СОГЛАШЕНИЕ
ОБ ОБМЕНЕ ДОКУМЕНТАМИ В ЭЛЕКТРОННОМ ВИДЕ (ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ) ПО СИСТЕМЕ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Банк** – «Банк Глобус» (Акционерное общество), адрес: 115184, г. Москва, ул. Бахрушина, д.10, стр.1, ИНН 77250382220, ОГРН 770501001, БИК 044525473, регистрационный номер Банка России 2438.

1.2. **Договор –** заключенные между Банком и Клиентом договоры, за исключением Договоров счета/вклада (например, кредитный договор, договор залога, договор поручительства).

1.3. **Договор счета –** Договор банковского счета физического лица заключенный между Банком и Клиентом.

1.4. **Договор вклада** – Договор банковского вклада, заключенный между Банком и Клиентом.

1.5. **Дополнительное соглашение** – Дополнительное соглашение об электронном документообороте с использованием системы «Клиент-Банк», заключенное между Банком и Клиентом в порядке и на условиях Соглашения:

- к Договору банковского счета физического лица,
- к Договорам банковского вклада, указанным Клиентом в Заявления о подключении услуги Клиент-Банк, а также заключенным после подключения услуги возможность осуществления операций по средствам Системы предусмотрена таким договором банковского вклада.

1.6. **Подпись ответственного лица Банка** – ЭП сотрудника Банка, которому в соответствии с распорядительными документами Банка предоставлены полномочия и возложена ответственность осуществлять от имени Банка соответствующие юридически значимые действия.

1.7. **Проверка авторства Электронных документов** – однозначная проверка подлинности, целостности и авторства Электронных документов.

1.8. **Система** – система дистанционного банковского обслуживания «Клиент-Банк».

1.9. **Соглашение** – настоящее Соглашения об обмене документами в электронном виде (об электронном документообороте) с использованием системы «Клиент-Банк».

1.10. **Логин** – уникальная цифровая последовательность, используемая для идентификации Клиента в Системе

1.11. **Пароль** – буквенно-цифровая с использованием специальных символов последовательность соответствующая Логину

1.12. **Телефон (мобильный телефон)** – мобильное программно–аппаратное устройство Клиента, используемое Клиентом для получения от Банка SMS- сообщений, в том числе SMS-кодов

1.13. **Электронный документ (ЭД)** – составленные с помощью Системы Распоряжение Клиента, Заявки и иные документы, направленные в Банк по Системе.

1.14. **Электронная подпись (ЭП)** – применяемое в Системе средство Проверки авторства Электронных документов.

1.15. **Простая Электронная подпись (ПЭП)** – простая электронная подпись в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ., которая по совокупности Номера телефона и SMS-кода подтверждает формирование Клиентом ЭД и подписания Клиентом ЭД.

1.15.1. **SMS-код** – одноразовый шестизначный секретный код, формируемый Системой без участия человека, и предоставляемый Клиенту на Номер телефона в SMS-сообщении. SMS-код используется для подтверждения совершаемых в Системе действий.

1.15.2. **Номер Телефона** – последовательность цифр, присвоенная Клиенту оператором сотовой связи как пользователю телефонной сети, зная которую Банк может направить Клиенту на Телефон SMS-код, или информацию о событиях в Системе. Клиент может использовать до трех Номеров Телефона одновременно, при этом один из них указывается как «основной». SMS-сообщения приходят на все Номера телефонов, используемые Клиентом,при этом на каждый Номер телефона приходит уникальный SMS-код.

Переводы на счета, открытые в других банках (в том числе счета Клиента), на сумму более Лимита, установленного Приложением № 1 к Соглашению осуществляются только при подписании распоряжения в Системе и ПЭП и усиленной электронной подписью, носителем которой является специального устройства (токена, смарт карты и проч.) Формирование и применение усиленной электронной подписи осуществляется в соответствии с Приложением № 2 к Соглашению.

1.16. Все иные термины и определения применяются в соответствии с Договором счета.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Соглашение определяет порядок и условия заключения Дополнительных соглашений, а также условия предоставления Банком Клиенту услуги по передаче и обмену ЭД посредством Системы и устанавливает в том числе:

- условия и порядок обмена в электронном виде расчетными и иными документами между Банком и Клиентом;
- условия признания ЭД, в том числе ЭД, равнозначными документам на бумажном носителе;
- порядок проверки ЭП.

2.2. Дополнительное соглашение заключается между Банком и Клиентом в порядке присоединения Клиента в соответствии со статьей 428 Гражданского кодекса Российской Федерации к Соглашению полностью путем подачи Заявления о подключении услуги Клиент-Банк.

Дополнительное соглашение заключается с Клиентами, заключившими с Банком Договор счета или при условии одновременного заключения Договора счета и Дополнительного соглашения и при условии оплаты комиссии за подключение Системы в соответствии с Тарифами.

2.3. Дополнительное соглашение считается заключенным на условиях, изложенных в Заявлении о подключении услуги Клиент-Банк, Договоров счета, Договоров вклада и Соглашении с момента акцепта Банком Заявления о подключении услуги Клиент-Банк. Акцепт Банка подтверждается проставлением в специально обозначенных для этого полях Заявления о подключении услуги Клиент-Банк даты, номера Дополнительного соглашения, должности, фамилии и инициалов, а так же подписи уполномоченного сотрудника Банка и оттиска печати Банка.

2.3.1. В случае согласия Банка акцептовать Заявление о присоединении, Банк снимает с Заявления о подключении услуги Клиент-Банк (его первого листа) копию, акцептует оригинал и копию Заявления о подключении услуги Клиент-Банк (его первого листа) и возвращает под подпись на оригинале, акцептованную Банком копию Заявления о подключении услуги Клиент-Банк (его первого листа) Клиенту. Акцептованное Банком Заявление о подключении услуги Клиент-Банк является единственным документов, подтверждающим заключение Дополнительного соглашения.

2.4. Банк принимает решение об акцепте/отказе от акцепта Заявления о подключении услуги Клиент-Банк обычно в день получения его от Клиента. Банк вправе увеличить срок для принятия решения об акцепте/отказе от акцепта Заявления о подключении услуги Клиент-Банк, до пяти рабочих дней по усмотрению Банка без объяснения причин.

2.5. Банк вправе в любое время до акцепта Заявления о подключении услуги Клиент-Банк отказаться от заключения Дополнительного соглашения по иным основаниям без объяснения причин.

2.6. Акцепт Банком Заявления о подключении услуги Клиент-Банк влечет возникновение у Сторон прав и обязанностей, предусмотренных Дополнительным соглашением.

3. ОСНОВНЫЕ УСЛОВИЯ

3.1. Стороны признают, что ЭД, подписанные ЭП, направляемые Сторонами друг другу в соответствии с условиями Соглашения, являются равнозначными документам на бумажном носителе, заверенным собственноручной подписью Клиента или уполномоченного Банком лица.

3.1.1. Стороны признают, что ЭД направляемые Клиентом Банку, подписанные ЭП, являются равнозначными документам на бумажном носителе, заверенным собственноручной подписью Клиента.

3.1.2. Стороны признают, что ЭД направляемые Банком Клиенту, подписанные ЭП, являются равнозначными документам на бумажном носителе, заверенным собственноручной подписью ответственного лица Банка и скрепленным оттиском печати Банка.

3.1.3. Стороны признают, что при обмене вложенными в сообщения документами, каждый документ вложения подписан так же, как и само сообщение. В случае если во вложениях находятся электронные копии документов, то такая электронная копия считается заверенной Клиентом, при условии что такая электронная копия заверена соответствующей ЭП.

3.1.4. Стороны признают, что ЭД направленные друг другу и подписанные ЭП, являются идентичными подобным документам на бумажных носителях и устанавливают аналогичные им права и обязанности Сторон.

3.2. Стороны признают, что включенная в Систему подсистема защиты информации, которая обеспечивает целостность ЭД и аутентификацию их отправителей, при выполнении условий раздела 7 Соглашения, достаточна для обеспечения, а также для подтверждения авторства и контроля целостности (неизменности содержания) ЭД.

3.3. Стороны признают включенные в Систему подсистемы обработки, хранения и передачи информации достаточными для обеспечения надежности, эффективности и безопасности Системы

3.4. Использование ЭД, переданных по средствам Системы, не изменяет установленные законодательством и Договорами счета, вклада прав и обязанностей Сторон, продолжительности операционного дня Банка, содержания Распоряжений правил заполнения их реквизитов и правил контроля приема Распоряжений к исполнению.

3.5. При осуществлении Операций по Счетам Клиентом могут использоваться Распоряжения как переданные посредством Системы, так и на бумажных носителях. В случае поступления в Банк ЭД и аналогичных им Распоряжений на бумажном носителе без отметки Клиента на оборотной стороне Распоряжения о том, что аналогичное Распоряжение направлено ранее по средствам Системы, Банк принимает все поступившие Распоряжения.

4. ПОДКЛЮЧЕНИЕ К СИСТЕМЕ И ПРОЦЕДУРА ФОРМИРОВАНИЯ ЛОГИНА И ПАРОЛЯ

4.1. Банк размещает руководство по использованию Системы на сайте в сети Интернет по адресу: www.bankglobus.ru.

4.2. Для подключения Системы Клиент представляет в Банк подписанное в присутствии сотрудника Банка Заявление о подключении Системы.

4.3. Необходимыми условиями для подключения Клиента к Системе является одновременно следующее:

- наличие у Клиента мобильного телефона, подключенного к сети операторов, поддерживающих стандарты GSM с возможностью приема SMS-сообщений;
- наличие у Клиента компьютера или мобильного телефона с доступом в сеть Интернет.

Для осуществления операций на сумму, превышающую Лимит, установленный Приложением № 1 к Соглашению, наличие компьютера является необходимым условием.

4.4. Клиент самостоятельно регистрируется в Системе и получает при регистрации Логин и Пароль.

4.5. **Возможность пользоваться информационным и платежным сервисами Системы появляется у Клиента спустя 1 сутки после окончания регистрации в Системе.**

4.6. В случае утери Логина и/или Пароля клиент обязан направить в Банк сообщение о Блокировке системы. Восстановление доступа к системе (генерация нового Логина, Пароля), производится в соответствии с разделом 6 Соглашения.

5. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

5.1. Клиент самостоятельно устанавливает соединение с Интернет-сервером Системы и следит за поддержанием сеанса связи во время работы в Системе.

5.2. Идентификация и аутентификация Клиента при вход в Систему осуществляется на основании Логина, Пароля и SMS –кода.

5.2.1. При входе в Систему производится авторизированный запрос Логина и Пароля, при положительном результате проверки которых Клиенту направляется SMS-сообщение содержащие SMS-код и номер сессии,

5.2.2. Каждой попытке входа Клиента в систему присваивается отдельный номер сессии. Пара SMS-код (для входа в Систему) +номер сессии являются уникальными, Полученный SMS-код необходимо ввести в Систему, проверив номер сессии.

5.2.3. По результатам проверки Системой совпадения SMS-кода Клиенту предоставляется доступ к платежному и информационному сервисам Системы.

5.3. Информационный сервис:

- просмотр и детализация выписок по текущим Счетам;
- изменение Пароля;
- направление документов, уведомлений, информационных сообщений (документов свободного формата) в рамках заключенных Договоров счета, вклада и иных Договоров;
- доступ к справочной информации.

5.4. Платежный сервис:

- перевод средств в валюте РФ со Счета, за исключением Счета карты, на счета любых лиц, открытых как в Банке, так и иных кредитных организациях (перевод по реквизитам), в соответствии с ограничениями, указанными в Приложении №1 к Соглашению;
- перевод средств в валюте РФ и иностранной валюте между своими Счетами, за исключением переводов со Счетов карты, в том числе конверсионные операции, в соответствии с ограничениями, указанными в Приложении №1 к Соглашению.

5.5. Обмен электронными документами включает в себя:

- формирование ЭД;
- отправку и доставку ЭД;
- проверку ЭД;
- подтверждение получения ЭД;
- хранение электронных документов (ведение архивов ЭД).

5.6. Каждое действие Клиента направление документов в Банк подтверждается SMS – кодом.

5.6.1. SMS–сообщение, направляемое Банком Клиенту на этапе приема к исполнению ЭД для совершения Операции по Счету помимо SMS–кода также содержит следующую информацию (реквизиты платежа):

- сумму платежа;
- наименование операции;
- номер сессии.

5.6.2. SMS–код, полученный Клиентом на Номер телефона, вводится Клиентом в поле Системы «Одноразовый пароль» только после проверки правильности указания Реквизитов платежа в соответствующем SMS–сообщении. При положительном результате проверки Системой соответствия введенной Клиентом в Систему комбинации цифр SMS–коду, направленному Банком Клиенту на Номер телефона, ЭД поступает в Банк для обработки и последующего исполнения.

5.6.3. Система автоматически отображает сведения о текущем этапе обработки Клиентом и (или) Банком ЭД, посредством присвоения такому ЭД соответствующего статуса. Система присваивает ЭД следующие статусы:

- «новый»: присваивается вновь созданному Клиентом ЭД в Системе, не прошедшему ни одного этапа обработки Клиентом и/или Банком (Документ находится в стадии редактирования Клиентом);
- «доставлен»: присваивается ЭД, успешно прошедшему процедуру проверки документа и процедуру проверки SMS – ключа), в том числе удостоверения права распоряжения денежными средствами. Время присвоения ЭД статуса «доставлен» считается временем поступления ЭД в Банк. Присвоение ЭД статуса «доставлен» не означает принятия Банком обязательства исполнить ЭД, т.к. документ к этому времени еще не прошел все виды банковского контроля;
- «на обработке» присваивается ЭД, доставленному в Банк, по которому Банком проводятся процедуры приема к исполнению в соответствии с действующим законодательством и Договором счета и Договором вклада
- «на исполнении»: присваивается ЭД, исполнение которого не завершено;
- «исполнен»: присваивается исполненному Банком ЭД в результате выполнения Банком операции, совершенной с использованием Системы, по счету Клиента;
- «отвергнут»: присваивается ЭД, не принятому Банком к исполнению:
  - ✓ по причине его несоответствия требованиям, установленным действующим законодательством Российской Федерации или Договором счета/Договором вклада;
  - ✓ по причине отказа в исполнении его в платежной системе.

  Документ со статусом «отвергнут» можно удалить или создать на его основе новый документ. Также клиент может отредактировать отвергнутый документ, вновь подписать его и отправить в Банк

5.6.4. Статус каждого ЭД, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами Банка во время сеансов связи, проводимых Клиентом. Свидетельством того, что ЭД принят Банком для проведения процедуры приема к исполнению в соответствии с законодательством РФ и утвержденным в Банке порядком, является присвоение ему в Системе статуса «доставлен».

5.6.5. Статус «Исполнен» ЭД подтверждает осуществление Банком положительного результата контроля целостности электронного расчетного документа, структурного контроля, контроля значений реквизитов ЭД и контроля достаточности денежных средств на Счетах Клиента, а также иных видов контроля, предусмотренных законодательством и Договором счета/Договором вклада, необходимых для исполнения ЭД, а также списание средств со Счета.

5.6.6. Информация об отрицательном результате приема к исполнению ЭД, доводится до Клиентов путем присвоения ЭД статуса «отвергнут», доступна Клиенту в Системе не позднее следующего рабочего дня после получения Банком ЭД (с учетом установленного Банком режима обслуживания физических лиц), с указанием причины, по которой документ не принят к исполнению.

5.7. Клиент самостоятельно до момента получения информации об исполнении либо об отказе в исполнении ЭД, но не позднее чем в течение 24 часов с момента отправки ЭД в Банк или получения от Банка ЭД, отслеживает информацию об этапах и результатах их обработки. В случае если Клиент своевременно не осуществил контроль за результатами обработки ЭД, ответственность за возникающие в данном случае риски несет Клиент.

5.8. **Об исполнении Банком ЭД (совершении Операции по Счету с использованием Системы) Банк уведомляет Клиента посредством направления ему SMS-уведомления по факту исполнения такого ЭД.**

Клиент является уведомленным о совершении каждой Операции по Счету, совершенной с использованием Системы в день получения SMS-уведомления:

Днем получения SMS-уведомления является день его отправления Банком, зафиксированный сервером отправителя, вне зависимости от фактического восприятия получателем по причинам, которые находятся вне зоны контроля Банка (Телефон Клиента выключен, Телефон Клиента находится вне зоны контроля Клиента, сбой в работе оператора связи, обслуживающего Клиента, расположение Телефона вне зоны обслуживания его оператором связи и т.д.).

5.9. Информирование Клиента о событиях, в случаях, предусмотренных законодательством, Соглашением, Договором счета, Договором вклада, а также передача Клиентом Банку информации и документов, осуществляется путем направления соответствующих писем, уведомлений, требований, документов направляемых по Системе. Если это предусмотрено Договорам, сообщения, уведомления в рамках таких Договоров могут осуществляться сторонами по Системе. Сроки направления писем (уведомлений, требований), определяются в соответствии с законодательством, Соглашением, Договором и иными соглашениями между Банком и Клиентом.

5.10. Банк обеспечивает возможность получения сформированных для Клиента и предназначенных ему ЭД, а также передачи Банку созданных Клиентом ЭД круглосуточно, за исключением времени проведения профилактических работ. О проведении профилактических работ Банк уведомляет Клиента по Системе не позднее, чем за 24 часа до начала их проведения. **При этом обработка ЭД производится только по рабочим дням и в течение операционного дня, установленного Банком.**

5.11. Банк хранит электронные журналы протоколов сеансов связи, архив принятых и отправленных ЭД, результаты проверки подлинности ЭД в течение пяти лет с даты передачи. Все указанные базы данных используются в качестве доказательства при возникновении споров.

6. БЛОКИРОВКА СИСТЕМЫ

6.1. Блокировка (временное отсутствие у Клиента возможности пользования Системой) может осуществляться Банком по собственной инициативе в соответствии с условиями Соглашения, или по обращению Клиента.

6.2. В случае:

- утраты Логина, Пароля, Телефона
- или использования Системы без согласия Клиента (например, Клиент получил SMS-сообщение об Операции, которую не совершал, или Клиенту пришло сообщение о входе в Систему, которого он не совершал и проч.)
- или подозрении, что неуполномоченные лицо могло получить доступ к Системе, в том числе, если есть подозрение что Логин, Пароль узнали неуполномоченные лица, утрате Телефона на Номер которого направляются SMS-сообщения, доступа к Телефону неуполномоченных Клиентом лиц (компрометация Логина, Пароля, Телефона),

Клиент обязан незамедлительно, но не позднее дня, следующего за днем получения от Банка SMS-уведомления о совершенной Операции (п. 5.8. Соглашения), уведомить Банк в рабочие часы Банка по телефону +7 (495) 644-00-11, доб. 145, 177, во внерабочие часы Банка на адрес электронной почты hotline@bankglobus.ru.

После получения такого сообщения доступ к Системе блокируется Банком.

6.3. Банк при наличии подозрений о компрометации Логина, Пароля или Номера Телефона, а также в иных случаях, когда операции в Системе соответствуют признакам осуществления перевода денежных средств без согласия Клиента, осуществляет блокировку Системы. Система блокируется Банком на срок не более двух рабочих дней. Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу:
http://www.cbr.ru/content/document/file/47786/priznaki_20180928.pdf

6.3.1. По факту приостановления операций Банк уведомляет Клиента по Телефону, номер которого указан как «основной», и одновременно:

- сообщает о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия клиента,
- запрашивает у Клиента подтверждение разблокировки Системы.

6.3.2. При получении от Клиента подтверждения, Банк незамедлительно разблокирует Систему. При неполучении от Клиента подтверждения Банк возобновляет работу Системы по истечении двух рабочих дней после дня совершения им действий, предусмотренных пунктом 6.3.1.

6.4. Все разговоры по телефону при обращении Клиентов о блокировке, утрате Логина, Пароля, Телефона и использования Системы без согласия Клиента, уведомлении Банка в соответствии с п. 6.3, фиксируются Банком (записываются).

6.5. Для идентификации при телефонном звонке Клиент должен быть готов указать Банку

- фамилию имя отчество и дату рождения, место рождения, адрес регистрации,
- или фамилию имя отчество и Кодовое слово, установленное в соответствии с Договором счета.

При указании неверных данных (полностью или в ЛЮБОЙ части) Клиент не идентифицирован. Сообщение Клиента в таком случае считается не поступившим, но у Банка появляются сомнения в компрометации Номера Телефона, и Банк предпринимает действия в соответствии с п. 6.3 Соглашения.

6.6. После блокировки Системы по заявлению Клиента, или получении подтверждения, что подозрения Банка в компрометации были обоснованы, доступ к системе восстанавливается только на основании письменного заявления Клиента в Банк, при этом обязательно изменяются Логин и Пароль. При восстановлении Клиенту доступа к Системе Банк предоставляет новый Логин и временный пароль, который необходимо сменить Клиенту самостоятельно при первом входе в Систему. Платёжный сервис не доступен при входе в Систему по Временному паролю.

6.7. В случае нарушения Клиентом сроков внесения оплаты, со дня следующего за днем, когда оплата должна быть внесена, Банк блокирует работу Клиента в Системе, до момента внесения платы

6.8. При блокировке работы Клиента в Системе по любым основаниям ранее уплаченная плата перерасчету и возврату не подлежит, а за следующий период абонентская плата не начисляется и не взимается.

7. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ

Для обеспечения безопасности при работе в системе необходимо:

7.1. Использовать только лицензионное системное (Windows 8.1, Windows 10) и прикладное программное обеспечение. Следить и своевременно производить обновление программного обеспечения, по мере выпуска обновлений компанией разработчиком.

7.2. Использовать только лицензионное антивирусное программное обеспечение. Банк рекомендует к использованию антивирусное программное обеспечение, которое хорошо себя зарекомендовавшее и от известных разработчиков.

7.3. Отключить в настройках интернет-браузера функции автозаполнения и запоминания паролей, и включить функцию автоматической очистки истории посещений при завершении работы интернет-браузера.

7.4. Не использовать и не позволять к установке программное обеспечение удаленного доступа для управления компьютером («TeamViewer», «RADmin», «AmyAdmin», разного рода VNC-системы). Банк не предлагает своим клиентам к использованию подобное программное обеспечение, и не использует подобное программное обеспечение при предоставлении услуг клиентам.

7.5. Не открывать файлы и документы, полученные из неизвестных и(или) подозрительных источников (неизветные отправители, поддельные письма, поддельные сайты в сети Интернет и пр.). Не посещать ресурсы с предложениями подозрительного свойства или с предложениями бесплатно скачать документы или файлы, официально не распространяемые бесплатно. Не производить установку неизвестного программного обеспечения или программного обеспечения «взломанного», «вылеченного» или с так называемыми «таблетками или лекарствами» в комплекте. Подобное программное обеспечение может иметь встроенные инструменты не контролируемого удаленного доступа или компоненты вирусного программного обеспечения, обеспечивающего злоумышленникам полный и неконтролируемый доступ к компьютеру.

7.6. Осуществлять вход в Систему только через сайт «Клиент-Банка» https://online.bankglobus.ru/web_banking при этом необходимо убедиться в том, что соединение с сайтом «Клиент-Банка» защищено (в адресной строке указано «https», в адресной строке должен отображаться символ закрытого замка. В качестве альтернативного входа допускается использовать ссылку, размещенную на основном сайте Банка www.bankglobus.ru, в разделе «Частным Лицам».
Не вводить идентификационные данные Системы (логин, пароль), а также иные данные, используемые при работе в Системе, если адрес ресурса отличается хоть на один символ от указанного в соглашении или переход на сайт «Клиент-Банка» осуществлен из не доверенного источника (ссылка в письме, ссылка на стороннем ресурсе Интернет, не относящимся к официальным ресурсам Банка)

7.7. Не передавать третьим лицам, включая работников Банка логины, пароли и одноразовые SMS-коды, используемые при входе в Систему и при подтверждение платежный и иных операций в Системе. Работники Банка никогда не просят передавать им данные персонального пароля и одноразовых SMS-кодов ни по телефону, ни SMS-сообщением, ни посредством электронной почты и ни при очном общении на территории Банка. При осуществлении подобных попыток работником Банка, Банк просит незамедлительно сообщать о подобных фактах в службу собственной безопасности Банка.

7.8. Избегать утери, хищения или передачи третьим лицам Логина, Пароля, Телефонов, номера которых зарегистрированы в Системе и указаны в соответствующих приложениях к данному соглашению, а также других компонентов системы (токенов, смарт-карт при их наличии)

7.9. Периодически (не реже раза в 90 дней) производить смену Пароля. Не использовать простые комбинации в Пароле. Не использовать пароль, применяемый в системе «Клиент-Банк» в любых других интернет-сервисах и системах, включая вход в операционную систему. Пароль должен состоять

минимум из 8 символов, включающих заглавные и строчные буквы, цифры, а также специальные символы (!, ?, #, @).

7.10. Регулярно просматривать информацию о совершенных операциях и все информационные сообщения, полученные из Банка.

7.11. При обнаружении факта (в случае возникновения подозрений) несанкционированного доступа неуполномоченных лиц, компрометации парольной информации, проинформируйте сотрудников Банка. Помните: немедленное обращение в Банк значительно снижает вероятность хищения денежных средств, а также позволяет предотвратить мошенничество.

7.12. По завершению работы в системе обязательно нажимать кнопку «ВЫХОД».

7.13. Клиент принимает на себя все риски и потенциальные последствия при нарушении требований п.п. 7.1 – 7.12 данного соглашения.

7.14. Памятка по информационной безопасности клиента системы дистанционного банковского обслуживания передается Клиенту при заключении Дополнительного соглашения, а также является Приложением №4 к Соглашению.

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. В данном разделе описан порядок разрешения спорных ситуаций между Клиентами и Банком. Под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки Простой электронной подписи Клиента под Электронным документом. Настоящий раздел НЕ разрешение спорных ситуаций по претензиям Клиента к исполнению ЭД, подписанных усиленной электронной подписью. Претензии по ЭД, подписанных усиленной электронной подписью принимаются и рассматриваются в соответствии с соответствующим разделом Приложения №2 к Соглашению

8.2. Клиент представляет Банку собственноручно подписанное заявление в произвольной форме, содержащее существо претензии с указанием на документ, подписанный ПЭП на основании которого Банк выполнил операции по Счету Клиента.

8.3. Рассмотрение претензий в Банке осуществляется в течение 10 (Десять) дней с даты получения претензии относительно операции по Счету.

8.4. По итогам рассмотрения и в зависимости от принятого решения Банк либо удовлетворяет претензию Клиента, либо передает Клиенту письменное заключение о необоснованности его претензии, подписанное уполномоченным работником Банка.

8.5. В случае несогласия с заключением Банка по предъявленной Банку претензии Клиент направляет в Банк письменное уведомление о несогласии с формированием разрешительной комиссии для рассмотрения спора.

8.6. Банк обязан в течение не более 5 (Пяти) рабочих дней от даты подачи уведомления Клиента о несогласии с заключением Банка по предъявленной Банку претензии сформировать разрешительную комиссию. В состав комиссии включаются представители Клиента, представители Банка, в случае необходимости представители компании-разработчика Системы «iBank2», а также независимые эксперты. Выбор членов комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора он проводится случайно (по жребию).

8.7. Стороны передают разрешительной комиссии материалы и документы, подтверждающие факт передачи в Банк Клиентом Электронного документа, авторство, неизменность, подлинность и правильность исполнения Банком Электронного документа. Материалы и документы могут включать файлы, записи баз данных, протоколы Соединений (лог-файлы), в том числе подтверждающие факты отправок SMS с сеансовыми паролями, магнитные и иные носители с записями сеансов связи, договоры и соглашения, в соответствии и во исполнение которых сформирован спорный Электронный документ, заявления и другие документы, включающие техническую информацию об устройстве (устройствах), которое использовалось для доступа к Системе, о выполнении или невыполнении Требований Банка по обеспечению безопасности при работе в системе (указанных в п.7).

8.8. Разрешительная комиссия на основании изучения представленных Сторонами материалов проводит экспертизу и выносит заключение об обоснованности претензии Клиента большинством голосов.

8.9. Заключение Комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон и подписывается всеми членами Комиссии.

8.10. Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.

8.11. Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с Заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда Комиссия должна быть создана, возникший спор передается на рассмотрение и разрешение по существу суду. Все иные не урегулированные споры Сторон, связанные с обменом ЭД по Системе, также передаются на рассмотрение суда.

9. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ

9.1. За пользование Системой Клиент уплачивает Банку плату, сумма которой и сроки уплаты определяются в соответствии с Тарифами Банка. **Тарифы устанавливаются, изменяются и раскрываются Банком в соответствии с условиями Договора счета, сообщение об изменении Тарифов направляется также и по средствам Системы (в рамках информационного сервиса). Совершение операции по Счету в Системе после даты изменения Тарифов, означает сознательное согласие Клиента и принятие измененных Тарифов**

9.2. Дополнительные услуги, оказываемые Банком в соответствии с Дополнительным соглашением, оплачиваются в сроки и размере, установленном Тарифами.

9.3. При расторжении Дополнительного соглашения уплаченная Клиентом сумма платы за пользование Системой пересчету не подлежит и Клиенту не возвращается.

9.4. Клиент выражает свое согласие (заранее дает свой акцепт) на списание Банком, по требованию Банка, с любых Счетов средств вознаграждения, причитающегося Банку в соответствии с Дополнительным соглашением, в сроки, предусмотренные Тарифами. В случае отсутствия средств на Счетах Клиента в Российских рублях, Банк производит списание средств со счетов в валюте, по курсу Банка России, установленному на день списания.

10. ПРОЧИЕ ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. При использовании Системы Клиент обязан:

10.1.1. Оплачивать услуги Банка.

10.1.2. Не передавать Логин и/или пароль третьим лицам.

10.1.3. Контролировать получение из Банка подтверждения факта надлежащей доставки в Банк и обработки переданного документа.

10.1.4. Немедленно сообщать Банку о попытках несанкционированного доступа к Системе.

10.1.5. По требованию Банка предоставлять Банку надлежаще оформленные подлинные экземпляры документов, направленных в Банк с использованием Системы. До предоставления указанных документов Банк имеет право не производить платежи по счетам Клиента, о чем Банк обязан сообщить Клиенту не позднее окончания текущего операционного дня Банка. При предоставлении в Банк указанных документов Клиент должен на их обороте проставить отметку о том, что они уже были направлены в Банк посредством Системы.

10.2. Банк гарантирует:

10.2.1. Блокирование Системой ЭД при некорректных Логине и/или Пароле и/или SMS – коде.

10.3. Банк обязан:

10.3.1. Принять измененные Логин и Пароль по письменному заявлению Клиента в порядке, предусмотренном Соглашением.

10.3.2. Сообщить Клиенту об обнаружении попытки несанкционированного доступа к Системе.

10.3.3. Хранить архивы поступивших с помощью Системы ЭД, подписанных ЭП, в течение всего срока, предусмотренного для хранения соответствующих документов на бумажном носителе.

10.4. Банк имеет право:

10.4.1. Отказать Клиенту в приеме от него ЭД, подписанного ЭП, и потребовать предоставить надлежащим образом оформленный документ на бумажном носителе, известив об этом Клиента до окончания операционного дня.

10.4.2. Отказать в приеме ЭД, подписанных ЭП, если они составлены с нарушениями правил, установленных настоящим Соглашением.

10.4.3. Приостановить на неопределенный срок, предварительно уведомив Клиента путем направления сообщения по средствам Системы за 1 (один) рабочий день, прием от Клиента документов, подписанных ЭП в случае нарушения Клиентом своих обязательств, указанных в пунктах 10.1.2, 10.1.5, Соглашения, при нарушении обязательств Клиента по любому из договоров, заключенных между Банком и Клиентом, в том числе, при непредставлении Клиентом документов и информации, запрошенных Банком в рамках указанных договоров, и(или) при возникновении у Банка подозрений о проведении Клиентом сомнительных операций. При этом ранее оплаченные суммы за пользование Системой пересчету не подлежат и Клиенту не возвращаются.

10.5. Стороны несут ответственность за невыполнение или ненадлежащее выполнение своих обязательств в соответствии с законодательством Российской Федерации.

10.6. Банк не несет ответственность:

– за умышленную или неосторожную передачу Клиентом Логина и Пароля, доступа к Телефону, Номеру телефона неуполномоченным лицам;

- за неисполнение обязательств при отсутствии вины со стороны Банка в случаях обрыва линий связи, выхода из строя оборудования у любой третьей стороны, предоставляющей услуги связи;
- за исполнение за счет средств Клиента ЭД, подготовленных без участия Клиента и переданных по Системе если такие документы заверены надлежащей ЭП;
- за операции по Счетам, совершенные на основании ЭД, подписанных лицами, не обладающими или утратившими полномочия на соответствующий доступ к Системе, в том числе по причине несвоевременного уведомления Клиентом Банка о произошедших изменениях;
- за сбои в работе Системы, произошедшие не по вине Банка и повлекшие для Клиента невозможность передачи ЭД;
- за несвоевременное получение или неполучение Клиентом SMS-ключа, SMS-сообщения, получение этих сообщений третьим лицом, получение Клиентом соответствующих сообщений, адресованных третьему лицу, если данные обстоятельства произошли в связи с техническими сбоями или по иным причинам, не зависящим от Банка;
- за утерю Клиентом Телефона и/или утраты Клиентом контроля над Телефоном и/или Номером телефона;
- за финансовые потери, понесенные Клиентом в связи с нарушением и/или ненадлежащим исполнением Клиентом требований по защите от вредоносного кода компьютера (телефона), с использованием которого Клиент осуществляет работу в Системе.

10.7. В случае неисполнения или ненадлежащего исполнения одной из Сторон обязательств, предусмотренных Дополнительным соглашением, эта Сторона возмещает другой Стороне реальный ущерб (подтвержденный документально), понесенный последней в связи с указанным неисполнением или ненадлежащим исполнением Стороной своих обязательств.

11. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В СОГЛАШЕНИЕ

11.1. Банк вправе самостоятельно изменять Соглашение, но не чаще чем один раз в квартал.

11.2. Банк осуществляет предварительное раскрытие информации обо всех изменениях Соглашения.

11.3. Предварительное раскрытие информации осуществляется Банком не позднее, чем за 10 (Десять) календарных дней до вступления в силу изменений и дополнений в Соглашение.

11.4. Все изменения и дополнения, вносимые Банком в Соглашение, вступают в силу, начиная со дня, следующего за днем истечения срока, предусмотренного для раскрытия информации, в соответствии с Соглашением.

11.5. Использование Клиентом Системы после ввода в действие Тарифов является согласием Клиента на применение Тарифов.

11.6. С целью обеспечения гарантированного ознакомления всех лиц, присоединившихся к Соглашению до вступления в силу изменений или дополнений, Клиент обязан самостоятельно обращаться в Банк для получения сведений не менее 2 раз в месяц;

11.7. Банк с целью ознакомления Клиентов с условиями (изменениями) Соглашения размещает его путем предварительного раскрытия информации любым из нижеуказанных способов:
- размещение такой информации на сайте Банка в сети Интернет по адресу: www.bankglobus.ru;
- размещение объявлений и документов на бумажных носителях в помещениях Банка в месте, доступном для любого посетителя Банка

11.8. Моментом ознакомления Клиента с опубликованной информацией считается момент, с которого информация доступна для Клиентов.

11.9. Любые изменение и дополнения в Соглашение и/или Тарифы с момента вступления их в силу и/или ввода в действие с соблюдением процедур, указанных Соглашением, распространяются на всех лиц, присоединившихся к Соглашению, в том числе присоединившихся к Соглашению ранее даты вступления в силу изменений в Соглашение. В случае несогласия с изменениями или дополнениями, внесенными Банком в Соглашение, и/или с установленными Тарифами Клиент имеет право до вступления в силу таких изменений или дополнений (до осуществления операции в соответствии с изменениями) отказаться от Соглашения (расторгнуть Дополнительное соглашение) в порядке, предусмотренном в разделе 12 Соглашения. Присоединение к Соглашению на иных условиях не допускается.

12. СРОКИ ДЕЙСТВИЯ ДОПОЛНИТЕЛЬНОГО СОГЛАШЕНИЯ И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

12.1. Дополнительное соглашение действует по дату прекращения Договора счета.

12.2. Дополнительное соглашение может быть досрочно расторгнуто в следующих случаях:

12.2.1. По инициативе Клиента: по письменному заявлению Клиента в день получения Банком указанного заявления.

12.2.2. По инициативе Банка:

- без предварительного уведомления при отсутствии оборотов по Счетам Клиента в течение трех месяцев подряд;
- без предварительного уведомления в случае если в течение одного месяца после блокировки работы системы Клиентом не совершена замена Логина и пароля, в случаях и в порядке, установленными Соглашением;
- по уведомлению Банка, направленному Клиенту с помощью Системы за 15 (пятнадцать) дней в ином случае. Днем расторжения Дополнительного соглашения в этом случае является дата, указанная в уведомлении.

12.3. В день расторжения Дополнительного соглашения Банк отключает Клиента от Системы. Отключение, двухсторонним актом не оформляется и означает прекращение права Клиента использовать переданное ему программное обеспечение. В любом случае, уплаченные ранее Клиентом суммы абонентской платы перерасчету не подлежат и Клиенту не возвращаются.

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Все споры разрешаются Сторонами путем переговоров. В случае не урегулирования споров между Сторонами путем переговоров, они подлежат разрешению в суде согласно законодательству Российской Федерации.

13.2. При исполнении Дополнительного соглашения Стороны также руководствуются действующим законодательством Российской Федерации, нормативными документами Банка России.

14. АДРЕС И РЕКВИЗИТЫ БАНКА

Полное наименование:	«Банк Глобус» (Акционерное общество)
Сокращенное наименование:	Банк Глобус (АО)
Адрес места нахождения	115184, Россия, г. Москва, ул. Бахрушина, д.10, стр.1
ИНН/КПП	7725038220/770501001
ОГРН	1027739050833
БИК	044525473
Номер лицензии, выданной Банком России	2438
Корреспондентский счет в Банке России	30101 810 3 4525 0000 473 в ГУ Банка России по ЦФО г. Москва

Приложения:

Приложение №1 Ограничения на совершение платежей в системе Клиент-Банк

Приложение №2 Соглашение об использовании усиленной электронной подписи

Приложение №3 Формы Заявлений

Приложение №4 Памятка по информационной безопасности клиента системы дистанционного банковского обслуживания

Приложение №1
К Соглашению об обмене документами в электронном виде (электронными документами) по Системе «Клиент-Банк» в Банке Глобус (АО)

ОГРАНИЧЕНИЯ НА СОВЕРШЕНИЕ ПЛАТЕЖЕЙ В СИСТЕМЕ КЛИЕНТ-БАНК

1. **Лимит на Операции, совершаемые в Системе без усиленной электронной подписи – 100 000,00 в день (однократно или суммарно).**
2. Иные ограничения (в дополнение к Лимиту):

№ п/п	Тип операции	Валюта операции	Ограничение по сумме		Ограничение по получателю	
			календарный день	календарный месяц	балансовый счет получателя	валюта счета получателя
1.	Рублевый перевод					
2.2.	Списание со счета					
2.2.1.	с текущего счета	Российский рубль	Не установлено	Не установлено	Не установлено	Российский рубль
2.2.2.	со счета карты	Операция запрещена				
3.	Валютный перевод					
3.1.	Списание с текущего счета					
3.1.1.	На свой счет в Банке Глобус (АО)	Доллар США / Евро	Не установлено	Не установлено	Не установлено	Доллар США / Евро
3.1.2.	На чужой счет в Банке Глобус (АО)	Операция запрещена				
3.1.3.	На счет в другой кредитной организации	Операция запрещена				
3.2.	Списание со счета карты	Операция запрещена				
4.	Конверсия					
4.1.	Списание со счета карты					
4.1.1.	На свой счет в Банке Глобус (АО)	Операция запрещена				
4.1.2.	На чужой счет в Банке Глобус (АО)	Операция запрещена				
4.1.3.	На счет в другой кредитной организации	Операция запрещена				
4.2.	Списание с текущего счета					
4.2.1.	На свой счет в Банке Глобус (АО)	Российский рубль	Не установлено	Не установлено	Не установлено	Доллар США / Евро
		Доллар США / Евро	Не установлено	Не установлено	Не установлено	Российский рубль
		Доллар США / Евро	Операция запрещена			Доллар США / Евро

№ п/п	Тип операции	Валюта операции	Ограничение по сумме		Ограничение по получателю	
			календарный день	календарный месяц	балансовый счет получателя	валюта счета получателя
4.2.2.	На чужой счет в Банке Глобус (АО)	Операция запрещена				
4.2.3.	На счет в другой кредитной организации	Операция запрещена				

Приложение №2
к Соглашению об обмене документами в электронном виде (электронными документами) по Системе «Клиент-Банк» в Банке Глобус (АО)

СОГЛАШЕНИЕ ОБ ИСПОЛЬЗОВАНИИ УСИЛЕННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Владелец сертификата ключа проверки УЭП (Владелец ключа УЭП)** – Клиент, и/или уполномоченное им лицо, осуществляющее работу в Системе, которому выдан Сертификат ключа проверки УЭП.

1.2. **Ключ УЭП** – уникальная последовательность символов, предназначенная для создания ЭП.

1.3. **Ключ проверки УЭП** – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее - проверка электронной подписи).

1.4. **Компрометация ключа УЭП** – утрата доверия к тому, что используемые секретные ключи недоступны посторонним лицам.

1.5. **ПАК -** специальное устройство, необходимое для работы в Системе реализованное в виде USB-токена, содержащее средство криптографической защиты информации и программное обеспечение, предназначенное для выработки и хранения ключа УЭП Клиента и формирования УЭП Клиента внутри самого устройства, и обеспечивающее неизвлекаемость (невозможность считывания) Ключа УЭП Клиента.

1.6. **Компьютер Клиента** – персональный компьютер на котором установлено программное обеспечение необходимое и достаточное для осуществления электронного документооборота документами, подписываемыми УЭП.

1.7. **Реестр сертификатов** – электронный реестр выданных и аннулированных Банком Сертификатов ключей проверки УЭП, в том числе включающий в себя информацию, содержащуюся в выданных Банком Сертификатах ключей проверки УЭП, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки УЭП и об основаниях таких прекращения или аннулирования.

1.8. **Сертификат ключа проверки УЭП (Сертификат)** – документ на бумажном носителе по форме Приложения №___, выданный Банком и подтверждающий принадлежность Ключа проверки УЭП владельцу сертификата ключа проверки УЭП.

1.9. **Усиленная электронная подпись (УЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

УЭП, создаваемая в Системе, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» является усиленной неквалифицированной ЭП.

В Системе реализованы российские криптографические алгоритмы в соответствии с ГОСТ 28147-89, ГОСТ Р34.11-2012 (хеш-функция) и, ГОСТ Р34.10-2012 и требованиям ФСБ России к СКЗИ класса КС1 и КС2.

1.10. Все иные термины и определения применяются в соответствии с Соглашением об обмене документами в электронном виде (электронными документами) по Системе «Клиент-Банк» в Банке Глобус (АО) (далее – Основное соглашение).

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Приложение устанавливает:

- порядок генерации/перегенерации Ключей УЭП:
- условия признания ЭД, равнозначными документам на бумажном носителе;
- порядок проверки УЭП.

2.2. Для подписания электронных документов УЭП Стороны применяют только штатные – включенные в Систему средства УЭП. Используемые в Системе Средства УЭП:

- позволяют установить факт изменения подписанного ЭД после момента его подписания;

– обеспечивают практическую невозможность вычисления Ключа УЭП из УЭП или из ключа ее проверки,

а при создании УЭП:

– показывают лицу, подписывающему ЭД, содержание информации, которую он подписывает;
– создают УЭП только после подтверждения лицом, подписывающим ЭД, операции по созданию УЭП;
– однозначно показывают, что УЭП создана.

УЭП жестко увязывает в одно целое содержание ЭД и Ключ УЭП лица, подписавшего ЭД, и делает невозможным изменение ЭД без нарушения подлинности данной УЭП. После подписания ЭД УЭП любое изменение, дополнение или удаление символов документа делает УЭП некорректной и проверка УЭП с помощью Ключа проверки УЭП Стороны, подписавшей ЭД, дает отрицательный результат. По содержанию ЭД, подписанных УЭП, невозможно определить Ключ УЭП.

2.3. Стороны признают, что включенная в Систему подсистема защиты информации, которая обеспечивает целостность ЭД и позволяет определить лицо, подписавшее ЭД, путем заверения ЭД электронной подписью, при условии выполнения условий раздела 4 настоящего Соглашения, достаточна для обеспечения, а также для подтверждения авторства и контроля целостности (неизменности содержания) ЭД.

3. ПРОЦЕДУРА ФОРМИРОВАНИЯ (ГЕНЕРАЦИИ) КЛЮЧЕЙ УЭП

3.1. Банк передает Клиенту ПАК по Заявке Клиента и при условии оплаты вознаграждения за предоставление ПАК в соответствии с Тарифами.

Банк размещает руководство по генерации Ключей УЭП на сайте в сети Интернет по адресу: https://online.bankglobus.ru/web_banking

3.2. Клиент самостоятельно устанавливает драйвера носителей УЭП на Компьютере Клиента и осуществляет генерацию (создание) Ключей УЭП.

3.3. По результатам генерации Ключей УЭП Клиент распечатывает Сертификат на бумажном носителе в двух экземплярах. Сертификат собственноручно подписывается Владельцем ключа ЭП.

5.6.1. Для регистрации открытых ключей, Клиент предоставляет в Банк оба экземпляра Сертификата. Банк сверяет информацию в полученных от Клиента экземплярах Сертификата с данными, представленными в Системе по результатам генерации Клиентом Ключа УЭП. При положительном результате сверки данных Банк принимает от Клиента Сертификат (один из экземпляров Сертификата), регистрирует Сертификат в Реестре сертификатов и возвращает Клиенту второй экземпляр Сертификата с соответствующими отметками Банка о приеме Сертификата.

3.4. В Реестре сертификатов хранятся только Ключи проверки УЭП Клиента, Ключи УЭП Клиента Банку не известны.

3.5. Клиент получает возможность подписывать ЭД в Системе УЭП только после регистрации Сертификата Банком в Реестре сертификатов Факт регистрации Сертификата в Реестре и дата регистрации удостоверяется отметкой Банка о приеме Сертификата, в соответствии с п. 3.3. настоящего Соглашения.

3.6. Ключи УЭП, при отсутствии фактов о компрометации, действуют до времени, указанного в Сертификате.

3.7. Аннулирование Сертификата проверки ключа ЭП производится Банком в следующих случаях:

– по истечении срока его действия;
– при компрометации Ключа УЭП;
– по письменному заявлению Клиента в любое время;
– при перегенерации Ключей УЭП;
– при прекращении действия Дополнительного соглашения об электронном документообороте с использованием системы «Клиент-Банк».

Получить консультацию по вопросам генерации/перегенерации Ключей УЭП можно в Банке по тел. (495) 644-00-11

3.8. Перегенерация (замена) Ключей УЭП, не связанная с компрометацией Ключей УЭП, может производиться по инициативе любой из Сторон.

5.6.1. Перегенерация Ключей УЭП по инициативе Банка может осуществляться планово и экстренно:
- О плановой перегенерации Ключей УЭП Банк обязан проинформировать Клиента по Системе не менее чем за один месяц до предполагаемой даты перегенерации. С указанной Банком даты прежние ключи Клиента считаются недействительными, а Сертификат проверки ключа УЭП аннулируется;
- Об экстренной перегенерации обусловленной техническими неполадками Системы (разрушение или компрометация базы данных системы, обнаружение попыток взлома системы и т.д.), Банк сообщает Клиенту за один день до даты перегенерации. С указанной Банком даты прежние ключи Клиента считаются недействительными, а Сертификат аннулируется.

5.6.2. Если перегенерация Ключей УЭП производится по инициативе Клиента, Клиент обязан проинформировать об этом Банк по Системе не менее чем за один день до предполагаемой даты перегенерации. При этом прежние Ключи ЭП Клиента независимо от факта перегенерации считаются недействительными с даты и времени, указанных Клиентом в соответствующем сообщении.

3.9. При наличии действующего Сертификата перегенерация Ключей УЭП может осуществляться как в порядке, установленном п. 3.3, так и в следующем порядке:

5.6.1. По результатам перегенерации, Клиент направляет сформированный и подписанный действующей УЭП Сертификат по средствам Системы (без формирования Сертификата на бумажном носителе). Банк сверяет информацию в полученном от Клиента по Системе Сертификате с данными, представленными в Системе по результатам перегенерации генерации Клиентом Ключа УЭП. При положительном результате сверки данных Банк принимает от Клиента Сертификат, регистрирует Сертификат в Реестре сертификатов и направляет по Системе сообщение о принятии Сертификата. Одновременно Банк аннулирует предыдущий Сертификат.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ ПО СИСТЕМЕ, ХРАНЕНИЮ И ИСПОЛЬЗОВАНИЮ КЛЮЧЕЙ УЭП

4.1. Способ хранения Клиентом закрытых ключей УЭП должен исключать их утрату и использование неуполномоченными лицами. **Клиент обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение закрытых ключей**.

4.2. Банк располагает исключительно Ключами проверки УЭП. После исключения Сертификата проверки ключа УЭП из Реестра сертификатов такие Сертификаты хранятся в Банке не менее пяти лет после прекращения всех отношений с Клиентом.

4.3. Клиент гарантирует Банку и принимает на себя все риски, связанные с несоблюдением правил хранения Ключей УЭП, а именно:
- хранить Ключей УЭП только на предоставленном Банком ПАК и держать их в надежном, недоступном для третьих лиц месте
- не хранить на жестком диске в каком-либо виде, сетевых каталогах и на прочих общедоступных ресурсах;
- не создавать копии с ПАК.

Ответственность за безопасное хранение и использование Ключа УЭП лежит на Владельце ключа УЭП.

4.4. Для обеспечения безопасности при работе с Системой Клиенту рекомендуется:
- не использовать на Компьютере Клиента нелицензионное программное обеспечение (операционную систему, иное программное обеспечение) (далее – ПО), которое заведомо может содержать вредоносный код, или уязвимости, позволяющие произвести компрометацию Ключа УЭП;
- установить на Компьютере Клиента лицензионное антивирусное программное обеспечение с актуальными антивирусными базами, и ежедневно обновляемое;
- ежегодно производить перегенерацию Ключей УЭП;
- подключать внешние носители с Ключами УЭП только в момент работы с Системой. Извлекать ПАК из Компьютера если не осуществляются платежные операции. Не оставлять внешний носитель с Ключом УЭП постоянно подключенным к Компьютеру Клиента.;

- никогда и никому не сообщать логины / пароли Системы и тем более не доверять ключевые носители, включая родственников и сотрудников Банка;
- избегать использования Системы на чужих компьютерах или в интернет-кафе, на подобных ПК Вы рискуете скомпрометировать свои ключи / логин / пароль;
- контролировать действия IT-специалистов, особенно внештатных, в момент технического обслуживания, установки программного обеспечения на Компьютере Клиента с установленной Системой, не сообщать IT-специалистам пароли для проверки работы Системы, для входа в компьютер либо иные реквизиты доступа – делать это самостоятельно;
- перед открытием внешнего подключаемого носителя – обязательно проверить его содержимое на наличие вредоносного кода используемым антивирусом;
- также в качестве мер обеспечения безопасности необходимо следовать требованиям, указанным в разделе 7 Соглашения..

4.5. **Дополнительно к случаям, изложенным в разделе 6 Основоного соглашения, Клиент должен немедленно обратиться в Банк для блокировки при Компрометации Ключей УЭП,**

К событиям, связанным с компрометацией ключей, относятся, в том числе следующие:

- утрата носителя Ключа ЭП (ПАК), в том числе с последующим обнаружением;
- передача ключа ЭП в линию связи в открытом виде;
- временный доступ посторонних лиц к носителям Ключей УЭП;
- физическое повреждение носителя ключа ЭП (ПАК) не позволяющее произвести считывание ключа;
- утрата парольной фразы или пин-кода, установленной в процессе генерации (создания) ключа;
- блокирование доступа к закрытому ключу в результате ввода ошибочной парольной фразы или пин-кода

РИСКИ, СВЯЗАННЫЕ С НЕСВОЕВРЕМЕННЫМ СООБЩЕНИЕМ В БАНК О СЛУЧАЯХ УТРАТЫ ИЛИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ УЭП, НЕСЕТ КЛИЕНТ.

5. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ ПО ПОВОДУ АВТОРСТВА И НЕИЗМЕННОСТИ СОДЕРЖАНИЯ ЭД, ПОДПИСАННЫХ УЭП

5.1. Споры Сторон по поводу авторства и неизменности содержания ЭД рассматриваются Экспертной комиссией, формируемой Сторонами (далее по тексту – «Комиссия»). Процедура рассмотрения спора состоит из следующих этапов:

- предъявление претензии одной из Сторон другой Стороне;
- формирование Комиссии для рассмотрения спора;
- разрешение Комиссией спора по существу.

В состав Комиссии входят представители Клиента и Банка. Каждая Сторона самостоятельно определяет лиц, которые будут представлять ее в Комиссии.

5.2. При рассмотрении спора об авторстве и неизменности содержания ЭД Комиссия устанавливает следующие факты:

- предмет спора Сторон;
- перечень ЭД, относящихся к предмету спора;
- идентичность созданного Клиентом ЭД документу на бумажном носителе, распечатанному Банком и хранимому в документах дня Банка;
- принадлежность УЭП Электронного документа Клиенту.

5.3. При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:

- данные имеющегося в Банке архива отправленных/принятых ЭД;
- Ключи проверки УЭП, содержащиеся в Сертификатах ключей проверки УЭП, подписанных Клиентом и Банком и хранящиеся в Банке (Эталонные сертификаты).

5.4. Разрешение споров осуществляется на основании результатов проверки УЭП Клиента в спорном ЭД.

5.5. Комиссия осуществляет свою работу на территории Банка с использованием персонального компьютера, свободного от вирусов и программных закладокДля рассмотрения спора Комиссией Банк предоставляет Эталонный(е) сертификат(ы).

5.6. Клиент для рассмотрения спора Комиссией предоставляет Сертификат(ы) ключа(ей) проверки УЭП, хранящийся (хранящиеся) у Клиента.

5.7. Если инициатором рассмотрения спора является Клиент, Комиссией устанавливается актуальность Ключей проверки УЭП Клиента на момент передачи ЭД, являющегося объектом спора. Ключи проверки УЭП Клиента считаются актуальными, если соответствующие Сертификаты ключей

проверки ЭП были зарегистрированы в Реестре сертификатов в соответствии с настоящим Соглашением и действовали в момент, когда спорный ЭД был направлен Клиентом в Банк.

5.8. Принимая во внимание математические свойства алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации, ГОСТ Р34.10-2012,ГОСТ Р34.11-2012,, гарантирующими невозможность подделки значения сертифицированной УЭП любым лицом, не обладающим Ключом УЭП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания ЭПД заключается в доказательстве принадлежности УЭП конкретного ЭД конкретной Стороне.

5.9. В целях формирования Протокола проверки каждой УЭП которой был подписан спорный ЭД администратор безопасности Системы в присутствии Комиссии осуществляет следующие действия:

- выводит на печать Сертификат ключа проверки УЭП Клиента из Реестра сертификатов;
- сравнивает распечатанный Сертификат проверки ключа УЭП с Эталонным сертификатом, предоставленным Комиссии Банком, а также с аналогичным Сертификатом проверки ключа ЭП представленным Комиссии Клиентом.

  Значения Ключа проверки УЭП Клиента, содержащиеся в Реестре сертификатов, в Эталонном сертификате и в предоставленном Клиентом Сертификате, должны совпасть. В случае их несовпадения верным признается Эталонный сертификат;
- находит спорный ЭД и, используя меню «Проверить ЭП», формирует результат проверки ЭП;
- выводит на печать Документ (распечатывает ЭД) со списком идентификаторов подписавших его ключей ЭП.

5.10. Принадлежность УЭП Клиенту и подлинность ЭД считается установленными, если идентификаторы Ключей проверки УЭП, содержащиеся в списке идентификаторов, подписавших Документ, и Эталонном сертификате совпадают; в Документе сформирована запись «ЭП корректна» и распечатанный Сертификат из Реестра сертификатов совпадает с Эталонным сертификатом.

5.11. Заключение Комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон – подписывается всеми членами Комиссии.

5.12. Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.

5.13. Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с Заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда в соответствии с Соглашением Комиссия должна быть создана, возникший спор передается на рассмотрение и разрешение по существу суду.

Все иные не урегулированные споры Сторон, связанные с обменом ЭД по Системе, также передаются на рассмотрение суда.

Приложение №3
к Соглашению об обмене документами в электронном виде (электронными документами) по Системе «Клиент-Банк» в Банке Глобус (АО)

ФОРМЫ ЗАЯВЛЕНИЙ

1. ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ К СОГЛАШЕНИЮ ОБ ОБМЕНЕ ДОКУМЕНТАМИ В ЭЛЕКТРОННОМ ВИДЕ (ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ) ПО СИСТЕМЕ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)
2. ЗАЯВЛЕНИЕ О ВЫДАЧЕ ПЕРСОНАЛЬНОГО АППАРАТНОГО КРИПТОПРОВАЙДЕРА (ПАК) ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМЕ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)
3. СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА В СИСТЕМЕ «iBank»
4. ЗАЯВЛЕНИЕ О РЕГИСТРАЦИИ ДОПОЛНИТЕЛЬНОГО НОМЕРА МОБИЛЬНОГО ТЕЛЕФОНА ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМЕ «КЛИЕНТ-БАНК»
5. ЗАЯВЛЕНИЕ ОБ ИЗМЕНЕНИИ ПЕРЕЧНЯ СЧЕТОВ, ПОДКЛЮЧЕННЫХ К СИСТЕМЕ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)
6. ЗАЯВЛЕНИЕ О БЛОКИРОВКЕ / ВЫДАЧЕ НОВОГО ЛОГИНА / ПАРОЛЯ В СИСТЕМЕ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)
7. ЗАЯВЛЕНИЕ О РАСТОРЖЕНИИ ДОПОЛНИТЕЛЬНОГО СОГЛАШЕНИЯ ОБ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «КЛИЕНТ-БАНК» В БАНКЕ ГЛОБУС (АО)

Приложение №4
к Соглашению об обмене документами в электронном виде (электронными документами) по Системе «Клиент-Банк» в Банке Глобус (АО)

ПАМЯТКА
по информационной безопасности клиента системы «Клиент-Банк» Банка Глобус (АО)

Для обеспечения сохранности используемых Вами денежных средств, при осуществлении платежных операций с помощью системы «Клиент-Банк» Банка Глобус (АО) необходимо выполнять несколько простых рекомендаций.

1. Для работы с системой используйте компьютер с установленным лицензионным системным и прикладным программным обеспечением, регулярно обновляемым и поддерживаемым разработчиком.
2. Для защиты от вредоносного кода используйте лицензионные и полные версии антивирусного программного обеспечения от известных разработчиков(Антивирус Касперского, NOD32, DrWeb). В состав некоторых антивирусов входит модуль защиты платежей, при его наличии рекомендуем все операции, выполняемые в системе осуществлять с использованием данного модуля.
3. Никому не передавайте Ваши учетные данные (логин и пароль), используемые Вами для входа в систему.
4. Не используйте долговременный пароль для входа в систему на других ресурсах Интернет, таких как сайты, личные кабинеты на порталах, почтовые сервисы. Храните ваши учетные данные в хорошо защищенном месте, куда есть доступ только у Вас и ни у кого больше.
5. Не сообщайте никому и никогда поступающие Вам сообщения от Банка, особенно одноразовые коды подтверждения и одноразовые пароли.
6. Не передавайте никому предоставленный Вам USB-токен. Храните пароль от ключа на USB-токене также как и Ваши учетные данные для входа в систему. Никому не озвучивайте и не передавайте пароль от ключа.
7. Никому не передавайте свой персональный телефон, зарегистрированный в системе для получения одноразовых паролей и кодов подтверждения.
8. Не используйте на компьютере или на смартфоне программ предоставления удаленного доступа, таких как RAdmin, TeamViewer и т.п.
9. Не открывайте неизвестные Вам файлы и не устанавливайте неизвестное программное обеспечение, даже если на вашем компьютере установлен проверенный антивирус. Не переходите по ссылкам на неизвестные вам сайты в сети Интернет, даже, если они получены с Вашей точки зрения из доверенных источников (по электронной почте или в интернет-мессенджерах).
10. При утере или получении доступа третьих лиц к Вашим учетным данным, паролям, USB-токену, телефону или компьютеру – незамедлительно сообщите доступным образом об этом в Банк.

Помните, работники Банка никогда не просят Вас озвучить логин и/или пароль входа в систему, одноразовые коды SMS-сообщений, полученных Вами от Банка, пароль на доступ к USB-токену. Также никогда не предложат установить на ваш компьютер или смартфон программное обеспечение удаленного доступа для осуществления технической или иной поддержки.

О выявлении подобных действий работников Банка просим незамедлительно сообщать на Горячую линию Банка Глобус (АО):

+7 (968) 088-11-00
hotline@bankglobus.ru