Клиентом в Подразделение Банка Заявки на отключение использования простой электронной подписи для удостоверения документов в Электронной системе «Клиент-Банк» на бумажном носителе или путем направления указанной Заявки в электронном виде по Системе «Клиент-Банк» (Приложение 7 к настоящим Правилам). Банк исполняет Заявку не позднее следующего рабочего дня после ее получения

18.9. Отключение производится без заявления Клиента в случае выявления Банком неактуальности контактных сведений, ранее указанных Клиентом в Заявлении о присоединении. Банк не несет ответственности за возможные неблагоприятные последствия для Клиента в связи с выявлением Банком неактуальности ранее представленных Клиентом контактных сведений, а также несвоевременным сообщением Клиентом Банку актуальных данных.

18. Порядок электронного документооборота с использованием сервиса «Онлайн конверсия» Системы «Клиент- Банк»

19.1. Банк проводит следующие виды Конверсионных сделок в сервисе «Онлайн конверсия»:

– покупка/продажа Иностранной валюты за Валюту РФ;
– покупка/продажа Иностранной валюты за другую Иностранную валюту.

Не производится продажа Иностранной валюты с транзитных валютных счетов Клиента.

19.2. Клиент в сервисе «Онлайн конверсия» формирует Поручение на конверсию валюты:

- путем самостоятельного заполнения следующих параметров Конверсионной сделки:
  - номера расчетного счета Клиента[4], с которого производится списание продаваемой Валюты;
  - номера расчетного счета Клиента, на который должно производиться зачисление приобретенной Валюты;
  - суммы покупаемой или продаваемой Валюты;
- автоматического заполнения сервисом «Онлайн Конверсия» следующих параметров Конверсионной сделки:
  - Курс Банка,
  - суммы покупаемой/продаваемой Валюты, рассчитанной исходя из Курса Банка данной Конверсионной сделка.

Конверсионные сделки в сервисе «Онлайн конверсия» совершаются только для валютных пар и на суммы, для которых доступен Курс Банка. В случае, если совершение Конверсионной сделки невозможно, на экранной форме сервиса «Онлайн конверсия» Клиент получает уведомление «Курс не задан. Обратитесь в

[4] В сервисе «Онлайн конверсия» доступны только расчетные счета Клиента, открытые в Банке

Банк».

19.3. В случае согласия Клиента с условиями Конверсионной сделки, в сервисе «Онлайн конверсия» формируется Поручение на конверсию валюты, которое в целях исполнения сделки Уполномоченное лицо Клиента подписывает УНЭП/ Средством ЭП PayControl.

19.4. Направление Клиентом Поручения на конверсию валюты признается безусловным и безотзывным согласием Клиента совершить Конверсионную операцию на условиях, указанных в Поручении на конверсию валюты.

19.5. Клиент понимает и принимает на себя риск, связанный с колебаниями курсов Валют, в результате которого Клиент может заключить Конверсионную сделку по невыгодному для себя курсу.

19.6. Банк принимает к исполнению и исполняет Поручение на конверсию валюты, полученное в сервисе «Онлайн конверсия», в текущий рабочий день Банка в период с 10 часов 00 минут до 19 часов 00 минут по Московскому времени. В иное время сервис «Онлайн-конверсия» для Клиента недоступен.

19.7. Банк в режиме реального времени при получении Поручения на конверсию валюты производит процедуры приема к исполнению в соответствии с п. 13.15 настоящих Правил, и при положительном результате контроля и наличии технической возможности исполнить Конверсионную сделку по Курсу Банка, исполняет Конверсионную сделку на условиях расчетов «сегодня» (today).

В момент исполнения Поручения Банком Поручению на конверсию валюты в сервисе «Онлайн конверсия» присваивается статус «Исполнен».

19.8. При отрицательном результате контроля процедур приема к исполнению в соответствии с п. 13.15. настоящих Правил, Банк не исполняет Конверсионную сделку. В Поручении на конверсию валюты в сервисе «Онлайн конверсия» отражается информация о причине неисполнения Конверсионной сделки.

19.9. Сервис «Онлайн конверсия» Системы «Клиент- Банк» предоставляется, при наличии технической возможности

Приложение №1
к Правилам обмена электронными документами
по системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

Заявление
о присоединении к Правилам обмена
электронными документами по системе дистанционного банковского обслуживания и подключении Системы «Клиент-Банк» в ЭКСИ-Банк (АО)

Наименование Клиента _____
_____
ИНН _____
ОГРН _____
Адрес местонахождения: _____
Контактная информация:
телефон/факс _____
адрес электронной почты _____
комментарии _____

- ❑ Первичный доступ
- ❑ Изменение реквизитов доступа

Настоящим Заявлением_____
_____
(наименование клиента)

1. Заявляю о присоединении к действующей редакции Правил обмена электронными документами по Системе «Клиент-Банк» в ЭКСИ-Банк (АО) (далее – Правила) в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации, и подтверждаем, что все положения Правил известны и разъяснены в полном объеме.
2. Прошу предоставить доступ к Системе обмена электронными документами «Клиент-Банк» ЭКСИ-Банк (АО) и обеспечить возможность ее использования в соответствии с условиями Правил.
3. Пароль для первичного входа в Систему «Клиент-Банк» ЭКСИ-Банк (АО) прошу направить на Зарегистрированный номер телефона: + 7 (_ _ _) - _ _ _ - _ _ - _ _.
4. Выражаю намерение использовать Простую электронную подпись (ПЭП) для подписания Акта признания ключа проверки Электронной подписи и согласен считать ПЭП равнозначной моей собственноручной подписи и собственноручной подписи Пользователя Системы, указанного в п.5 настоящего Заявления.
5. **Право подписания Акта признания ключа проверки Электронной подписи ПЭП в Системе «Клиент-Банк» предоставлено Руководителю / индивидуальному предпринимателю / физическому лицу, занимающемуся частной практикой с использованием принадлежащего ему номера мобильного телефона (Зарегистрированный номер)**

Фамилия, Имя, Отчество Уполномоченного лица	
Документ, удостоверяющий личность	Серия_____ Номер_____
Мобильный телефон	+ 7 (_ _ _) - _ _ _ - _ _ - _ _
Emeil	

6. Выражаю намерение использовать Средство электронной подписи PayControl для подписания электронных документов и согласен считать Средство электронной подписи PayControl равнозначной моей собственноручной подписи и собственноручной подписи каждого Пользователя Системы, указанного в п.7 настоящего Заявления.
7. **Право доступа в Систему «Клиент-Банк», создания и подписания Средством электронной подписи PayControl правоустанавливающих, электронных расчетных документов и электронных сообщений в опции Документы свободного формата, просмотра информации , а также право обмена сообщениями с Банком[5] предоставлено следующим Пользователям Системы с использованием принадлежащего каждому из них номера мобильного телефона[6]**

Сведения о владельцах ключей ЭП и их права:

[5] по вопросам, не связанным с заключением / расторжением / изменением условий банковских договоров, подключением / отключением услуг.
[6] для предоставления права доступа в Систему «Клиент-Банк» большему количеству Пользователей необходимо оформить настоящее Заявление повторно.

№ п/п	Фамилия, имя, отчество (полностью)	Должность и Электронная почта	Право подписи	Право просмотра
1 сочетание подписей			❑	❑
			❑	❑
2 сочетание подписей			❑	❑
			❑	❑

_____ _____ /_____/
(должность Руководителя) *(подпись)* *(фамилия, имя, отчество полностью)*

«____» _____20 ___ г.

М.П. (при наличии)

Заполняется Банком
Заявление получено в ____ часов _____ минут «____» _____ _____ г.

Работник Банка: _____ _____
подпись *Фамилия И.О.*

Заявка на сертификат
№_____
Генеральному
директору ООО
«Айтиком»
Е.Н. Мельниковой

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки
электронной подписи

1. **Я, _____(ФИО)**, паспорт серии ____ № _____
выдан_____

, прошу зарегистрировать и сформировать ключ электронной подписи, записать сформированный ключ электронной подписи на ключевой носитель и изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «Айтиком» в соответствии с указанными в настоящем заявлении данными:

	Ключ №1
Наименование организации (organizationName)	
Общее имя (CommonName)	
Улица, дом (streetAddress)	
Город (localityName)	
Область, край (stateOrProvinceName)	
Страна (countryName)	
Электронная почта (E-Mail (E))	
ИНН (INN)	
ОГРН организации (OGRN)	
ОГРНИП организации (OGRNIP)	
Неструктурированное имя (unstructuredName)	
Ограничения использования квалифицированного сертификата	
Информация о владельце квалифицированного сертификата (по требованию заявителя)	
Подразделение организации (organizationUnitName)	
Должность (title)	
Фамилия (surname)	
Имя и отчество (givenName)	
Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)	

Ключ №1 выпускается для_____
Ключевая фраза, использующаяся для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов: нет

2. Я, **ФИО**, в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту УЦ

ООО «Айтиком» по выпуску квалифицированных сертификатов ключей проверки электронной подписи от 18.03.2019 года, условия которого определены ООО «Айтиком» и опубликованы на сайте Удостоверяющего центра ООО «Айтиком» по адресу http://uc-itcom.ru/files/reglamentITCOM.pdf.
Руководство по обеспечению безопасности использования ЭП и средств ЭП получил в печатном виде и ознакомился.

С регламентом Удостоверяющего центра по выпуску квалифицированных сертификатов ключа проверки электронной подписи и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.

3. Я, **ФИО** паспорт серии _____ № _____, выдан _____(дата выдачи и кем выдан паспорт)
, код подразделения _____, дата рождения _____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», с целью получения квалифицированного сертификата ключа проверки электронной подписи и осуществления действий, предусмотренных регламентом Удостоверяющего центра ООО «АйтиКом», даю согласие ООО «АйтиКом» (далее – Удостоверяющий центр), расположенному по адресу: 127083, г. Москва, ул. Верхняя Масловка, д.20, стр.1, пом.3, ком.10, а также ООО «ИТК», расположенному по адресу: 350051, Краснодарский край, Краснодар, ул. Дальняя, д. 39/3, пом. 140 (лицо, осуществляющее обработку персональных данных по поручению ООО «АйтиКом») на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных: фамилия, имя, отчество, пол, дата и место рождения; адрес места жительства, реквизиты основного документа, удостоверяющего личность (серия, номер, дата выдачи, орган, осуществившей выдачу, код подразделения); место работы, должность; фотоизображение, контактная информация (электронная почта, телефон), идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), фотокопии основного документа, удостоверяющего личность, страхового свидетельства обязательного пенсионного страхования (СНИЛС), собственноручная подпись, иные персональные данные, необходимые для выпуска квалифицированного сертификата ключа проверки электронной подписи, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу) обезличивание, блокирование, уничтожение, а также осуществление любых иных действий, предусмотренных нормативными правовыми актами в области электронной подписи. Я соглашаюсь с включением моих персональных данных в общедоступные источники, которыми являются сертификат ключа проверки электронной подписи, реестр сертификатов ключей проверки электронной подписи; а также на передачу моих персональных данных в единую систему идентификации и аутентификации в объеме, необходимом для регистрации в системе идентификации и аутентификации в соответствии с требованиями действующего законодательства. Подтверждаю, что обладаю правами доступа, достаточными для чтения и отправки электронных сообщений с помощью ящика электронной почты rasul_shalabaev@mail.ru и даю согласие на использование этого ящика для информационного взаимодействия с ООО «Айтиком». Настоящее согласие на обработку персональных данных действует с момента подписания бессрочно и может быть отозвано мной в порядке, установленном Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 года №152-ФЗ, в любое время на основании моего письменного заявления в произвольной форме.
Я, **ФИО**, подтверждаю достоверность данных, указанных в настоящем Заявлении.
Подписи:
Пользователь Удостоверяющего центра_____ФИО __.__.____г.

Приложение №3
к Правилам обмена электронными документами по системе
дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

В ЭКСИ-Банк (АО)

Заявление
на прекращение права доступа в Систему «Клиент-Банк» сертификата ключа подписи Пользователя Удостоверяющего Центра

_____
(наименование Клиента)

в лице _____
(должность руководителя)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит прекратить право доступа в Систему «Клиент-Банк» с «___» _____ 20___ г. сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего Центра, содержащий следующие идентификационные данные:

Серийный номер сертификата (SN)	
Фамилия, Имя, Отчество (CN)	
Наименование клиента (O)	

в связи с _____
*(причина отзыва сертификата *)*

_____ _____ / _____ /
Должность руководителя Подпись Ф.И.О

М.П. (при наличии)

* – прекращение работы Пользователя Удостоверяющего Центра, компрометация закрытого ключа подписи, утеря пин-кода, и т.д.;

Приложение №4
к Правилам обмена электронными документами по системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

В ЭКСИ-Банк (АО)

ЗАЯВКА
на установление/снятие ограничения на подключение к электронной системе «Клиент-Банк» по сетевым адресам

Настоящей Заявкой
_____
_____
(наименование клиента, ИНН)
в лице _____
действующего на основании _____ в целях увеличения безопасности работы со своими средствами в банке, выражает намерение установить ограничение на доступ своей учетной записи в Систему «Клиент-Банк» для всех подключений, кроме производимые из сетей указанных ниже:

❑ установить ограничение*

❑ Использовать фильтрацию по внутреннему IP адресу	*Указывается список IP адресов, либо диапазон IP адресов, либо маска подсети*
❑ Использовать фильтрацию по MAC адресу	*Указывается список MAC адресов устройств*
❑ Использовать фильтрацию по внешнему IP адресу	*Указывается список IP адресов, либо диапазон IP адресов, либо маска подсети*

❑ снять ограничение*

❑ Использовать фильтрацию по внутреннему IP адресу	*Указывается список IP адресов, либо диапазон IP адресов, либо маска подсети*
❑ Использовать фильтрацию по MAC адресу	*Указывается список MAC адресов устройств*
❑ Использовать фильтрацию по внешнему IP адресу	*Указывается список IP адресов, либо диапазон IP адресов, либо маска подсети*

* Возможно одновременное указание нескольких полей.

Руководитель (должность)	Ф.И.О.	Подпись
_____	_____	_____

М.П. (при наличии)

«____» _____ 20 __ г.

Приложение №5
к Правилам обмена электронными документами по системе
дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

В ЭКСИ-Банк (АО)

ЗАЯВКА
на подключение к электронной системе «Клиент-Банк» со встроенными сертифицированными средствами криптографической защиты информации

Настоящей Заявкой
_____
_____
(полное наименование клиента)
Сокращенное наименование Клиента: _____
Полное наименование на иностранном языке: _____
(при наличии)
Сокращенное наименование на иностранном языке: _____
(при наличии)

в лице _____
действующего на основании _____выражает намерение использовать электронную систему «Клиент-Банк» (далее по тексту – Система) для управления своим счетом (счетами).

Оборудование и помещения, предназначенные для установки программного обеспечения Системы, удовлетворяют техническим требованиям, изложенным в п.3.3.4. Правил обмена электронными документами по системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО).

Оплату стоимости подключения системы «Клиент-Банк», своевременную оплату абонентской платы гарантируем.

Подтверждаем получение USB-токенов, перечисленных ниже.

Сведения о владельцах ключей ЭП (и шифрования) и их права:

№ п/п	Фамилия, имя, отчество (полностью)	Должность и Электронная почта	Право подписи	Право просмотра
1 сочетание подписей			❑	❑
			❑	❑
2 сочетание подписей			❑	❑
			❑	❑

Ответственные лица (Ф.И.О., должность, телефон, факс, адрес электронной почты):

по техническим вопросам:
_____
_____

по вопросам обмена информацией (не менее двух человек):

1)_____
_____

2)_____
_____

Юридический адрес Клиента на русском языке:
_____

Адрес Клиента на иностранном языке:
_____
(при наличии)

ИНН _____ ОКВЭД _____ ОКПО _____КПП_____

№ счета(ов) в ЭКСИ-Банк (АО):
_____

Руководитель (должность)

	Ф.И.О.	Подпись
_____	_____	_____

М.П. (при наличии)

«____» _____ 20 __ г.

Отметка Банка:

Настоящим подтверждаю, что сведения, указанные в ЗАЯВКЕ проверены «____» _____ 20__г.

_____	_____ /_____/	
Должность уполномоченного представителя Банка		Подпись
Ф.И.О.		

Приложение №6
к Правилам обмена электронными документами по системе
дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

Заявление
о расторжении Договора об обслуживании с использованием системы дистанционного банковского обслуживания

Наименование Клиента _____
ИНН _____
_____

Контактная информация:
телефон _____
адрес электронной почты _____
комментарии _____

Настоящим заявляем о расторжении с «_____» _____ 20____г. Договора об обслуживании с использованием системы дистанционного банковского обслуживания, заключенного путем присоединения к Правилам обмена электронными документами по Системе дистанционного банковского обслуживания в ЭКСИ-Банк (АО) на основании Заявления от «___» _____20__г.

_____
(должность Руководителя)

_____/_____ /
(подпись) *(фамилия, имя, отчество полностью)*

«____» _____20 ___ г.

М.П.(при наличии)

Заполняется Банком

Заявление получено в ____ часов _____ минут «____» _____ _____ г.

Работник Банка: _____ _____
подпись *Фамилия И.О.*

Приложение №7
к Правилам обмена электронными документами по системе
дистанционного банковского обслуживания в ЭКСИ-Банк (АО)

Заявка на отключение использования простой электронной подписи/ Средством электронной подписи PayControl для удостоверения документов в Электронной системе «Клиент-Банк»

Настоящей Заявкой
_____
(наименование клиента/фамилия, имя, отчество индивидуального предпринимателя/физического лица, занимающегося частной практикой)
ИНН _____
выражает намерение отказаться от использования:

- ❑ Простой электронной подписи (ПЭП) для подписания Акта признания ключа проверки ЭП
- ❑ Средством электронной подписи PayControl для подписания электронных документов

Руководитель (должность)	Ф.И.О.	Подпись
_____	_____	_____

«____» _____ 20 __ г.

Отметка Банка:

Настоящим подтверждаю, что сведения, указанные в ЗАЯВКЕ проверены «___» _____ _____г.

_____ _____/_____
Должность уполномоченного представителя Банка Подпись Ф.И.О.