

## ТЕХНИЧЕСКИЕ УСЛОВИЯ ПУБЛИЧНОЙ ОФЕРТЫ

Закрытое акционерное общество «Белорусско-Швейцарский Банк «БСБ Банк» (далее – Банк), с одной стороны, и юридическое лицо / индивидуальный предприниматель (нотариус, адвокат) (далее - Клиент), который имеет открытый счет в Банке и обслуживание которого может быть осуществлено посредством доступа к Системе «Интернет-Банк», с другой стороны, вместе именуемые Стороны, заключили настоящий договор о нижеследующем:

### 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Банк - Закрытое акционерное общество «Белорусско-Швейцарский Банк «БСБ Банк».

1.2. Клиент - юридическое лицо, индивидуальный предприниматель (нотариус, адвокат).

1.3. Система – система «Интернет-Банк», предназначенная для обслуживания Клиента, в том числе осуществления операций по счетам Клиента, открытым в Банке, предоставления информационных и иных услуг путем направления Клиентом распоряжения в электронном виде с использованием глобальной компьютерной сети Интернет по адресу [ibank.bsb.by](http://ibank.bsb.by).

1.4. Сайт Системы – Интернет-сайт по адресу [ibank.bsb.by](http://ibank.bsb.by).

1.5. Корпоративный Интернет-сайт - Интернет-сайт по адресу [www.bsb.by](http://www.bsb.by).

1.6. Услуга Банк-IT/[ibank-informer](http://ibank-informer) – использование Системы в режиме просмотра, в том числе получение выписок по счету, наличие картотеки к счетам Клиента, просмотр остатка по счетам Клиента и иное.

1.7. Услуга Банк-IT/[ibank](http://ibank) – использование Системы с возможностью осуществления операций по счетам.

1.8. Договор на обслуживание в системе «Интернет-Банк» (далее – Договор) включает в себя Общие условия публичной оферты (далее – Общие условия) и Технические условия публичной оферты (далее – Технические условия).

1.9. Распоряжение – запрос Клиента, сформированный в Системе, о предоставлении информации Банком и/или указание Банку на совершение определенных действий, в том числе осуществления операций по счетам Клиента, открытым в Банке.

1.10. Электронная цифровая подпись (далее – ЭЦП) - последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности.

1.11. Электронный документ - документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность.

1.12. Сертификат открытого ключа (далее – СОК) – электронный документ, изданный Банком и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную законодательством Республики Беларусь.

1.13. Пользователь – Администратор Системы или иное лицо, которому Администратор Системы предоставил права Пользователя.

1.14. Администратор Системы – лицо, уполномоченное Клиентом на создание учетных записей Пользователей, управление настройками Пользователей, предоставление им прав, присвоение им регистрационных номеров и создание для них временных паролей и являющееся контактным лицом Клиента.

1.15. Аутентификация – проверка подлинности Пользователя с использованием регистрационных и секретных данных Пользователя.

1.16. Параметры Аутентификации – Имя пользователя, Пароль, Авторизационный код, Кодовая фраза.

1.17. Имя Пользователя – уникальное имя, определенное Пользователем для доступа в Систему.

1.18. Пароль - последовательность символов, используемая для аутентификации Пользователя многократно.

1.19. Временный пароль - последовательность символов, используемая для аутентификации Пользователя однократно.

1.20. Авторизационный код - дополнительный пароль Пользователя, используемый для изменения глобальных настроек Системы.

1.21. Регистрационный номер - идентификатор, однозначно определяющий Пользователя в Системе.

1.22. Тарифы на операции и услуги - Тарифы на выполнение операций и оказание услуг, утвержденные Банком и действующие на момент проведения соответствующей операции.

1.23. Комплект абонента – носитель ключей ЭЦП (SafeNet iKey1000) и лицензия на ЭЦП (Криптопровайдер Avest).

## 2. ОСНОВНЫЕ УСЛОВИЯ

2.1. Для удостоверения информации, составляющей содержание электронного документа, а также для подтверждения его подлинности и целостности используется ЭЦП.

2.2. Для обеспечения безопасности и конфиденциальности передачи электронных документов применяются протокол безопасной передачи данных TLS (Transport Layer Security), Параметры Аутентификации и ЭЦП.

2.3. Клиенту предоставляется возможность с использованием Системы направлять в Банк распоряжения для их исполнения и получать из Банка необходимую информацию.

## 3. УСЛОВИЯ ЭКСПЛУАТАЦИИ И ПОЛУЧЕНИЯ ДОСТУПА К СИСТЕМЕ

3.1. Для корректной работы Системы необходим браузер:

- Internet Explorer версий 9+
- Opera актуальной версии или предыдущей
- Google Chrome актуальной версии или предыдущей
- Firefox актуальной версии или предыдущей
- Safari 5.1+ (для Windows), Safari актуальной версии или предыдущей и наличие доступа в Интернет.

3.2. Для получения доступа к Системе Клиент заполняет Регистрационную форму Администратора Системы (далее – Регистрационная форма).

3.3. Для совершения действий в Системе Клиент уполномочивает одного из своих сотрудников на управление доступом к Системе - Администратора Системы, других сотрудников – Пользователей - на совершение действий в Системе.

3.4. Клиент подтверждает, что Администратор Системы и Пользователи уполномочены им на совершение действий в Системе, и принимает меры для исключения работы в Системе неуполномоченных лиц.

3.5. Для доступа к Системе Пользователи используют свои Параметры Аутентификации, которые определяют самостоятельно. Доступ к Системе Пользователь получает при вводе уникального Имени пользователя и Пароля или с использованием ЭЦП в пределах прав, установленных для него Администратором Системы.

3.6. Администратор Системы регистрирует новых Пользователей, предоставляет Пользователям права для работы с Системой, создает временные пароли, выполняет иные действия, касающиеся работы Системы, а также связывается с Банком по телефону для решения технических вопросов эксплуатации Системы.

#### 4. УСЛОВИЯ ИСПОЛНЕНИЯ РАСПОРЯЖЕНИЙ

4.1. Пользователь от имени Клиента формирует распоряжения, в ответ на которые Банк предоставляет необходимую информацию, принимает распоряжения к исполнению либо отклоняет их.

4.2. Прием распоряжений Пользователя к исполнению осуществляется в соответствии с банковским днем, установленным для обслуживания Клиентов.

4.3. Распоряжения Пользователя в зависимости от их содержания и типа должны заверяться ЭЦП, а также сопровождаться в случае необходимости передачей в Банк дополнительных электронных или бумажных документов.

4.4. Банк принимает от Клиента все виды платежных и иных документов в электронном виде, установленные Банком и реализованные в Системе. Ограничения на применение электронных документов могут быть установлены в случаях, предусмотренных законодательством Республики Беларусь. Банк обязуется обеспечить своевременность и правильность обработки распоряжений в соответствии с законодательством Республики Беларусь и нормативными актами Банка.

4.5. Для формирования распоряжений Клиент заполняет реквизиты в электронной форме документа и направляет в Банк, который при получении осуществляет проверку ЭЦП и контроль правильности оформления распоряжений. При несоответствии реквизитов, не прохождении контроля, а также в иных случаях, предусмотренных законодательством Республики Беларусь, Банк операции по распоряжению не проводит, о чем Клиент получает соответствующее электронное сообщение.

4.6. Клиент получает информацию об этапах прохождения распоряжений в виде статусов распоряжений и контролирует совершение операций по счету посредством получения выписки.

4.7. Оперативность исполнения распоряжений и своевременность исправления ошибок зависит от равномерной передачи формируемых электронных документов в течение дня в случае их большого количества.

4.8. При отсутствии или недостаточности средств на счете Клиента обработка правильно оформленных распоряжений выполняется в соответствии с законодательством Республики Беларусь и условиями договоров, заключенных с Банком.

4.9. По требованию Клиента Банком выдается бумажная копия электронных документов с отметкой Банка об исполнении.

4.10. При обнаружении ошибок в работе Системы при создании распоряжений Клиент обязуется сообщать о них Банку, а также по требованию Банка предоставлять письменное изложение ошибочных случаев и сопутствующую им информацию (снимок экрана).

## 5. УСЛОВИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

5.1. Взаимодействие Клиента и Банка осуществляется на Сайте Системы.

5.2. Система предоставляет информацию через открытые средства коммуникации. Для обеспечения безопасности передачи данных используется протокол TLS (Transport Layer Security).

5.3. Вход Пользователя в Систему осуществляется по Имени Пользователя и Паролю или по ключам ЭЦП.

5.4. Распоряжения Клиента подписываются ЭЦП. Путем применения средств ЭЦП осуществляется удостоверение информации, составляющей содержание электронного документа, а также подтверждается подлинность и целостность электронного документа.

5.5. Пользователь обязан хранить в секрете и не передавать третьим лицам носитель ключей ЭЦП и свои Параметры Аутентификации.

## 6. ПОДКЛЮЧЕНИЕ КЛИЕНТА

6.1. Для подключения к Системе Клиент на сайте Системы заполняет Регистрационную форму, выбирает режим работы Системы и направляет ее в Банк. Для регистрации Администратора Системы используется УНП или номер счета Клиента в Банке.

6.2. Сотрудник Банка получает от Клиента Регистрационную форму, обрабатывает и принимает или отклоняет ее. При отклонении Регистрационной формы Клиент оформляет новую Регистрационную форму.

6.3. После получения уведомления о принятии Регистрационной формы Клиент обращается в Банк для подписания соглашения о присоединении к условиям Договора.

6.4. В случае подключения услуги Банк-IT/internet в режиме платежей Клиент дополнительно подписывает акт передачи комплекта абонента, по которому Банк передает, а Клиент принимает комплект абонента.

6.5. После заключения Договора Сотрудник Банка передаёт Временный пароль Клиенту, который используется для активации Системы.

6.6. Администратор Системы выполняет активацию Системы, выбрав на Сайте Системы в «Центр помощи» раздел «Активация системы». При активации указываются УНП или номер счета и Временный пароль. Далее Администратор Системы вводит Имя пользователя и новый Пароль, который придумывает самостоятельно. Дальнейший доступ к Системе Администратор Системы получает при вводе Имени пользователя и нового Пароля.

6.7. Добавление и подключение новых Пользователей осуществляет Администратор Системы. Для этого он добавляет нового Пользователя и предоставляет ему Регистрационный номер и Временный пароль.

6.8. Пользователь выполняет активацию Системы. Для этого Пользователь на Сайте Системы в «Центр помощи» выбирает раздел «Активация системы». При активации указываются Регистрационный номер и Временный пароль, которые выдал Администратор Системы. Далее Пользователь вводит Имя пользователя и новый Пароль, которые придумывает самостоятельно. Дальнейший доступ к Системе Пользователь получает при вводе Имени пользователя и нового Пароля.

6.9. Все права доступа Пользователям к задачам и счетам в Системе предоставляет Администратор Системы.

## 7. ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ ЭЦП И ВЫДАЧА СОК

### ДЛЯ ИСПОЛЬЗОВАНИЯ УСЛУГИ БАНК-IT/INTERNET В РЕЖИМЕ ПЛАТЕЖЕЙ

7.1. Для использования услуги Банк-IT/Internet в режиме платежей Клиент должен сгенерировать ключ ЭЦП. Генерация ключа ЭЦП осуществляется на компьютере Клиента на носителе ключей ЭЦП.

7.2. Клиент самостоятельно устанавливает на своем компьютере программное обеспечение из раздела Системы «Справка/Установка Криптозащиты», которое содержит следующие программные модули:

7.2.1. драйвер носителя ключей iKey;

7.2.2. криптопровайдер Авест;

7.2.3. персональный менеджер сертификатов Авест;

7.2.4. BSBBankAgent – сервис подписания Электронных документов.

7.3. Для получения нового СОК Пользователь самостоятельно:

7.3.1. формирует запрос на выдачу СОК в разделе Системы «Настройка – Запрос на сертификат»;

7.3.2. генерирует ключи ЭЦП;

7.3.3. печатает карточку открытого ключа проверки подписи, на которой проставляется подпись владельца карточки открытого ключа, руководителя и печать организации и передает ее в Банк;

7.3.4. после выпуска СОК Банком Клиент устанавливает его из раздела Системы «Настройка – Мои сертификаты» путем нажатия кнопки «Установить сертификат».

7.4. В случае предоставления Клиентом карточки с образцами подписей и оттиска печати Банк проверяет существующие карточки открытого ключа Клиента. При этом в случае изменения владельца карточки открытого ключа или его персональных данных Банк блокирует СОК Пользователя.

7.5. В случае использования услуги Банк-IT/ibank-viewer в режиме просмотра Клиент может переключиться на услугу Банк-IT/ibank в режиме платежей, для чего он осуществляет действия в соответствии с п. 6.4. настоящих Технических условий.

## 8. УТЕРЯ НОСИТЕЛЯ КЛЮЧЕЙ ЭЦП ИЛИ КОМПРОМЕНТАЦИЯ ЛИЧНОГО КЛЮЧА ПОДПИСИ

8.1. В случае утери носителя ключей ЭЦП или компрометации личного ключа подписи Администратор Системы запрещает использование ЭЦП Пользователю, которому предоставлено право использования ЭЦП.

8.2. В случае утери, кражи носителя, компрометации личного ключа ЭЦП Клиент обращается в Банк с заявлением в произвольной форме, подписанным руководителем и заверенным печатью Клиента.

8.3. Сотрудник Банка принимает от Клиента заявление, после чего СОК и ключи ЭЦП блокируются Банком, при этом создание и регистрация новых ключей ЭЦП осуществляется в соответствии с п. 7.3. настоящих Технических условий.

## 9. СМЕНА АДМИНИСТРАТОРА СИСТЕМЫ

9.1. Для смены Администратора Системы новый Администратор Системы на Сайте Системы в «Центр помощи» выбирает раздел «Смена администратора» и заполняет новую Регистрационную форму и направляет ее в Банк через Систему.

9.2. Сотрудник Банка принимает от Клиента Регистрационную форму, сверяет информацию, принимает или отклоняет ее. При отклонении Регистрационной формы Клиент оформляет новую Регистрационную форму. При предоставлении доступа

новому Администратору Системы доступ предыдущему Администратору Системы блокируется.

9.3. Сотрудник Банка передаёт Временный пароль руководителю организации, который составляет расписку о получении Временного пароля.

9.4. Администратор Системы выполняет активацию Системы. Для этого Администратор Системы на Сайте Системы в «Центр помощи» выбирает раздел «Активация системы». При активации указываются УНП или номер счета и Временный Пароль. Далее Администратор Системы вводит Имя пользователя и новый пароль, которые придумывает сам. Дальнейший доступ к Системе Администратор Системы получает при вводе Имени пользователя и нового Пароля.

## 10. ВОССТАНОВЛЕНИЕ ПАРОЛЯ ИЛИ АВТОРИЗАЦИОННОГО КОДА АДМИНИСТРАТОРА

10.1. Если Администратор Системы забыл Пароль или Авторизационный код, он заполняет на Сайте Системы в «Центр помощи» форму «Восстановление пароля Администратора».

10.2. Сотрудник Банка принимает от Клиента заявление на восстановление пароля Администратора, сверяет информацию, принимает или отклоняет его. При отклонении заявления на восстановление пароля Администратора Клиент оформляет новое заявление.

10.3. Сотрудник Банка передаёт Временный пароль руководителю организации, который составляет расписку о получении Временного пароля.

10.4. Администратор Системы активирует Систему с указанием УНП или номера счета и Временного пароля. Далее Администратор Системы вводит свое Имя Пользователя и задает новый Пароль, который придумывает сам. Дальнейший доступ к Системе Администратор Системы получает при вводе Имени пользователя и нового Пароля.

## 11. ВОССТАНОВЛЕНИЕ ПАРОЛЯ ИЛИ АВТОРИЗАЦИОННОГО КОДА ПОЛЬЗОВАТЕЛЯ

11.1. Если Пользователь забыл Пароль или Авторизационный код, он обращается к Администратору Системы.

11.2. Администратор Системы задает Временный пароль для Пользователя.

11.3. Пользователь, получив доступ к Системе с использованием временного пароля, на Сайте Системы задает новый Пароль. Дальнейший доступ к Системе Пользователь получает при вводе Имени пользователя и нового Пароля.

## 12. ВОССТАНОВЛЕНИЕ ИМЕНИ ПОЛЬЗОВАТЕЛЯ

12.1. Если Пользователь забыл Имя Пользователя, он обращается к Администратору Системы.

12.2. Администратор Системы задает Временный пароль для Пользователя.

12.3. Пользователь активирует Систему, указав на Сайте Системы Регистрационный номер и Временный пароль, которые выдал Администратор Системы. Далее Пользователь вводит Имя пользователя, которое придумывает сам. Дальнейший доступ к Системе Пользователь получает при вводе нового Имени Пользователя и Пароля.

### 13. ЭКСТРЕННАЯ БЛОКИРОВКА И РАЗБЛОКИРОВКА ДОСТУПА К СИСТЕМЕ

13.1. В случае обращения Клиента в Банк в связи с утерей, кражей носителя, подозрения в компрометации ключа ЭЦП, несанкционированного использования Системы третьими лицами Банк производит экстренную блокировку Системы.

13.2. После осуществления экстренной блокировки доступа к Системе Клиент должен направить в Банк заявление на блокировку доступа к Системе в письменной форме, подписанное руководителем и заверенное печатью Клиента.

13.3. В случае наличия у Банка достаточных оснований полагать, что возможна попытка несанкционированного доступа от имени Пользователя, Банк производит экстренную блокировку доступа к Системе.

13.4. При необходимости блокировки доступа к Системе отдельных Пользователей Администратор Системы может выполнить эту операцию самостоятельно.

13.5. Для разблокировки доступа к Системе Администратор Системы на Сайте Системы в «Центр помощи» выбирает раздел «Разблокировать доступ», заполняет заявление на разблокировку доступа к Системе и направляет его через систему в Банк.

13.6. Сотрудник Банка принимает от Клиента заявление на разблокировку доступа к Системе, сверяет информацию, предоставляет Администратору Системы доступ к Системе или отклоняет его. При отклонении заявления на разблокировку доступа к Системе Клиент оформляет новое заявление.

### 14. ПРЕКРАЩЕНИЕ ИЛИ ПРИОСТАНОВЛЕНИЕ ОБСЛУЖИВАНИЯ В СИСТЕМЕ

14.1. Для прекращения обслуживания в Системе Клиент обращается в Банк для подписания дополнительного соглашения на расторжение договора; при использовании услуги Банк-іТ/internet в режиме платежей Клиент также возвращает Банку полученный комплект абонента и подписывает акт приемки-передачи комплекта абонента.

14.2. Приостановление обслуживания в Системе возможно в случае:

- неоплаты вознаграждения Банку, согласно Тарифам на операции и услуги, - до полного погашения задолженности;
- по требованию Клиента в случае временного неосуществления операций – до обращения Клиента в Банк с требованием о возобновлении обслуживания в Системе;
- предотвращения легализации доходов, полученных преступным путем, и финансирования террористической деятельности или распространения оружия массового поражения, если операции Клиента подозрительны для Банка;
- в иных случаях, предусмотренных законодательством или настоящим Договором.

14.3. Приостановление обслуживания в Системе осуществляется Банком за вознаграждение, согласно Тарифам на операции и услуги.

ЗАО « БСБ Банк»

Республика Беларусь, 220004, г. Минск, пр. Победителей, д.23, корп.4

к/с 3200001750013 в Национальном банке Республики Беларусь,

УНП 807000069, ОКПО 37580914