

ПРАВИЛА ИСПОЛЬЗОВАНИЯ АНАЛОГОВ СОБСТВЕННОРУЧНОЙ ПОДПИСИ ПРИ УДАЛЕННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ В ПАО "БЫСТРОБАНК"

(редакция утверждена Президентом ПАО "БыстроБанк" 23.03.2020 г.)

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 1.1 Термины и сокращения, применяемые в настоящем тексте, используются в следующем значении:
- 1.1.1 ПРАВИЛА АСП — настоящие Правила, являющиеся составной частью СОГЛАШЕНИЯ и устанавливающие порядок и случаи использования аналогов собственноручной подписи при удаленном банковском обслуживании КЛИЕНТА. ПРАВИЛА размещаются на САЙТЕ БАНКА.
- 1.1.2 ПРАВИЛА УБО — Правила удаленного банковского обслуживания физических лиц в ПАО "БыстроБанк", Правила удаленного банковского обслуживания юридических лиц и индивидуальных предпринимателей в ПАО "БыстроБанк". В ПРАВИЛАХ АСП применяются термины, значение которых определено в ПРАВИЛАХ УБО: КЛИЕНТ, СОГЛАШЕНИЕ, ЗАЯВЛЕНИЕ, УБО, СИСТЕМА, одноразовый пароль, биометрическая верификация.
- 1.1.3 БАНК — Публичное акционерное общество "БыстроБанк", зарегистрированное и находящееся по адресу: 426008, Удмуртская Республика, г. Ижевск, ул. Пушкинская, 268.
- 1.1.4 Уполномоченное лицо КЛИЕНТА (УЛ) — физическое лицо, которое вправе использовать АСП в соответствии с ПРАВИЛАМИ АСП на основании предоставленных ему КЛИЕНТОМ согласно ПРАВИЛАМ УБО полномочий.
- 1.1.5 Заявление о регистрации в системе — заявление физического лица по форме БАНКА, устанавливающее принадлежность заявителю указанных в нем АСП для использования в СИСТЕМЕ.
- 1.1.6 КАНАЛЫ СВЯЗИ — используемые в СИСТЕМЕ сети связи общего пользования, устройства и технологии обмена информацией в электронном виде:
- 1.1.6.1 Интернет — сеть "Интернет".
- 1.1.6.2 Устройства самообслуживания — банкоматы БАНКА.
- 1.1.6.3 Телефонная связь — соединение, устанавливаемое посредством обращения на номера телефонов БАНКА 8 (800) 333-22-65 или 8 (3412) 90-80-90.
- 1.1.7 Электронный документ — документированная информация в электронной форме, возможность создания и(или) передачи которой предусмотрена СИСТЕМОЙ.
- 1.1.8 Аналог собственноручной подписи (АСП) — информация, присоединенная к электронному документу КЛИЕНТА и(или) иным образом связанная с ним, позволяющая удостоверить факт подписания (подтверждения) КЛИЕНТОМ/УЛ электронного документа, а также удостоверяющая подлинность такого электронного документа, включая все его обязательные реквизиты. В качестве АСП используется электронная подпись (ЭП) в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи", ПРАВИЛАМИ УБО и ПРАВИЛАМИ АСП.
- 1.1.8.1 Усиленная ЭП — информация в электронной форме, полученная с использованием средств ЭП в результате криптографического преобразования информации с использованием ключа ЭП, которая присоединена к файлу подписываемого электронного документа (или иным образом связана с ним), и используется для определения лица, подписавшего электронный документ, и обнаружения факта внесения изменений в электронный документ после его подписания. В рамках настоящих правил используется усиленная неквалифицированная электронная подпись.
- 1.1.8.2 Простая ЭП — данные аутентификации, подтверждающие факт формирования и подписания электронного документа определенным лицом, полученные при использовании КАНАЛА СВЯЗИ Интернет или КАНАЛА СВЯЗИ устройства самообслуживания.
- 1.1.9 Данные аутентификации — информация об удачной процедуре аутентификации, в том числе сведения об используемом идентификаторе (внутренний идентификатор / внешний идентификатор / карта / сертификат).
- 1.1.10 Идентификация — процедура определения личности КЛИЕНТА/УЛ при его обращении в БАНК с использованием СИСТЕМЫ. Для настоящей процедуры в соответствии с ПРАВИЛАМИ АСП используются следующие идентификаторы:
- 1.1.10.1 Внутренний идентификатор — уникальная последовательность символов, создаваемая КЛИЕНТОМ/УЛ самостоятельно на САЙТЕ БАНКА и(или) с помощью БАНКА, и используемая для идентификации по КАНАЛУ СВЯЗИ Интернет.
- 1.1.10.2 Внешний идентификатор — уникальная последовательность символов, создаваемая КЛИЕНТОМ/УЛ самостоятельно на сайте в сети "Интернет", предоставляющем услуги федеративной аутентификации, поддерживаемой СИСТЕМОЙ, и используемая для идентификации по КАНАЛУ СВЯЗИ Интернет.
- 1.1.10.3 Сертификат ключа проверки электронной подписи (сертификат) — электронный документ, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата, а также используемый для идентификации по КАНАЛУ СВЯЗИ

Интернет.

1.1.10.4 Карта — основная карта в соответствии с [Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк"](#), используемая для идентификации по КАНАЛУ СВЯЗИ устройства самообслуживания.

1.1.10.5 Доверенный контакт — номер телефона сотовой связи (доверенный телефон) и/или адрес электронной почты (доверенная почта) физического лица (КЛИЕНТА/УЛ), указанный им в заявлении о регистрации в СИСТЕМЕ или посредством соответствующей процедуры в СИСТЕМЕ с использованием карты/реквизитов карты, держателем которой является такое физическое лицо в соответствии с [Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк"](#).

1.1.11 Аутентификация — процедура удостоверения правомочности обращения КЛИЕНТА/УЛ в БАНК с использованием СИСТЕМЫ, основанная на владении КЛИЕНТОМ/УЛ различного рода конфиденциальной информацией в соответствии с ПРАВИЛАМИ АСП:

1.1.11.1 Ключ ЭП — уникальная конфиденциальная последовательность символов, предназначенная для создания усиленной ЭП, и(или) используемая КЛИЕНТОМ/УЛ совместно с сертификатом для прохождения процедуры аутентификации.

1.1.11.2 Код доступа — конфиденциальная информация, используемая КЛИЕНТОМ/УЛ совместно с внутренним или внешним идентификатором для прохождения процедуры аутентификации.

1.1.11.3 Персональный идентификационный номер (ПИН-код) — конфиденциальная информация в соответствии с Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк", используемая КЛИЕНТОМ совместно с картой для прохождения процедуры аутентификации.

1.1.11.4 Персональная информация — известная БАНКУ различного рода информация о КЛИЕНТЕ/УЛ, используемая КЛИЕНТОМ/УЛ для прохождения процедуры аутентификации в СИСТЕМЕ по КАНАЛУ СВЯЗИ телефонная связь.

1.1.12 Федеративная аутентификация — аутентификация, проводимая БАНКОМ с привлечением третьей стороны с использованием созданного в информационной системе такой стороны внешнего идентификатора и различного рода конфиденциальной информации, предназначенной для проведения третьей стороной такой аутентификации (кода доступа, ключа ЭП совместно с сертификатом или иной информации).

1.1.13 Авторизация в ЕСИА — процедура авторизации физического лица с использованием федеративной аутентификации в единой системе идентификации и аутентификации (ЕСИА) при использовании усиленной квалифицированной электронной подписи или простой электронной подписи в соответствии с п. 1.12 ст. 7 Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

1.1.14 Реквизиты карты — наносимая на карту информация при ее эмитировании. В качестве такой информации могут использоваться, но не ограничиваясь: уникальный 16-значный номер карты, CVV2/CVC2-код.

1.1.15 ОТП-ключ (One-time-Password-ключ) — разделяемый между КЛИЕНТОМ/УЛ и БАНКОМ секрет, предназначенный для генерации одноразовых паролей с использованием специальных алгоритмов и устройств (программного обеспечения), сведения о котором указаны КЛИЕНТОМ/УЛ в заявлении о регистрации в СИСТЕМЕ или посредством соответствующей процедуры в СИСТЕМЕ с использованием карты/реквизитов карты, держателем которой является такое физическое лицо в соответствии с [Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк"](#).

1.1.16 Фотоизображение лица — фотографическое изображение физического лица, используемое для его биометрической верификации в СИСТЕМЕ в соответствии с ГОСТ ИСО/МЭК 19794-5-2013, сведения о котором указаны КЛИЕНТОМ/УЛ в заявлении о регистрации в СИСТЕМЕ или посредством соответствующей процедуры в СИСТЕМЕ с использованием карты/реквизитов карты, держателем которой является такое физическое лицо в соответствии с [Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк"](#).

1.1.17 САЙТ БАНКА — сайт в сети "Интернет", доступный по принадлежащему БАНКУ доменному имени www.bystrobank.ru.

2 ОБЩИЕ УСЛОВИЯ

2.1 Присоединение КЛИЕНТА к ПРАВИЛАМ АСП осуществляется при заключении между КЛИЕНТОМ и БАНКОМ (совместно именуемые — Стороны) СОГЛАШЕНИЯ в порядке, установленном ПРАВИЛАМИ УБО.

2.2 Использование Сторонами АСП в рамках получения (предоставления) услуг УБО осуществляется в соответствии с законодательством, нормативными документами Банка России и ПРАВИЛАМИ АСП.

2.3 Стороны договорились об использовании предусмотренных ПРАВИЛАМИ АСП аналогов собственноручной подписи в СИСТЕМЕ для совершения любых банковских операций в соответствии с законодательством; заключения и исполнения любых гражданско-правовых сделок с БАНКОМ; обмена

с БАНКОМ любой информацией; подписания расчетных и иных документов в отношении любых счетов КЛИЕНТА, в том числе и вновь открываемых; достижения договоренности с БАНКОМ об использовании АСП; совершения иных юридически значимых действий, направленных на исполнение обязательств, установление, изменение или прекращение правоотношений с БАНКОМ. Возможность совершения КЛИЕНТОМ конкретных операций в СИСТЕМЕ определяется ПРАВИЛАМИ УБО.

2.4 Стороны признают СИСТЕМУ достаточной для выполнения работ по созданию и проверке электронной подписи, идентификации, аутентификации, подтверждения авторства и подлинности электронных документов, а также разбора спорных ситуаций по ним.

2.5 КЛИЕНТ/УЛ подписывает электронные документы в СИСТЕМЕ с использованием АСП, прошедших процедуру регистрации в БАНКЕ в соответствии с разделом 3 ПРАВИЛ АСП.

2.6 Все передаваемые БАНКОМ электронные документы КЛИЕНТУ в СИСТЕМЕ подписываются аналогом собственноручной подписи уполномоченного лица БАНКА (обеспечивается использованием ключа ЭП и соответствующего ему сертификата БАНКА, используемых для установления защищенного соединения с СИСТЕМОЙ). БАНК обязуется соблюдать конфиденциальность указанного ключа ЭП БАНКА и не использовать его в случае нарушения условий его конфиденциальности.

2.7 Электронные документы, требующие подписи обеих Сторон, подписываются КЛИЕНТОМ в соответствии с разделом 3 ПРАВИЛ АСП, а БАНКОМ согласно п. 2.6 ПРАВИЛ АСП.

2.8 Стороны признают юридическую силу электронных документов, подписанных в СИСТЕМЕ аналогами собственноручных подписей Сторон (уполномоченных лиц Сторон) в соответствии с ПРАВИЛАМИ АСП, равнозначной юридической силе документов на бумажном носителе, в установленном порядке подписанных и заверенных оттиском печати (если наличие печати предусмотрено законодательством или соглашением Сторон).

2.9 БАНК в режиме реального времени фиксирует в электронных журналах СИСТЕМЫ результаты идентификации и аутентификации, дату и время совершения операций, в том числе с электронными документами. Стороны признают указанные электронные журналы в качестве доказательств соответствующих событий в СИСТЕМЕ, в том числе в целях проверки электронной подписи. В качестве единой шкалы времени Стороны признают всемирное координированное время (UTC), а контрольным временем — время системных часов аппаратных средств БАНКА (UTC+4).

2.10 В случае определения КЛИЕНТОМ уполномоченного лица (УЛ), которое вправе от имени КЛИЕНТА совершать действия в СИСТЕМЕ согласно предоставленным ему полномочиям, такое лицо совершает все необходимые действия по регистрации АСП, использует АСП и выполняет иные обязанности УЛ в соответствии с ПРАВИЛАМИ АСП. Обязанность ознакомления УЛ с условиями ПРАВИЛ АСП лежит на КЛИЕНТЕ.

3 ПОРЯДОК РЕГИСТРАЦИИ, ИСПОЛЬЗОВАНИЯ И ПРОВЕРКИ АСП

3.1 **Регистрация АСП** осуществляется следующими способами:

3.1.1 Путем оформления на бумажном носителе и подписания в БАНКЕ КЛИЕНТОМ/УЛ заявления о регистрации в системе с указанием сведений о заявителе, необходимой информации о регистрируемых АСП и иных реквизитах заявителя в соответствии с ПРАВИЛАМИ АСП.

3.1.2 С учетом возможностей технической реализации СИСТЕМЫ, в случаях, установленных разделом 3 ПРАВИЛ АСП, заявление о регистрации в системе может быть сформировано КЛИЕНТОМ/УЛ в СИСТЕМЕ и подписано АСП.

3.1.3 С учетом возможностей технической реализации СИСТЕМЫ, в случаях, установленных разделом 3 ПРАВИЛ АСП, заявление о регистрации в системе может быть подано КЛИЕНТОМ в электронном виде при регистрации в СИСТЕМЕ с использованием карты / реквизитов карты / авторизации в ЕСИА одновременно с подачей в электронном виде ЗАЯВЛЕНИЯ, если ПРАВИЛАМИ УБО для КЛИЕНТА предусмотрена такая возможность.

3.2 При регистрации АСП в соответствии с п.3.1 ПРАВИЛ АСП КЛИЕНТ/УЛ подтверждает, что владеет информацией, необходимой для использования соответствующих АСП в СИСТЕМЕ (в зависимости от вида АСП — ключ ЭП, код доступа, ПИН-код), и ее конфиденциальность не нарушена.

3.3 **Для регистрации в качестве АСП усиленной ЭП и простой ЭП с предъявлением сертификата КЛИЕНТ/УЛ:**

3.3.1 Самостоятельно приобретает (производит установку) средств ЭП и использует их в соответствии с законодательством, ПРАВИЛАМИ АСП и эксплуатационной документацией на средства ЭП.

3.3.2 Самостоятельно изготавливает ключ ЭП в условиях, обеспечивающих невозможность нарушения конфиденциальности такого ключа, и получает сертификат согласно порядку, установленному соответствующим удостоверяющим центром. В качестве удостоверяющих центров могут выступать удостоверяющий центр БАНКА или удостоверяющий центр ООО "КРИПТО-ПРО" при заключении СОГЛАШЕНИЯ с условиями присоединения КЛИЕНТА к [Регламенту предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО"](#).

3.3.3 Предоставляет в БАНК заявление о регистрации в системе в соответствии с п. 3.1.1 / 3.1.2 ПРАВИЛ АСП с указанием информации о сертификате:

3.3.3.1 дата начала и окончания срока действия сертификата;

3.3.3.2 информация, позволяющая сопоставить КЛИЕНТА/УЛ и владельца сертификата;

3.3.3.3 ключ проверки ЭП;

3.3.3.4 стандарты, требованиям которых соответствуют ключ ЭП и ключ проверки ЭП;

3.3.3.5 наименование удостоверяющего центра, выдавшего сертификат;

3.3.3.6 отпечаток сертификата.

3.4 Аналоги собственноручной подписи, зарегистрированные в соответствии с действующим между Сторонами на момент такой регистрации соглашением об условиях удаленного банковского обслуживания, признаются усиленными ЭП и простыми ЭП с предъявлением сертификата, зарегистрированными в качестве АСП.

3.4 Для регистрации в качестве АСП простой ЭП с предъявлением внутреннего идентификатора КЛИЕНТ/УЛ:

3.4.1 Самостоятельно создает уникальный внутренний идентификатор посредством САЙТА БАНКА в соответствии с размещенными на нем инструкциями.

3.4.2 Самостоятельно формирует код доступа для внутреннего идентификатора в условиях, обеспечивающих невозможность нарушения его конфиденциальности.

3.4.3 Предоставляет в БАНК заявление о регистрации в системе в соответствии с п. 3.1.1 / 3.1.2 / 3.1.3 ПРАВИЛ АСП с указанием уникального внутреннего идентификатора, простая ЭП с предъявлением которого регистрируется в качестве АСП.

3.5 Для регистрации в качестве АСП простой ЭП с предъявлением внешнего идентификатора КЛИЕНТ/УЛ:

3.5.1 Самостоятельно создает уникальный идентификатор на сайте в сети "Интернет", предоставляющем услуги федеративной аутентификации (за исключением ЕСИА), поддерживаемой СИСТЕМОЙ, в соответствии с правилами такого сайта. Возможность регистрации в качестве АСП простой ЭП с предъявлением внешнего идентификатора определяется БАНКОМ.

3.5.2 Самостоятельно формирует код доступа для внешнего идентификатора или иную конфиденциальную информацию, предназначенную для проведения федеративной аутентификации, в условиях, обеспечивающих невозможность нарушения конфиденциальности такой информации.

3.5.3 Предоставляет в БАНК заявление о регистрации в системе в соответствии с п. 3.1.1 / 3.1.2 / 3.1.3 ПРАВИЛ АСП с указанием уникального внешнего идентификатора, простая ЭП с предъявлением которого регистрируется в качестве АСП.

3.6 Для регистрации в качестве АСП простой ЭП с предъявлением внешнего идентификатора ЕСИА КЛИЕНТ/УЛ:

3.6.1 Создает подтвержденную учетную запись в ЕСИА в соответствии с [Условиями использования Единой системы идентификации и аутентификации](#), формирует код доступа для идентификатора ЕСИА или иную конфиденциальную информацию, предназначенную для проведения федеративной аутентификации с использованием ЕСИА, в условиях, обеспечивающих невозможность нарушения конфиденциальности такой информации.

3.6.2 Предоставляет в БАНК заявление о регистрации в системе в соответствии с п. 3.1.1 / 3.1.2 / 3.1.3 ПРАВИЛ АСП с указанием уникального идентификатора ЕСИА, простая ЭП с предъявлением которого регистрируется в качестве АСП.

3.7 Для регистрации в качестве АСП простой ЭП с предъявлением карты КЛИЕНТ:

3.7.1 Самостоятельно получает карту в соответствии с Правилами предоставления, обслуживания и использования банковских расчетных карт ПАО "БыстроБанк" и соответствующий ей ПИН-код.

3.7.2 Предоставляет в БАНК заявление о регистрации в системе в соответствии с п. 3.1.3 ПРАВИЛ АСП с указанием карты, простая ЭП с предъявлением которой регистрируется в качестве АСП.

3.8 Порядок использования усиленной ЭП в СИСТЕМЕ.

3.8.1 Использование усиленной ЭП в СИСТЕМЕ для подписания электронных документов возможно только в случае регистрации такой ЭП в качестве АСП. Использование усиленной ЭП в СИСТЕМЕ невозможно в случае блокирования такого АСП в соответствии с ПРАВИЛАМИ АСП.

3.8.2 Усиленная ЭП формируется с использованием ключа ЭП в соответствии с криптографическими стандартами.

3.8.3 Криптографические стандарты формирования усиленной ЭП определяются сертификатом.

3.8.4 Проверка усиленной ЭП производится с использованием сертификата в соответствии с указанными в нем криптографическими стандартами.

3.8.5 Усиленная ЭП признается корректной, если на момент подписания электронного документа АСП, в качестве которого зарегистрирована такая ЭП, не был заблокирован в соответствии с ПРАВИЛАМИ АСП, а также получен положительный результат проверки ЭП электронного документа программно-аппаратными средствами СИСТЕМЫ в соответствии с п. 3.8.4. ПРАВИЛ АСП.

3.8.6 Корректная усиленная ЭП КЛИЕНТА/УЛ подтверждает целостность подписанного электронного документа (неизменность электронного документа с момента его подписания), авторство такого электронного документа (принадлежность электронной подписи документа КЛИЕНТУ/УЛ), а также дату и время его подписания в соответствии с криптографическими стандартами.

3.9 Порядок использования простой ЭП в СИСТЕМЕ.

3.9.1 Использование простой ЭП для подписания электронных документов в СИСТЕМЕ возможно только в случае регистрации такой ЭП в качестве АСП. Использование простой ЭП в СИСТЕМЕ

невозможно в случае блокирования такого АСП в соответствии с ПРАВИЛАМИ АСП.

3.9.2 Использование данных аутентификации для совершения операции в СИСТЕМЕ является подтверждением авторства создаваемого в результате такой операции электронного документа — принадлежности электронной подписи документа КЛИЕНТУ/УЛ.

3.9.3 Неизменность электронного документа, подписанного с использованием простой ЭП, обеспечивается фиксацией его реквизитов (контрольных сумм и(или) иной информации) в электронных журналах СИСТЕМЫ.

3.9.4 Простая ЭП, для которой выполнены все условия пп. 3.9.2 — 3.9.3 ПРАВИЛ АСП, признается корректной и подтверждает авторство и неизменность соответствующего электронного документа, а также дату и время его подписания в соответствии с п.2.9 ПРАВИЛ АСП.

3.10 Порядок блокирования АСП.

3.10.1 БАНК круглосуточно принимает уведомления КЛИЕНТА/УЛ о фактах нарушения конфиденциальности ключей ЭП, кодов доступа, ПИН-кодов. Указанные уведомления принимаются по КАНАЛУ СВЯЗИ телефонная связь.

3.10.2 Для блокирования АСП КЛИЕНТ/УЛ проходит процедуру идентификации и аутентификации в соответствии с п. 3.11 ПРАВИЛ АСП и сообщает, какие АСП КЛИЕНТА/УЛ подлежат блокированию, а также причину их блокирования.

3.10.3 В случае, если полномочия КЛИЕНТА/УЛ по блокированию АСП успешно подтверждены, БАНК осуществляет блокирование соответствующих АСП КЛИЕНТА/УЛ с фиксацией в электронных журналах СИСТЕМЫ даты, времени и иной информации об операции блокирования, в том числе аудиозаписи разговора с КЛИЕНТОМ/УЛ. БАНК, в связи с принятием решения о приостановлении использования КЛИЕНТОМ электронных средств платежа СИСТЕМЫ в результате блокирования АСП, направляет на адрес электронной почты владельца соответствующего АСП уведомление о блокировании АСП с указанием причины.

3.10.4 Для блокирования АСП КЛИЕНТ/УЛ может лично обратиться в БАНК с представлением документов, удостоверяющих личность КЛИЕНТА/УЛ. БАНК в таком случае осуществляет блокирование АСП КЛИЕНТА/УЛ на основании соответствующего письменного заявления КЛИЕНТА/УЛ по форме БАНКА.

3.10.5 Для возобновления использования АСП в СИСТЕМЕ КЛИЕНТ/УЛ осуществляет необходимые действия по восстановлению условий конфиденциальности информации, необходимой для использования АСП, и необходимые мероприятия по повторной регистрации АСП в соответствии с ПРАВИЛАМИ АСП.

3.10.6 Простая ЭП, конфиденциальная информация для использования которой была нарушена и привела к блокированию АСП, может использоваться/регистрироваться повторно в качестве АСП на усмотрение КЛИЕНТА/УЛ (за исключением простой ЭП с предъявлением сертификата) только в случае выполнения им мероприятий по восстановлению условий конфиденциальности соответствующей информации. В случае, если восстановление указанных условий конфиденциальности невозможно, повторное использование/регистрация такой ЭП в качестве АСП не допускается.

3.10.7 Усиленная ЭП, конфиденциальность соответствующего ключа ЭП которой была нарушена и привела к блокированию АСП КЛИЕНТА/УЛ, не может использоваться/регистрироваться повторно в качестве АСП.

3.11 Порядок идентификации и аутентификации по КАНАЛУ СВЯЗИ телефонная связь.

3.11.1 Для прохождения процедуры идентификации по КАНАЛУ СВЯЗИ телефонная связь КЛИЕНТ/УЛ использует доверенный телефон и(или) сообщает запрошенную БАНКОМ информацию для однозначного определения КЛИЕНТА/УЛ. В зависимости от необходимой КЛИЕНТУ/УЛ операции с использованием указанного КАНАЛА СВЯЗИ, КЛИЕНТ/УЛ сообщает персональную информацию, запрашиваемую БАНКОМ для прохождения процедуры аутентификации.

3.11.2 Состав указанных процедур идентификации и аутентификации зависит от операции, которую КЛИЕНТ/УЛ собирается совершить с использованием КАНАЛА СВЯЗИ телефонная связь, и определяется БАНКОМ.

4 ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1 БАНК обязуется:

4.1.1 Размещать ПРАВИЛА АСП на САЙТЕ БАНКА, а в случае внесения изменений в ПРАВИЛА АСП уведомлять КЛИЕНТА об этом посредством САЙТА БАНКА и(или) СИСТЕМЫ в сроки, установленные ПРАВИЛАМИ АСП.

4.1.2 Осуществлять регистрацию АСП КЛИЕНТА/УЛ в соответствии с ПРАВИЛАМИ АСП и внутренними документами БАНКА.

4.1.3 Не предоставлять третьим лицам и не распространять конфиденциальную информацию, связанную с использованием КЛИЕНТОМ/УЛ АСП, за исключением случаев, предусмотренных законодательством и ПРАВИЛАМИ АСП.

4.1.4 Обеспечивать сохранность и целостность электронных журналов СИСТЕМЫ в течение всего срока, установленного законодательством для хранения документов, возможность создания которых

предусмотрена СИСТЕМОЙ.

4.1.5 Обеспечивать сохранность и целостность реестра зарегистрированных АСП и заявлений о регистрации в системе.

4.1.6 Обеспечивать сохранность и целостность реестра выданных и аннулированных удостоверяющим центром БАНКА сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных удостоверяющим центром БАНКА сертификатах, информацию о датах и основаниях прекращения действия или аннулирования сертификатов в соответствии с законодательством.

4.1.7 Принимать уведомления о фактах нарушения конфиденциальности ключей ЭП, кодов доступа, ПИН-кодов и осуществлять все необходимые мероприятия по блокированию АСП в соответствии с ПРАВИЛАМИ АСП.

4.1.8 Аннулировать выданный удостоверяющим центром БАНКА сертификат в случае получения согласно ПРАВИЛАМ АСП уведомления о нарушении конфиденциальности соответствующего ключа ЭП.

4.1.9 Аннулировать выдаваемые удостоверяющим центром БАНКА сертификаты по окончании срока их действия.

4.1.10 Обеспечивать конфиденциальность ключа ЭП БАНКА.

4.1.11 Не использовать ключ ЭП БАНКА при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

4.1.12 В случае нарушения конфиденциальности ключа ЭП БАНКА временно приостановить оказание услуг УБО и осуществить все необходимые мероприятия по смене соответствующих ключей ЭП с уведомлением КЛИЕНТА посредством САЙТА БАНКА в течение не более чем одного рабочего дня со дня обнаружения БАНКОМ факта нарушения конфиденциальности ключа ЭП БАНКА.

4.2 БАНК имеет право:

4.2.1 Приостановить обслуживание КЛИЕНТА при использовании АСП в случае, если КЛИЕНТ не выполняет обязанности по предоставлению запрашиваемой БАНКОМ информации и документов в соответствии с ПРАВИЛАМИ УБО, а также при нарушении КЛИЕНТОМ иных условий СОГЛАШЕНИЯ.

4.2.2 Требовать от КЛИЕНТА/УЛ замены ключей ЭП, кодов доступа, иной конфиденциальной информации, в случае нарушения или подозрения на нарушение конфиденциальности такой информации, а также в случае нарушения КЛИЕНТОМ/УЛ условий безопасного использования АСП, установленных ПРАВИЛАМИ АСП.

4.2.3 Блокировать АСП КЛИЕНТА/УЛ в случае подозрения на нарушение конфиденциальности соответствующих ключей ЭП, кодов доступа, иной конфиденциальной информации, предназначенной для использования АСП, а также в случае нарушения КЛИЕНТОМ условий безопасного использования АСП, установленных ПРАВИЛАМИ АСП. БАНК, в связи с принятым решением о приостановлении использования КЛИЕНТОМ электронных средств платежа СИСТЕМЫ в результате блокирования АСП, направляет на адрес электронной почты владельца соответствующего АСП уведомление о блокировании АСП с указанием причины.

4.2.4 Затребовать от КЛИЕНТА подписанное заявление о регистрации в системе на бумажном носителе (в случае регистрации АСП в соответствии с п. 3.1.2 / 3.1.3 ПРАВИЛ АСП).

4.2.5 Вести запись телефонных переговоров с КЛИЕНТОМ/УЛ при его обращении в БАНК по КАНАЛУ СВЯЗИ телефонная связь в соответствии с ПРАВИЛАМИ АСП.

4.3 КЛИЕНТ обязуется:

4.3.1 Соблюдать ПРАВИЛА АСП.

4.3.2 Выполнять процедуры и предоставлять БАНКУ документы, необходимые для регистрации АСП в соответствии с ПРАВИЛАМИ АСП, а также предоставлять документы, затребованные БАНКОМ в соответствии с ПРАВИЛАМИ УБО и ПРАВИЛАМИ АСП.

4.3.3 Предоставлять БАНКУ достоверную информацию, необходимую для регистрации АСП в соответствии с ПРАВИЛАМИ АСП.

4.3.4 Обеспечивать конфиденциальность ключа ЭП, кодов доступа и иной конфиденциальной информации, предназначенной для использования АСП.

4.3.5 В случае регистрации в качестве АСП усиленной ЭП и простой ЭП с предъявлением сертификата своевременно производить периодическую замену ключей ЭП и соответствующих им сертификатов с учетом даты окончания срока действия последних.

4.3.6 При формировании кодов доступа руководствоваться рекомендациями БАНКА / третьей стороны, предоставляющей услуги федеративной аутентификации, к их сложности и безопасности.

4.3.7 Не использовать ключи ЭП, коды доступа и иную конфиденциальную информацию при наличии оснований полагать, что конфиденциальность такой информации нарушена.

4.3.8 В случае нарушения конфиденциальности ключей ЭП, кодов доступа или иной конфиденциальной информации, предназначенной для использования АСП, осуществить все необходимые мероприятия, направленные на блокирование АСП КЛИЕНТА/УЛ в соответствии с ПРАВИЛАМИ АСП.

4.3.9 Не предоставлять третьим лицам и не распространять конфиденциальную информацию, связанную с использованием АСП, за исключением случаев, предусмотренных законодательством или ПРАВИЛАМИ АСП.

4.3.10 Соблюдать условия безопасного использования АСП, установленные ПРАВИЛАМИ АСП.

4.3.11 Обеспечить выполнение настоящих обязанностей уполномоченным лицами КЛИЕНТА, а также ознакомление таких лиц с ПРАВИЛАМИ АСП.

4.4 КЛИЕНТ имеет право:

4.4.1 Использовать и регистрировать АСП в соответствии с СОГЛАШЕНИЕМ.

4.4.2 Обращаться в БАНК для получения рекомендаций по безопасному использованию АСП.

4.4.3 Требовать от БАНКА предоставления любой редакции ПРАВИЛ АСП на бумажном носителе.

5 ОТВЕТСТВЕННОСТЬ СТОРОН

5.1 За невыполнение или ненадлежащее выполнение условий СОГЛАШЕНИЯ виновная Сторона несет ответственность в соответствии с законодательством.

5.2 БАНК не несет ответственность в случае невозможности использования АСП КЛИЕНТА/УЛ по причине неисправности используемых КЛИЕНТОМ/УЛ программно-аппаратных средств (в том числе персональных компьютеров и устройств), а также в случае несоответствия таких средств предъявляемым БАНКОМ требованиям.

5.3 БАНК не несет ответственность за несанкционированное использование в СИСТЕМЕ АСП КЛИЕНТА/УЛ вследствие нарушения КЛИЕНТОМ/УЛ обязательств по обеспечению конфиденциальности ключей ЭП, кодов доступа или иной конфиденциальной информации, предназначенной для использования АСП, и(или) условий безопасного использования АСП вне зависимости от причин — до момента блокирования КЛИЕНТОМ/УЛ АСП в соответствии с ПРАВИЛАМИ АСП.

5.4 БАНК не несет ответственность в случае реализации угроз несанкционированного доступа к персональному компьютеру (устройству) КЛИЕНТА/УЛ, используемого для работы в СИСТЕМЕ.

5.5 БАНК не несет ответственность за отсутствие у КЛИЕНТА/УЛ доступа к средствам, с использованием которых КЛИЕНТ/УЛ может обратиться в БАНК в целях блокирования АСП в соответствии с ПРАВИЛАМИ АСП.

5.6 КЛИЕНТ несет ответственность перед БАНКОМ за действия (бездействие) УЛ, связанные с использованием АСП, а также за содержание электронных документов, подписанных АСП уполномоченных лиц КЛИЕНТА.

5.7 Блокирование АСП КЛИЕНТА/УЛ или прекращение использования КЛИЕНТОМ/УЛ АСП не прекращает обязательств КЛИЕНТА/УЛ, возникших до момента блокирования или прекращения использования соответствующих АСП.

6 УСЛОВИЯ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ АСП

6.1 В целях предотвращения несанкционированного использования АСП КЛИЕНТ/УЛ обязуется:

6.1.1 Выполнять установленные ПРАВИЛАМИ АСП обязательства по обеспечению конфиденциальности ключей ЭП, кодов доступа и иной конфиденциальной информации, предназначенной для использования АСП, обязательства по формированию такой информации и обязательства, установленные для КЛИЕНТА/УЛ в случае нарушения ее конфиденциальности, в соответствии с ПРАВИЛАМИ АСП.

6.1.2 Использовать ключи ЭП и коды доступа только на личных (доверенных) персональных компьютерах (устройствах).

6.1.3 Обеспечивать защиту персонального компьютера (устройства) КЛИЕНТА/УЛ, используемого для работы в СИСТЕМЕ, от несанкционированного доступа третьих лиц, в том числе удаленного.

6.1.4 Использовать карты и ПИН-коды в соответствии правилами/договорами, на основании которых осуществляется обслуживание карт.

6.2 Использование КЛИЕНТОМ/УЛ АСП с нарушением условий настоящего раздела значительно увеличивает вероятность несанкционированного использования таких АСП.

7 СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ. ПОРЯДОК ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ СОГЛАШЕНИЯ

7.1 Срок действия СОГЛАШЕНИЯ, порядок его изменения и расторжения определяется ПРАВИЛАМИ УБО, а также настоящим разделом в части внесения изменений в ПРАВИЛА АСП.

7.2 БАНК в одностороннем порядке осуществляет внесение изменений в ПРАВИЛА АСП, уведомляя КЛИЕНТА о таких изменениях не позднее 14 календарных дней до введения их в действие любым из следующих способов: путем размещения информации на САЙТЕ БАНКА; путем размещения объявлений на стендах в БАНКЕ и его офисах, осуществляющих обслуживание клиентов; иными способами, позволяющими КЛИЕНТУ получить информацию и установить, что она исходит от БАНКА. Моментом ознакомления КЛИЕНТА с опубликованной информацией считается момент, с которого информация становится доступна для КЛИЕНТА.

7.3 Для получения сведений об изменениях ПРАВИЛ АСП КЛИЕНТ обязуется не реже одного раза в календарный месяц самостоятельно обращаться в БАНК для получения данной информации, а также знакомиться с указанной информацией любыми доступными ему способами.

7.4 Изменения и дополнения, внесенные в ПРАВИЛА АСП, распространяются на всех КЛИЕНТОВ, присоединившихся к ПРАВИЛАМ АСП ранее даты вступления изменений/дополнений в силу, если иное не предусмотрено в самих изменениях или не следует из их смысла.

7.5 Соглашение об использовании аналогов собственноручной подписи КЛИЕНТА (уполномоченных лиц КЛИЕНТА) при удаленном банковском обслуживании КЛИЕНТА, заключенное КЛИЕНТОМ с БАНКОМ на условиях присоединения исключительно к ПРАВИЛАМ АСП, расторгается с 30.12.2016. Использование зарегистрированных на основании такого соглашения АСП с 30.12.2016 продолжается в соответствии с СОГЛАШЕНИЕМ, составной частью которого являются в том числе настоящие правила.

7.6 Данные аутентификации с предъявлением внутреннего идентификатора, зарегистрированные до 30.12.2016 в качестве АСП, признаются простой ЭП с предъявлением внутреннего идентификатора, зарегистрированной в качестве АСП.

8 ПРОЧИЕ УСЛОВИЯ

8.1 Все разногласия, возникшие или могущие возникнуть из СОГЛАШЕНИЯ, подлежат разрешению с соблюдением досудебного претензионного порядка в соответствии с ПРАВИЛАМИ УБО.