

ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ФИЗИЧЕСКИХ ЛИЦ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация – процедура проверки соответствия введённого Клиентом логина и пароля к логину и паролю в базе данных сервиса «ФАКТУРА.RU», удостоверение правомочности обращения Клиента в Банк, в том числе для совершения операций и/или получения информации по счетам и продуктам в Банке в порядке, предусмотренном договором ДБО.

Банк – Акционерное общество Банк «Развитие-Столица».

Биометрические данные – сведения, характеризующие физиологические и биологические особенности человека, которые позволяют установить его личность и используются Банком для установления личности субъекта персональных данных. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» в Единой биометрической системе размещаются биометрические персональные данные физического лица следующих видов:

- данные изображения лица человека, полученные с помощью фото- и видеоприборов;
- данные голоса человека, полученные с помощью звукозаписывающих устройств.

Временный пароль – цифровой код, посылаемый в виде SMS-сообщения на номер мобильного телефона, предоставленный Клиентом при заключении договора ДБО. Используется при первом входе в систему, и в случае если Клиент забыл свой пароль. SMS-сообщение содержит, кроме самого временного пароля, срок его действия, в течение которого Клиенту необходимо самостоятельно войти в Систему и сменить временный пароль на постоянный Пароль.

Дистанционное банковское обслуживание (ДБО) в системе «Интернет-банк «ФАКТУРА.RU» – предоставление Банком Клиенту возможности самостоятельно формировать и передавать в Банк по телекоммуникационным каналам общего пользования распоряжения по Счету и обмениваться с Банком информационными сообщениями, в том числе осуществлять переводы денежных средств в пользу зарегистрированных в Системе Поставщиков.

Договор дистанционного банковского обслуживания (Договор ДБО) – договор между Банком и Клиентом, заключенный путем присоединения Клиента к Правилам Дистанционного банковского обслуживания физических лиц.

Единая биометрическая система (ЕБС) - единая информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации.

Единая система идентификации и аутентификации (ЕСИА) — федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Заявление о присоединении – Заявление о присоединении к настоящим Правилам, составленное по форме, установленной Банком, в том числе в электронном виде.

Идентификация – совокупность мероприятий по установлению определенных Федеральным законом №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Закон №115-ФЗ) сведений о Клиентах, их Представителях, Выгодоприобретателях, Бенефициарных владельцах, по подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем.

Идентификация по биометрическим данным – идентификация, осуществляемая Банком при приеме на обслуживание клиентов – физических лиц без их личного присутствия в офисе Банка путем установления и подтверждения достоверности сведений о них, определенных п.5.8 ст.7 Закона №115-ФЗ, с использованием персональных данных, содержащихся в ЕСИА, и биометрических данных, содержащихся в ЕБС, в порядке, установленном статьей 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации».

Клиент – физическое лицо, заключившее с Банком договор ДБО.

Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Логин – уникальная последовательность символов, используемая для идентификации Клиента при входе в систему Интернет-банк для физических лиц, в том числе созданная Клиентом самостоятельно.

Номер мобильного телефона – номер мобильного телефона Клиента, указанный Клиентом в Заявлении о присоединении, или зарегистрированный у Клиента на Портале Госуслуг (используется в случае заключения Договора при прохождении Идентификации по биометрическим данным), в том числе в предоставленном в дальнейшем в Банк Заявлении об изменении параметров доступа в Систему Интернет-банк для физических лиц.

Оператор сервиса «ФАКТУРА.RU» – ЗАО «Биллинговый центр» (ИНН 5401152049, ОГРН 1025400512400, 630055, Новосибирская область, город Новосибирск, улица Мусы Джалиля, дом 11, офис 218, тел.: +7(495) 925-95-00), осуществляющее информационное и технологическое обслуживание Клиента и Банка в рамках сервиса «ФАКТУРА.RU».

Пароль – уникальный набор символов, используемый в паре с логином для доступа в систему Интернет-банк для физических лиц. Пароль многократного использования задается Клиентом самостоятельно сразу после успешного ввода временного пароля.

Портал Госуслуг - «Единый портал государственных и муниципальных услуг» (ЕПГУ), является федеральной государственной информационной системой, обеспечивающей доступ к сведениям о государственных и муниципальных учреждениях, а также содержащей сведения о государственных и муниципальных услугах, с использованием которой осуществляется предоставление государственных и муниципальных услуг в электронной форме, доступ к которой обеспечивается с помощью «Единой системы идентификации и аутентификации» (далее – ЕСИА).

Поставщик – юридическое лицо или индивидуальный предприниматель, на основании договора с Оператором осуществляющий реализацию товаров (работ, услуг, имущественных прав) Клиентам, производящим оплату товаров (работ, услуг, имущественных прав) Поставщика с использованием Сервиса.

Правила Дистанционного банковского обслуживания (Правила) – настоящие правила, определяющие порядок работы системы Интернет-банк для физических лиц, а также порядок взаимодействия Банка и Клиента в рамках данной системы.

Разовый пароль – уникальный набор символов, используемый в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банк, а также при подтверждении клиентом права доступа к системе Интернет-банк.

Разовый пароль предоставляется Клиенту на номер мобильного телефона, предоставленный Клиентом при заключении договора ДБО или зарегистрированный у Клиента на Портале Госуслуг (используется в случае заключения Договора при прохождении Идентификации по биометрическим данным), в виде SMS-сообщения или уведомления через мобильное приложение (PUSH-уведомление), имеет ограниченный срок действия (не более 10 минут). Любые действия в Сервисе, подтвержденные Разовым паролем, считаются выполненными Клиентом лично.

Руководство пользователя – руководство пользователя Интернет-банк для физических лиц, утвержденное оператором сервиса «ФАКТУРА.RU».

Сайт Банка - информационный портал Банка в сети Интернет, расположенный по электронному адресу <http://www.dcapital.ru/>. Сайт Банка содержит информацию о банковских продуктах и услугах Банка, действующих Тарифах, условиях обслуживания, а также иную необходимую Клиенту информацию.

Сервис «ФАКТУРА.RU» (Сервис) – информационно-технологический сервис, позволяющий его участникам организовать обмен электронными документами, SMS-сообщениями, PUSH-уведомлениями, E-MAIL- сообщениями и прочей информацией.

Система Интернет-банк для физических лиц (система Интернет-банк, Система) – интегрированная автоматизированная система, реализующая технологию предоставления банковских услуг Клиентам без их непосредственного визита в банк, и использующая Интернет как средство коммуникации между Клиентом и Банком. Система реализована на базе Сервиса «ФАКТУРА.RU», обеспечивающего информационное и технологическое взаимодействие между Клиентом и Банком. Для работы в Интернет-банке необходимо стационарное (компьютер и ноутбук) или мобильное (смартфон или планшет) устройство с доступом в Интернет. Для доступа в Интернет-банк на мобильном устройстве рекомендовано использовать мобильное приложение Банка, опубликованное в AppStore и Google Play. Мобильное приложение позволяет получить доступ к большей части услуг, доступных в Интернет-банке.

Счет - банковский счет (текущий счет) Клиента, номер которого указан в Заявлении Клиента.

Тарифы – Тарифы на услуги Банка, предоставляемые физическим лицам, в которых указаны размеры,

сроки и порядок взимания вознаграждения Банка за совершение операций для Клиентов, правила и порядок оплаты Клиентом расходов Банка, лимиты (максимальные лимиты) расходования наличных денежных средств, иные сведения и условия. Тарифы АО Банк «Развитие-Столица» размещены в местах обслуживания Клиентов, а также в общедоступных источниках информации: на сайте Банка в сети Интернет - <https://www.dcapital.ru>.

Уведомление об операции – информирование Клиента о совершении каждой операции с использованием электронного средства платежа в порядке, установленном настоящими Правилами.

Электронное средство платежа (ЭСП) - средство и (или) способ, позволяющие клиенту Банка составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Электронный документ (ЭД) – документ, сформированный с использованием системы Интернет-банк и содержащий в электронной форме распоряжение Клиента Банку на совершение операций по счетам Клиента или иных операций.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила, Заявление, Тарифы, Руководство пользователя в совокупности являются договором ДБО и устанавливают правила и положения, регулирующие предоставление Банком услуг ДБО посредством системы Интернет-банк.

Настоящие Правила и Тарифы размещены на официальном сайте Банка в сети «Интернет» и в подразделениях Банка.

Правила сервиса «ФАКТУРА.RU», расположены в сети Интернет по адресу: <https://cft.group/contracts/>. Руководство пользователя оператор сервиса «ФАКТУРА.RU» размещает на сайте www.faktura.ru.

Клиент считается ознакомленным с опубликованной информацией с момента, с которого информация доступна для клиентов.

2.2. Заключение Договора осуществляется в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, путем присоединения Клиента в целом и полностью к Правилам посредством подачи в Банк подписанного Клиентом Заявления о присоединении по форме, содержащейся в Приложении 1 к настоящим Правилам, при личной явке Клиента в подразделение Банка или через сайт Банка www.dcapital.ru (мобильное приложение) после прохождения удаленной идентификации через ЕБС и ЕСИА и исполненного Банком.

Физическое лицо, обратившееся в Банк через сайт Банка www.dcapital.ru для заключения Договора путем прохождения идентификации по биометрическим персональным данным должно удовлетворять следующим требованиям:

- не являться на момент обращения Клиентом Банка;
- являться гражданином Российской Федерации;
- не действовать к выгоде другого лица и не намереваться это делать (не иметь выгодоприобретателя);
- не иметь иного лица в качестве бенефициарного владельца;
- действовать лично, без участия представителя;
- являться налоговым резидентом исключительно в Российской Федерации.

Договор считается заключенным с момента Подключение Клиента к системе Интернет-банк Банк осуществляет сбор данных Клиентов и их размещения в Единой биометрической системе, а также регистрации и обновления сведений о Клиенте в федеральной государственной информационной системе «Единая система идентификации и аутентификации» (ФГИС ЕСИА).

2.3. Представленное Клиентом Заявление подтверждает:

- ознакомление Клиента с настоящими Правилами, а также выражает согласие Клиента с тем, что настоящими Правилами будут регулироваться правоотношения Банка и Клиента по Договору ДБО;
- согласие Клиента с Тарифами и предоставление Клиентом Банку права без дополнительного распоряжения Клиента списывать со Счета/Счетов Клиента, подключенного/-ых к Системе, денежные средства в оплату Комиссий Банка за предоставление услуг по Договору ДБО.

Права и обязанности Банка и Клиента по договору ДБО возникают с момента заключения договора ДБО.

Не допускается заключение договора ДБО в пользу третьего лица. Не допускается уступка прав, принадлежащих Клиенту по договору ДБО.

2.4. Внесение изменений и дополнений в Правила, осуществляется Банком в одностороннем порядке, в том числе путем утверждения Банком новой редакции Правил. Изменения доводятся

Банком до сведения Клиента посредством уведомления не позднее, чем за 10 (Десять) календарных дней до даты вступления в силу таких изменений. Уведомление осуществляется путем опубликования на сайте Банка. В случае несогласия Клиента с изменениями и дополнениями, вносимыми в Правила, новой редакцией Правил Клиент вправе расторгнуть договор ДБО.

Договор ДБО считается измененным, а изменения и дополнения в Правила, в том числе новая редакция Правил, считаются принятыми Клиентом, если по истечении 10 (Десяти) календарных дней после их опубликования Банком Клиент письменно не заявит о расторжении договора ДБО.

- 2.5. Банк определяет условия использования системы Интернет-банк, меры безопасности при работе в системе Интернет-банк (Приложение 2 к настоящим Правилам) и доводит эту информацию до Клиента, в том числе до заключения договора ДБО, любыми не запрещенными способами, в том числе путем опубликования на сайте Банка.
- 2.6. Подключение Клиента к системе Интернет-банк осуществляется при условии заключения договора ДБО, ознакомления и принятия Клиентом настоящих Правил. Подключаясь к системе Интернет-банк, Клиент соглашается использовать сервис «ФАКТУРА.RU» для обмена электронными документами и информацией с Банком в порядке и на условиях, определенных Правилами сервиса «ФАКТУРА.RU».
- 2.7. Сервис «ФАКТУРА.RU» обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети "Интернет".
- 2.8. Оператор сервиса «ФАКТУРА.RU» предоставляет доступ Клиенту к сервису «ФАКТУРА.RU» и осуществляет информационное и технологическое обслуживание Клиента и Банка в рамках сервиса. Сервис «ФАКТУРА.RU» доступен по адресу www.dcapital.ru и www.faktura.ru. Банк осуществляет регистрацию Клиента (предоставление возможности Клиенту использовать сервис «ФАКТУРА.RU» для обмена информацией) в сервисе «ФАКТУРА.RU». В процессе регистрации Банк:
 - осуществляет проверку документов и полномочий Клиента в объеме, достаточном для открытия счета и управления счетом в Банке;
 - заключает с Клиентом договор ДБО,
 - обеспечивает получение Клиентом уникального логина и пароля для обмена электронными документами и информацией.
 - получает от Клиента информацию о номере мобильного телефона, адресе электронной почты (при наличии);
 - передает сведения о Клиенте, а также вышеуказанную информацию в сервис «ФАКТУРА.RU».
- 2.9. Банк самостоятельно определяет набор услуг, к которым Клиенту может быть предоставлен доступ, с учетом технических возможностей и заключенных с Клиентом договоров.
- 2.10. Доступ Клиента к услугам ДБО через сеть Интернет осуществляется при условии его успешной идентификации и аутентификации на основании логина, полученного Клиентом при заключении договора ДБО в подразделении Банка или на номер мобильного телефона при прохождении удаленной идентификации через ЕБС и ЕСИА, и пароля. В случае 3 (Трех) неверных попыток ввода Клиентом Логина и/или пароля при входе в Систему доступ автоматически блокируется и будет автоматически разблокирован по истечении времени, указанного на экране. После превышения максимального количества последовательных блокировок, установленных Системой, Система автоматически приостанавливает обслуживание Клиента. Для возобновления Обслуживания Клиенту необходимо обратиться в подразделение Банка с письменным заявлением.
- 2.11. При подключении к ДБО Клиенту предоставляется полный доступ ко всем его Счетам и к информации по Кредитам, как уже действующим на момент заключения Договора, так и к тем, которые Клиентом будут открыты в Банке в последующем.
- 2.12. Распоряжения Клиента, переданные в электронных документах (распоряжения о списании денежных средств, заявления, заявки) направляются Банку только при условии успешного подтверждения операций, совершенных Клиентом в сервисе «ФАКТУРА.RU», разовыми паролями, направленными Клиенту оператором сервиса «ФАКТУРА.RU» на номер мобильного телефона, предоставленный Клиентом и зарегистрированный Банком при заключении договора ДБО.

В системе Интернет-банк используется только один номер мобильного телефона. Изменение номера мобильного телефона осуществляется только при личном визите Клиента в подразделение Банка и подачи Заявления по форме Приложения № 3.

- 2.13. В целях аутентификации Клиента при осуществлении переводов денежных средств с использованием системы Интернет-банк, а также при подтверждении клиентом права доступа к системе Интернет-банк применяются пароли многоразового действия (Пароли) и одноразовые

- коды подтверждения (Разовые пароли).
- 2.14. Разовый пароль генерируется сервисом «ФАКТУРА.RU» и:
- действителен на протяжении ограниченного периода времени;
 - используется для подтверждения клиентом права доступа к системе Интернет-банк или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением (договором) условий;
 - однозначно соответствует сеансу использования системы Интернет-банк или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банк;
 - доводится до Клиента по альтернативному системе Интернет-банк каналу связи;
- 2.15. Клиент соглашается с тем, что пароль и разовый пароль являются аналогом собственноручной подписи. Электронные документы, подтвержденные паролями и/или разовым паролем, признаются Сторонами равнозначными документам на бумажном носителе и могут служить доказательством в суде.
- 2.16. Стороны признают, что способы и средства обеспечения информационной безопасности, используемые при подключении Клиента к услугам ДБО и при осуществлении обмена электронными документами в системе Интернет-банк, указанные в Руководстве пользователя, достаточны для защиты от несанкционированного доступа к персональным данным, счетам и операциям Клиента в системе, а также подтверждения авторства и подлинности электронных документов.
- 2.17. Клиент самостоятельно и за свой счет обеспечивает подключение своих вычислительных средств к сети Интернет, а также обеспечивает их защиту от несанкционированного доступа и вредоносного программного обеспечения.
- 2.18. Банк самостоятельно определяет типы счетов и виды операций и информации, доступные Клиенту.
- 2.19. Банк исполняет распоряжения Клиента не позднее рабочего дня, следующего за днем поступления в Банк соответствующего электронного документа, за исключением случаев выявления операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента. Электронные документы, поступившие в Банк после окончания операционного дня, официально установленного Банком, считаются поступившими на следующий рабочий день.
- 2.19.1. В соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк и оператор сервиса «ФАКТУРА.RU» выявляют операции, соответствующие признакам осуществления перевода денежных средств без согласия клиента. Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети Интернет по адресу: www.cbr.ru.
- 2.19.2. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, Банк до осуществления списания денежных средств со счета Клиента приостанавливает исполнение распоряжения о совершении такой операции, а также приостанавливает предоставление услуг Интернет-банк на срок не более двух рабочих дней. Банк после выполнения действий по приостановлению исполнения распоряжения:
- 1) уведомляет Клиента по номеру мобильного телефона и/или адресу электронной почты, предоставленным Клиентом Банку при заключении договора ДБО, и/или посредством системы Интернет-банк:
 - о приостановлении исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, а также приостановлении предоставления услуг Интернет-банк;
 - о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия клиента;
 - 2) незамедлительно запрашивает у Клиента подтверждение возобновления исполнения распоряжения.
- При получении от Клиента подтверждения возобновления исполнения распоряжения Банк незамедлительно возобновляет исполнение распоряжения, а также восстанавливает Клиенту доступ к услугам Интернет-банк. При неполучении от Клиента подтверждения возобновления исполнения распоряжения Банк возобновляет исполнение распоряжения, а также восстанавливает Клиенту доступ к услугам Интернет-банк по истечении двух рабочих дней после дня совершения им действий по приостановлению исполнения распоряжения.
- 2.19.3. При выявлении операции, соответствующей признакам осуществления перевода денежных

средств без согласия клиента, Банк приостанавливает исполнение распоряжения о совершении такой операции, а также блокирует возможность предоставления распоряжений о списании денежных средств.

Ответственный сотрудник Банка (либо оператор сервиса «ФАКТУРА.RU») связывается с Клиентом по контактному номеру телефона, предоставленному Клиентом Банку, для подтверждения/опровержения Клиентом факта отправки распоряжения о списании денежных средств.

Идентификация Клиента осуществляется в соответствии с идентификационными данными Клиента Банка (ФИО Клиента, паспортные данные Клиента, информация о ЭД, отправленных ранее Клиентом).

На основании беседы с Клиентом ответственный сотрудник Банка (либо оператор сервиса «ФАКТУРА.RU») принимает решение о возобновлении исполнения распоряжения о совершении такой операции, восстановления возможности предоставления распоряжений о списании денежных средств.

Если физическим лицом, с которым связался ответственный сотрудник оператора сервиса «ФАКТУРА.RU»), не пройдена процедура идентификации, оператор сервиса «ФАКТУРА.RU» уведомляет об этом Банк. В течение двух рабочих дней Банк принимает решение о возобновлении исполнения распоряжения Клиента или его отмене. С этой целью сотрудник Банка связывается с Клиентом по контактному номеру телефона, предоставленному Клиентом Банку. В случае изменения ФИО, паспортных данных, исполнение распоряжения Клиента возобновляется только после обновления имеющихся у Банка сведений. Изменение указанных сведений проводится при личном обращении Клиента в Банк.

При невозможности связаться с Клиентом в целях подтверждения/опровержения факта отправки распоряжения Клиентом по истечении двух рабочих дней ЭД передается в Банк. Банк возобновляет исполнение распоряжения. Если ранее Клиенту была заблокирована возможность предоставления распоряжений о списании денежных средств, то возможность отправки распоряжений о списании денежных средств восстанавливается.

2.20. В соответствии с Федеральным Законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк уведомляет Клиента о совершенной операции с использованием ЭСП путем их отражения в Выписке по Счету. Дополнительно Банк может осуществлять отставку сообщения по каждой совершенной операции на мобильный телефон, на адрес электронной почты и/или путем направления информации о совершенных транзакциях в Систему.

2.21. В случае потери/кражи мобильного телефона и/или SIM-карты (на который/которую приходят SMS-уведомления с разовыми паролями), и/или утраты, кражи, несанкционированного копирования или незаконного использования Логина и/или Пароля, и/или наличия подозрений, что они стали известны третьим лицам, а также при обнаружении факта использования Системы без согласия Клиента, Клиент обязан незамедлительно уведомить об этом Банк в целях блокировки доступа в Систему:

- по телефону: (495) 937-91-70 – в рабочие часы Банка;
- по телефону линии технологического сопровождения Сервиса: (495) 925-95-00 – круглосуточно;
- либо путем личного посещения подразделения Банка.

но не позднее дня, следующего за днем получения Клиентом от Банка Уведомления об операции, которая была совершена без согласия Клиента с использованием Системы.

В случае обращения Клиента по телефону, работник Банка идентифицирует его в соответствии с идентификационными данными, предоставленными Клиентом Банку. Данными, необходимыми для идентификации физического лица являются: ФИО Клиента, паспортные данные Клиента. После обращения по телефону Клиенту необходимо обратиться лично в Банк с письменным уведомлением.

Банк, получив уведомление Клиента, приостанавливает предоставление услуг Интернет-банк (блокирует доступ Клиента к услугам Интернет-банк). Возобновление доступа к услугам Интернет-банк осуществляется при личном визите Клиента в Банк.

2.22. При приостановлении или прекращении использования клиентом электронного средства платежа на основании полученного от Клиента уведомления или в связи с нарушением Клиентом настоящих Правил Банк в день такого приостановления или прекращения предоставляет Клиенту информацию о приостановлении или прекращении использования электронного средства платежа по номеру мобильного телефона и/или адресу электронной почты, предоставленным Клиентом Банку при заключении договора ДБО, и/или посредством системы Интернет-банк.

2.23. В сервисе «ФАКТУРА.RU» реализован форматно-логический контроль полноты заполнения

реквизитов распоряжений, а также контроль лимитов на совершение операций. Распоряжения Клиента передаются Банку и принимаются Банком к исполнению после проверки полноты и корректности реквизитов распоряжений.

- 2.24. Банк взимает с Клиента комиссионное вознаграждение за совершение операций в системе Интернет-банк. Размер комиссионного вознаграждения за предоставление Банком услуг в соответствии с Правилами устанавливается Тарифами. Клиент поручает Банку списывать комиссионное вознаграждение за предоставленные услуги со счета Клиента. Банк не предоставляет услуги, если на счете Клиента недостаточно денежных средств для оплаты комиссионного вознаграждения.

В случае отсутствия денежных средств на счете Клиента, указанном в Заявлении о присоединении, Банк вправе без дополнительного распоряжения Клиента списать комиссионное вознаграждение за предоставленные услуги с любых счетов Клиента в Банке, если это не противоречит режиму соответствующего счета, либо не исполнить распоряжение Клиента.

- 2.25. Договор ДБО может быть расторгнут:
- Клиентом в любой момент путем подачи заявления в письменном виде при личном визите в Банк или передачи заявления Банку посредством системы Интернет-банк;
 - Банком в случае прекращения отношений между Банком и Клиентом.
 - Банком, в случае расторжения договора банковского счета (вклада) с Клиентом.
- 2.26. При расторжении договора ДБО доступ к сервису «ФАКТУРА.RU» прекращается.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Банк обязуется:

- 3.1.1. Обеспечить регистрацию Клиента в сервисе «ФАКТУРА.RU» и предоставить Клиенту логин, временный пароль для доступа в систему Интернет-банк и получения услуг ДБО.
- 3.1.2. Принимать к исполнению поступившие от Клиента электронные документы, оформленные в соответствии с законодательством Российской Федерации, требованиями нормативных документов Банка России, настоящих Правил и договоров между Клиентом и Банком, при условии прохождения Клиентом авторизации в системе Интернет-банк, т.е. однозначного совпадения логина и пароля, а также разового пароля. Банк исполняет принятые электронные документы не позднее рабочего дня, следующего за днем их получения от Клиента.
- 3.1.3. Не разглашать и не передавать третьим лицам информацию о Клиенте и его операциях, за исключением случаев, предусмотренных законодательством Российской Федерации и настоящими Правилами.
- 3.1.4. Обеспечить сохранность информации об операциях Клиента в системе Интернет-банк в течение срока, установленного законодательством Российской Федерации.
- 3.1.5. В случае невозможности предоставления услуг Интернет-банк по техническим или иным причинам разместить на сайте Банка или в системе Интернет-банк соответствующую информацию.
- 3.1.6. Информировать Клиента о мерах информационной безопасности при использовании системы Интернет-банк, рисках клиента и возможных последствиях для клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком. Информирование осуществляется в системе Интернет-банк, в подразделениях Банка.

3.2. Банк имеет право:

- 3.2.1. В одностороннем порядке прекратить предоставление услуги Интернет-банк в случае нарушения Клиентом своих обязательств по настоящим Правилам.
- 3.2.2. Списывать со счетов Клиента комиссионное вознаграждение за услуги Интернет-банк в соответствии с Тарифами Банка.
- 3.2.3. Отказать Клиенту в проведении операции в случае отсутствия на счетах Клиента средств для списания комиссионного вознаграждения за проведение операции, указания неправильных реквизитов получателя перевода или некорректном заполнении реквизитов.
- 3.2.4. Потребовать от Клиента представления документов и сведений, подтверждающих основание платежа и/или его назначение, а также иные документы в соответствии с требованиями законодательства Российской Федерации и внутренними документами Банка. Требование может быть направлено Клиенту любым способом.
- 3.2.5. Приостановить на 24 часа предоставление услуг Интернет-банк при выявлении фактов и признаков нарушения информационной безопасности.
- 3.2.6. Устанавливать лимиты на совершение операций в системе Интернет-банк, а также реализовывать в системе Интернет-банк другие механизмы, снижающие риски Банка и Клиента.
- 3.2.7. В одностороннем порядке вносить изменения в настоящие Правила с предварительным

уведомлением Клиента не менее чем за 10 (Десять) календарных дней через сайт Банка в информационно-телекоммуникационной сети Интернет.

- 3.2.8. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, приостановить исполнение распоряжения Клиента о совершении операции на срок не более двух рабочих дней и направить информацию о случаях и (или) попытках осуществления переводов денежных средств без согласия клиента в Банк России.
 - 3.2.9. Приостановить работу Системы для проведения регламентных, профилактических и иных работ, а также в случае необходимости применения мер по управлению информационными, финансовыми и иными рисками, когда непринятие указанных мер может повлечь возникновение угрозы безопасности работы Системы.
 - 3.2.10. Приостановить предоставление услуг Интернет-банк после предварительного предупреждения, в том числе в приеме от него распоряжений в электронном виде на проведение операции по банковскому счету (вкладу).
 - 3.2.11. Приостановить предоставление услуг Интернет-банк в случае действия (бездействия) Клиента, препятствующего работнику Банка завершить обновление сведений, полученных в результате идентификации Клиента до получения указанных сведений.
 - 3.2.12. Приостановить пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации, и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу денежных средств стало известно о замене SIM-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре ДБО.
- 3.3. Банк не несет ответственность:**
- 3.3.1. В случае невозможности предоставления услуг Интернет-банк по независящим от Банка обстоятельствам, в том числе по причине непредставления Банку сторонними организациями, сервисов необходимых для услуги Интернет-банк.
 - 3.3.2. За задержки и сбои, возникающие в сетях сотовых операторов и сервисах провайдеров, которые могут повлечь за собой задержки или недоставку SMS-сообщений или сообщений электронной почты Клиенту.
 - 3.3.3. За последствия компрометации логина, пароля и/или разовых паролей Клиента, а также за убытки, понесенные Клиентом в связи с неправомерными действиями третьих лиц, если Клиент не уведомил Банк в порядке, установленном п. 2.18 настоящих Правил.
 - 3.3.4. В случаях финансовых потерь, понесенных Клиентом, в связи с нарушением или ненадлежащим исполнением Клиентом рекомендаций по обеспечению безопасности при работе с системой Интернет-банк, а также требований по защите автоматизированного места от вредоносного кода.
 - 3.3.5. В случаях необоснованного или ошибочного перечисления Клиентом денежных средств получателям через систему Интернет-банк. Клиент самостоятельно урегулирует вопрос возврата денежных средств с их получателями.
 - 3.3.6. За ошибочное совершение Клиентом перевода денежных средств посредством использования системы быстрых платежей платежной системы Банка России в соответствии с Условиями предоставления услуги по переводу денежных средств посредством использования системы быстрых платежей платежной системы Банка России, являющимися приложением к настоящим Условиям (далее – СБП);
 - 3.3.7. За отказ в совершении перевода денежных средств посредством использования СБП;
 - 3.3.8. За ошибки Клиента, совершенные им при указании идентификатора получателя денежных средств при осуществлении перевода денежных средств посредством использования СБП. В указанном случае Поручение Банку о переводе денежных средств посредством использования СБП считается исполненным Банком надлежащим образом, а Клиент самостоятельно урегулирует все возможные дальнейшие претензии и/или взаиморасчеты с получателем денежных средств, на счет которого поступили денежные средства по переводу посредством использования СБП;
 - 3.3.9. За непредставление/представление не в полном объеме сведений, необходимых для осуществления перевода денежных средств посредством использования СБП в соответствии нормативными актами Банка России, законодательством Российской Федерации и настоящими Условиями, а также корректность предоставленных сведений;
 - 3.3.10. За бесперебойность функционирования СБП, работоспособность которого обеспечивается и контролируется Банком России.

3.4. Клиент обязуется:

- 3.4.1. Уплачивать Банку комиссионное вознаграждение за услуги Интернет-банк в соответствии с Тарифами.
- 3.4.2. Войти в Систему только с официального сайта Банка <https://www.dcapital.ru/> и/или Системы www.faktura.ru или <https://elf.faktura.ru/elf/app/?site=razvitie-stolica>.
- 3.4.3. Проходить авторизацию в системе Интернет-банк, с использованием логина и пароля, а также разового пароля, если это предусмотрено Руководством пользователя. После прохождения вышеуказанной процедуры авторизации, направляемые Клиентом электронные документы, признаются однозначно подписанными Клиентом, при этом, средством подтверждения в данном случае являются одновременно используемые логин и пароль (разовый пароль - если это предусмотрено Руководством пользователя).
- 3.4.4. Ежедневно осуществлять контроль состояния своих Счетов (даже, если операции не проводились).
- 3.4.5. Хранить в тайне и не передавать другим лицам логин и пароль, а также разовые пароли.
- 3.4.6. Обеспечить защиту автоматизированного рабочего места от вредоносного кода посредством использования антивирусного программного обеспечения.
- 3.4.7. При компрометации или подозрении на компрометацию пароля незамедлительно произвести смену пароля в системе Интернет-банк. При невозможности незамедлительно выполнить смену пароля, а также в случае компрометации или подозрении на компрометацию логина незамедлительно обратиться в Банк.
- 3.4.8. Предоставить Банку сведения и документы в соответствии с требованиями законодательства РФ и требованиями Банка, необходимые для идентификации Клиента.
- 3.4.9. Уведомлять Банк об изменении в предоставленных согласно пункту 3.4.8. Правил ДБО сведениях не позднее 5 (Пяти) рабочих дней после наступления таких изменений.
- 3.4.10. Предоставлять Банку актуальные сведения о номере мобильного телефона, адресе электронной почты. В случае их изменения сообщить Банку актуальные сведения в порядке, предусмотренном настоящими Правилами.
- 3.4.11. Ознакомиться с рекомендациями по обеспечению безопасности при работе с Интернет-банком, а также мерами информационной безопасности, размещенными в Руководстве пользователя, а также неукоснительно их соблюдать.

3.5. Клиент имеет право:

- 3.5.1. Получать услуги Интернет-банк, к которым Банком предоставлен доступ при заключении договора ДБО в соответствии с Руководством пользователя.
- 3.5.2. Устанавливать ограничения по параметрам операций, изменять лимиты на совершение операций в системе Интернет-банк, в том числе на максимальную сумму перевода денежных средств за определенный период времени.
- 3.5.3. В случае возникновения у Клиента претензий, связанных с предоставлением услуг Интернет-банк, оформить соответствующее заявление в подразделении Банка.
- 3.5.4. В случае необходимости обратиться в подразделение Банка для получения письменного подтверждения об операции, произведенной в системе Интернет-банк.

4. ПРОЧИЕ УСЛОВИЯ

- 4.1. За невыполнение или ненадлежащее выполнение обязательств, установленных настоящими Правилами, Банк и Клиент несут ответственность в соответствии с законодательством Российской Федерации.
- 4.2. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Банком своих функций по настоящим Правилам, и иных обстоятельств, не зависящих от Банка, Банк освобождается от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.
- 4.3. В случае возникновения разногласий и споров по заключенному Договору ДБО стороны принимают меры для их решения путем переговоров или направления письменных претензий с учетом взаимных интересов. В случае неурегулирования спора путем переговоров или при неполучении ответа на направленную претензию в течение разумного срока споры разрешаются в судебном порядке в соответствии с действующим законодательством РФ.
- 4.4. Приложения к настоящим Правилам являются их неотъемлемой частью настоящего договора.

5. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 5.1. Обработка персональных данных (далее - ПДн) в АО Банк «Развитие-Столица» осуществляется

с согласия субъекта ПДн на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации.

5.2. Обработка ПДн субъекта ПДн осуществляется в соответствии с «Частной политикой обработки персональных данных», размещенной на официальном сайте Банка (<https://www.dcapital.ru/politika.pdf>).

5.3. Присоединяясь к настоящим Правилам, Клиент дает согласие Банку, адрес (место нахождения): 105064, г. Москва, Нижний Сусальный пер., д. 5, стр. 15, на передачу обработки своих ПДн третьим лицам:

- ЗАО «Биллинговый центр», адрес (место нахождения): 630055, Новосибирская область, город Новосибирск, улица Мусы Джалиля, дом 11, офис 218, тел.: +7(495) 925-95-00;

- ЗАО «Золотая корона», адрес: 630102, г. Новосибирск, ул. Кирова, д. 86, тел. +7(383) 339-92-42, +7(383) 336- 49-49, +7(383) 335-80-88);

- АО «НСПК», адрес: 115184, г. Москва, ул. Большая Татарская, д. 11, тел. +7(495) 705-99-99.

Обработка ПДн осуществляется автоматизированным (с использованием средств автоматизации) способом.

Банком и третьими лицами, указанными в пункте 5.3. настоящих Правил, осуществляется сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

Состав ПДн обрабатываемых в системах ДБО: ФИО; дата рождения; место регистрации; реквизиты документа, удостоверяющего личность; номер мобильного телефона; адрес электронной почты, информация о банковских реквизитах (номер счета).

Согласие даётся с целью предоставления Клиенту услуг дистанционного банковского обслуживания.

Настоящее согласие даётся на весь срок действия договора ДБО.

Настоящее согласие может быть отозвано путём направления письменного заявления в Банк и/или третьим лицам. В случае отзыва субъектом ПДн согласия на обработку ПДн Банк и/или третьи лица вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ от 27.07.2006 г.

6. ПРИЛОЖЕНИЯ

Приложение 1 Заявление о присоединении к Правилам Дистанционного банковского обслуживания физических лиц

Приложение 2 Меры безопасности при работе в Системе Интернет-банк для физических лиц

Приложение 3 Заявление об изменении параметров доступа в Систему Интернет-банк для физических лиц.

Приложение 4 Условия предоставления сервиса по переводу денежных средств в рамках Системы быстрых платежей

Приложение 5. Условия использования счета Клиента в сервисе бесконтактной оплаты (СБПэй) через систему быстрых платежей (СБП) для физических лиц

**Приложение 1
к Правилам Дистанционного банковского
обслуживания физических лиц**

**ЗАЯВЛЕНИЕ
о присоединении к Правилам Дистанционного банковского обслуживания физических лиц**

Персональные данные					
Фамилия		Имя		Отчество	
Данные документа, удостоверяющего личность					
Наименование документа		Серия		Номер	
Дата выдачи		Кем выдан			
Контактная информация					
Номер мобильного телефона	+7()	Адрес электронной почты (E-mail)			
Кодовое слово					

Настоящим заявляю о присоединении к действующим Правилам Дистанционного банковского обслуживания физических лиц АО Банка «Развитие-Столица» (далее – Правила), размещенных на сайте www.dcapital.ru, в порядке, предусмотренном статьей 428 Гражданского кодекса РФ. Я подтверждаю, что все положения Правил разъяснены мне в полном объеме, включая случаи повышенного риска и ограничения способов и мест использования системы Интернет-банк, случаи и порядок уведомлений об операциях, совершаемых по моим банковским счетам с использованием системы Интернет-банк, ответственность сторон, Тарифы и порядок внесения изменений и дополнений в Правила, Тарифы и соглашаюсь на заключение договора ДБО на указанных условиях.

Прошу предоставить мне доступ к системе Интернет-банк и обеспечить возможность ее использования **в полном объеме для получения дистанционного банковского обслуживания** в соответствии с Правилами, в том числе выдать логин и временный пароль для доступа в систему Интернет-банк.

Уведомлен(-а) и согласен(-на), что доступ в систему Интернет-банк предоставляется ДБО-провайдером FAKTURA.RU через сайт www.dcapital.ru в порядке, определенном настоящими Правилами и Правилами сервиса «FAKTURA.RU».

Клиент

Ф.И.О.		Подпись		Дата	
--------	--	---------	--	------	--

Отметки Банка о принятии заявления

Должность		Ф.И.О.		Подпись		Дата	
-----------	--	--------	--	---------	--	------	--

Номер Договора		Дата Договора		Логин	
----------------	--	---------------	--	-------	--

Подтверждаю получение регистрационных данных и логина для доступа в систему Интернет-банк «FAKTURA.RU».

Ф.И.О.		Подпись		Дата	
--------	--	---------	--	------	--

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ИНТЕРНЕТ-БАНК ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

Использование системы Интернет-Банк потенциально несет в себе риски неблагоприятных последствий, связанных с хищением денежных средств. Настоящее приложение описывает риски, возникающие на стороне клиента при использовании системы Интернет-Банк, и определяет перечень мер по снижению этих рисков.

1. Описание рисков

- 1.1. Основным риском при использовании системы Интернет-Банк является риск получения злоумышленником несанкционированного доступа к управлению счетом Клиента и к документам Клиента, передаваемым в Банк через систему Интернет-Банк.
- 1.2. Последствиями несанкционированного доступа могут быть списание денежных средств со счета Клиента или утечка конфиденциальной информации о совершаемых клиентом операциях.

2. Способы несанкционированного доступа к системе Интернет-Банк

- 2.1. Основными способами получения несанкционированного доступа к системе Интернет-Банк являются:

- перехват злоумышленником управления компьютером клиента (мобильным устройством);
 - кража логина и пароля клиента для входа в систему Интернет-Банк;
 - перехват данных, передаваемых клиентом в Банк и получаемых клиентом из Банка.
- Получение несанкционированного доступа может быть осуществлено:
- злоумышленниками, получившими доступ к компьютеру (мобильному устройству) клиента через сеть Интернет или иные каналы связи.
 - третьими лицами, имеющими физический доступ к компьютеру клиента (мобильному устройству).

3. Признаки несанкционированного использования рабочего места клиента, предназначенного для работы в системе Интернет-банк:

- 3.1. В истории поручений в системе Интернет-банк указаны поручения, которые Вы не совершали.
- 3.2. Подозрительная активность на компьютере, с которого осуществляется работа (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.).
- 3.3. Осуществлен запрос на ввод разового пароля для подтверждения выполнения действий, не связанных с входом в систему или совершением операций (подтверждение ознакомления с какими-либо правилами, инструкциями, или для подтверждения входа в какой-либо раздел системы, открытия страницы).
- 3.4. Входящий звонок от лиц, представляющихся работниками Банка, уведомляющих Вас о регламентных/восстановительных работах в системе Интернет-банк или Банке.
- 3.5. Получение сообщения о блокировке/разблокировке доступа в систему Интернет-банк.
- 3.6. Изменение адреса в адресной строке браузера при работе с системой Интернет-банк.
- 3.7. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
- 3.8. Невозможность получения доступа к системе Интернет-банк по причине несовпадения пароля при введении заведомо верного пароля.
- 3.9. “Зависание” системы Интернет-банк при одновременной нормальной работе других интернет-ресурсов.
- 3.10. Внезапное приостановление работы SIM-карты, на номер которой посредством SMS-сообщений направляются разовые пароли (блокировка SIM-карты). Возможно незаконное изготовление третьими лицами дубликата SIM-карты (необходимо обратиться к оператору мобильной связи).
- 3.11. Данный перечень признаков несанкционированного использования системы Интернет-банк не является исчерпывающим. В зависимости от новых видов атак список может дополняться или корректироваться.

4. Для обеспечения безопасности работы в системе Интернет-банк реализовано

- 4.1. Шифрование канала связи с использованием протокола SSL/TLS и сертификата, подписанного удостоверяющим центром.
- 4.2. Идентификация(логин) и аутентификация (пароль и разовый пароль) для входа в Систему Интернет-банк.
- 4.3. Средства подтверждения (разовый пароль) для подтверждения подлинности, неизменности, целостности и авторства распоряжений Клиента.
- 4.4. Направление SMS-сообщений о проведении транзакций по счетам Клиента о действиях в системе Интернет-банк (вход в Систему Интернет-банк, смена пароля, подключение услуг, проведение транзакций и т.д) (сервис подключается отдельно).

5. Рекомендации Клиенту при работе в системе Интернет-банк:

- 5.1. В целях снижения возможного риска несанкционированного использования рабочего места в системе Интернет-банк и списания третьими лицами денежных средств со счета клиента, необходимо выполнять следующие организационные и технические меры:

- 5.1.1. Для входа в Интернет-банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона для входа или дополнительной проверки персональной информации в Интернет-банке!
- 5.1.2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет-банк или для подтверждения платежей, даже работникам банка.
- 5.1.3. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.
- 5.1.4. В случае утери мобильного телефона, на который приходят SMS-сообщения с разовым паролем, немедленно заблокируйте (замените) SIM-карту.
- 5.1.5. Запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете Интернет-банка вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в банк по ранее записанному вами телефону.
- 5.1.6. Устанавливайте мобильные приложения «БРС онлайн» только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является Center of Financial Technologies. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего телефона/смартфона.
- 5.1.7. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным ПО и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.
- 5.1.8. При вводе личной информации, помните, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя, так как они будут переданы в открытом (незашифрованном) виде и могут быть перехвачены.
- 5.1.9. Используйте виртуальную клавиатуру для ввода пароля.
- 5.1.10. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в банк с целью оперативного блокирования доступа!
- 5.1.11. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- 5.1.12. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.
- 5.1.13. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.
- 5.1.14. Запретите в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешите соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы ваши электронные почтовые ящики.
- 5.1.15. Не давайте разрешения неизвестным программам выходить в Интернет.
- 5.1.16. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.
- 5.1.17. Не используйте в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в других системах. Пароль должен быть от 6 до 15 символов и содержать строчные и прописные латинские буквы, и цифры.
- 5.1.18. Избегайте регистрации номера Вашего мобильного телефона, на который приходят SMS-сообщения с разовым паролем, в социальных сетях и других открытых источниках.
- 5.1.19. Не рекомендуется работать с системой «Интернет-банк «ФАКТУРА.RU» на компьютерах в Интернет-кафе или на других компьютерах общего пользования. Если возможность выполнить данную рекомендацию отсутствует, то при первой же возможности измените Пароль, войдя в систему Интернет-банк «ФАКТУРА.RU» с личного компьютера.
- 5.1.20. Не забывайте корректно завершать работу в системе «Интернет-банк «ФАКТУРА.RU» – используйте всегда для этого пункт меню «Выйти».

Выполнение вами данных рекомендаций позволит значительно снизить риски совершения несанкционированных операций в системе Интернет-банк.

6. При возникновении подозрений в осуществлении несанкционированных операций в системе Интернет-банк, несанкционированного доступа к компьютеру, либо при компрометации пароля, разового пароля на вход в систему Интернет-банк необходимо:

- 6.1. Выйти из Системы.
- 6.2. Заблокировать устройства, используемые для работы в Системе (в том числе, выключить/перевести в режим гибернации (сна) компьютер).
- 6.3. Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе. Смена номера телефона, предоставленного при заключении договора ДБО

возможна только по заявлению, оформленному в Банке.

- 6.4. В письменном заявлении описать обстоятельства компрометации пароля, разовых паролей, несанкционированного доступа, либо другую информацию по фактам, вызвавшим Ваши подозрения.
- 6.5. Возобновление доступа в систему Интернет-банк производится в подразделении Банка при личном обращении клиента.

Приложение 3
к Правилам дистанционного банковского
обслуживания физических лиц

ЗАЯВЛЕНИЕ
об изменении параметров доступа в Систему Интернет-банк для физических лиц

Персональные данные					
Фамилия		Имя		Отчество	
Данные документа, удостоверяющего личность					
Наименование документа		Серия		Номер	
Дата выдачи		Кем выдан			
Номер Договора ДБО			Дата Договора ДБО		

Прошу в соответствии с Правилами Дистанционного банковского обслуживания физических лиц АО Банка «Развитие-Столица» (далее – Правила):

- Выдать новый Пароль
- Приостановить (временно заблокировать доступ) обслуживание
- Возобновить (разблокировать доступ) обслуживание
- Изменить номер мобильного телефона на +7 (____)_____
- Изменить адрес электронной почты на _____
- Изменить кодовое слово на _____
- Расторгнуть Договор дистанционного банковского обслуживания
- Установить следующие лимиты:

Дневной		Месячный	
---------	--	----------	--

- Иное _____

Все термины и определения, используемые в настоящем Заявлении, имеют тот же смысл и значение, что и в Правилах.

Клиент

Ф.И.О.		Подпись		Дата		Время	
--------	--	---------	--	------	--	-------	--

Отметки Банка о принятии заявления

Должность		Ф.И.О.		Подпись		Дата		Время	
-----------	--	--------	--	---------	--	------	--	-------	--

Отметки Банка об исполнении заявления

Должность		Ф.И.О.		Подпись		Дата		Время	
-----------	--	--------	--	---------	--	------	--	-------	--

Условия предоставления сервиса по переводу денежных средств в рамках Системы быстрых платежей

Настоящие Условия регулируют порядок осуществления/получения Клиентами Акционерного общества Банка «Развитие-Столица» переводов денежных средств в рамках Системы быстрых платежей, используя для этих целей Номер мобильного телефона Получателя перевода, QR-код, Платежную ссылку.

Термины и определения

Условия – Условия предоставления сервиса по переводу денежных средств в рамках Системы быстрых платежей (Приложение к Правилам дистанционного банковского обслуживания физических лиц в АО Банк «Развитие-Столица»).

Банк-отправителя - банк, являющийся участником Системы быстрых платежей, обслуживающий банковский счет Отправителя перевода.

Банк-получателя - банк, являющийся участником Системы быстрых платежей, обслуживающий банковский счет Получателя перевода.

Банк по умолчанию - банк, который будет автоматически предложен Отправителю для проведения переводов в адрес Получателя - физического лица в рамках Системы быстрых платежей.

Идентификатор Получателя - номер мобильного телефона, указанный Получателем - физическим лицом, позволяющий однозначно установить номер банковского счета Получателя для зачисления денежных средств по Переводу.

АО «НСПК» (НСПК) - Акционерное общество «Национальная система платежных карт» – операционный и платежный клиринговый центр Системы быстрых платежей, обеспечивающий на основании правил СБП информационное и технологическое взаимодействие при формировании, обслуживании и использовании Токена в целях проведения Операций.

Оператор Системы быстрых платежей - Центральный банк Российской Федерации (Банк России).

ОПКЦ СБП—АО «НСПК», выполняющее функции операционного и платежного клирингового центра при осуществлении переводов денежных средств с использованием СБП.

Операция - перевод денежных средств в российских рублях с использованием Системы быстрых платежей.

Операция В2С - Операция, осуществляемая при переводе денежных средств от Плательщика – юридического лица, индивидуального предпринимателя или самозанятого Получателю –физическому лицу.

Операция С2С - Операция, осуществляемая при переводе денежных средств от Плательщика –физического лица Получателю - физическому лицу.

Операция С2В - Операция СБП, осуществляемая при переводе денежных средств от Плательщика – физического лица Получателю – юридическому лицу, индивидуальному предпринимателю или самозанятому.

Операция Me2Me pull – Операция СБП, осуществляемая по инициативе получателя при переводе денежных средств физическим лицом, между своими счетами, открытыми в разных Банках.

Отправитель - физическое лицо, в том числе Клиент, юридическое лицо, индивидуальный предприниматель или самозанятый, со Счета которого списываются денежные средства по Операции.

Получатель – физическое лицо, в том числе Клиент, Номер мобильного телефона которого указан Отправителем перевода, юридическое лицо, индивидуальный предприниматель или самозанятый, на Счет которого зачисляются денежные средства по Операции.

Поручение - распоряжение Клиента о переводе денежных средств, содержащее поручение Банку об осуществлении действий в рамках Системы быстрых платежей на основании предоставленной Клиентом информации.

Самозанятые - физические лица, и индивидуальные предприниматели, являющиеся налогоплательщиками налога на профессиональный доход в соответствии с Федеральным законом от 27.11.2018 N 422-ФЗ "О проведении эксперимента по установлению специального налогового режима "Налог на профессиональный доход".

Система быстрых платежей (СБП) - сервис быстрых платежей платежной системы Банка России, позволяющий физическим лицам мгновенно (в режиме 24 часа в сутки/7 дней в неделю) переводить денежные средства по Номеру мобильного телефона себе или другим физическим лицам вне зависимости от банка – участника Системы быстрых платежей, обслуживающего Отправителя или Получателя, а также осуществлять платежи в пользу Торгово-сервисных предприятий с использованием QR-кода/Платежной ссылки и получать возвраты денежных средств по проведенным Операциям в случае возврата товаров/отмены услуг.

Сервис - сервис по переводу денежных средств с использованием Номера мобильного телефона Получателя либо с использованием QR-кода/Платежной ссылки в рамках Системы быстрых платежей.

Сумма перевода - сумма денежных средств в российских рублях, указанная Отправителем перевода либо установленная Торгово-сервисным предприятием для осуществления Операции с использованием Системы быстрых платежей.

Торгово-сервисное предприятие (ТСП) - имущественный комплекс, используемый для реализации товаров (работ, услуг) юридическим лицом, индивидуальным предпринимателем или самозанятым, в том числе в информационно-телекоммуникационной сети "Интернет", установившим договорные взаимоотношения с Банком Получателя в целях перевода денежных средств за реализуемые физическим лицам товары (работы, услуги) с использованием СБП.

QR-код - это двухмерный штрих-код, предоставляющий информацию для ее быстрого распознавания с помощью камеры на мобильном телефоне, либо на иных программно-технических устройствах, используемых Банком для проведения операций с использованием данного кода.

QR-наклейка (Статический QR-код) - Сценарий Операции СБП С2В с использованием QR-кода, сформированного для многократного использования (оплата товара, работ или услуг в ТСП по QR-наклейке).

QR на кассе (Динамический QR-код) - Сценарий Операции СБП С2В с использованием QR-кода, сформированного для однократного использования (оплата товара, работ или услуг в ТСП по QR на кассе)

Платежная ссылка СБП – ссылка, формируемая ОПКЦ СБП, при переходе по которой с использованием мобильного устройства, работающего под управлением операционной системы iOS или Android, становится доступной платежная информация, необходимая для инициирования Клиентом Платежа по СБП С2В с использованием «ФАКТУРА.RU».

Привязка счета к ТСП – совершенное Клиентом действие, при котором Клиент дает свое согласие на осуществление Платежей по СБП С2В, иницированных в платформе ТСП, а также устанавливает счет, с которого будут списываться средства при совершении платежей по СБП С2В, иницированных в платформе ТСП.

Система быстрых платежей F.Balance. С2В.Подписки – услуга по осуществлению Платежей по СБП С2В, иницированных Клиентом в платформе ТСП.

Перечень указанных определений не является исчерпывающим.

Другие пункты настоящих Условий могут устанавливать иные определения.

1. Общие положения

- 1.1. СБП доступен Клиентам в Системе Интернет-банк.
- 1.2. Переводы доступны только для клиентов кредитных организаций, подключенных к СБП. Перечень кредитных организаций, подключённых к СБП, размещается на сайте НСПК в информационно - телекоммуникационной сети «Интернет» по адресу: <https://sbp.nspk.ru>.
- 1.3. Клиент может в рамках СБП выступать как в качестве Отправителя, так и в качестве Получателя.
- 1.4. Настоящие Условия становятся неотъемлемой и составной частью заключенных Договоров ДБО.
- 1.5. Изменения настоящих Условий осуществляется Банком в порядке согласно п. 2.3. Правил ДБО.
- 1.6. Все споры, связанные с применением настоящих Условий и осуществлением Операций в соответствии с настоящими Условиями, разрешаются в порядке, предусмотренном Договором ДБО.

2. Условия предоставления Сервиса и порядок совершения Операций

- 2.1. Клиент, выступая в качестве Получателя:
 - 2.1.1. Соглашается на зачисление на свой Счет денежных средств по Переводу, в котором в качестве реквизитов указан Идентификатор Получателя.
 - 2.1.2. По своему усмотрению (желанию) может установить Банк по умолчанию для получения Переводов. Установка Банка по умолчанию для получения Переводов подтверждается вводом Клиентом одноразового пароля, направляемого НСПК на номер мобильного телефона Клиента (Идентификатор Получателя).
 - 2.1.3. По своему усмотрению (желанию) может установить Счет, привязанный к номеру мобильного телефона, который будет использоваться в качестве Идентификатора Получателя, в целях получения Переводов.
- 2.1. Клиент, выступая в качестве Отправителя, получает возможность:
 - 2.1.1. Совершать Переводы в адрес Получателя – физического лица с выбором Банка Получателя из списка кредитных организаций, подключенных к СБП.
 - 2.1.2. Формировать, подтверждать и передавать в Банк Поручения, в которых в качестве реквизитов Получателя указан Идентификатор Получателя.
 - 2.1.3. Совершать переводы в адрес Получателя – юридического лица, индивидуального предпринимателя или самозанятого с помощью QR-кода/Платежной ссылки, предоставленной ТСП.
 - 2.1.4. Предоставлять или отзываться предварительно данное согласие (распоряжение) на списание со своего счёта средств по запросам на перевод со своих счетов (Me2Me Pull), поступившим от другого банка участника СБП, выступающего в роли Банка-получателя, а также указать счёт для списания.
 - 2.1.5. В случае отсутствия предварительно данного согласия, подтверждать или отвергать выполнение перевода по запросу на перевод со своих счетов (Me2Me Pull), поступившему от другого банка участника СБП, выступающего в роли Банка-получателя, а также указать счёт для списания.
 - 2.1.6. Совершать переводы в адрес Получателя – юридического лица, индивидуального предпринимателя или самозанятого со счета, привязанного к ТСП в мобильном приложении Сервиса (С2В.Подписки).
- 2.2. Переводы осуществляются в российских рублях.

- 2.3. Переводы осуществляются со Счетов Отправителей на банковские счета Получателей, открытые в российских рублях;
- 2.4. Переводы в пользу физических лиц совершаются Клиентом путем направления Банку Распоряжения с указанием в них Идентификатора Получателя, суммы Операции, наименования Банка Получателя и иных параметров, если они запрошены Банком. По факту формирования Клиентом распоряжения на перевод в пользу физического лица Банк предоставляет Клиенту сведения для проверки (включая, но не ограничиваясь): наименование Банка Получателя, фамилия, имя, отчество (при наличии) Получателя (сведения могут предоставляться в маскированном виде). В случае успешной проверки Клиентом предоставленных сведений, Клиент подтверждает распоряжение.
- 2.5. Переводы в пользу ТСП совершаются Клиентом путем направления Банку Распоряжения с указанием в них реквизитов, содержащихся в QR-коде/Платежной ссылке и иных параметров, если они запрошены Банком.
- 2.6. По факту формирования Клиентом распоряжения на перевод в ТСП Банк предоставляет Клиенту сведения для проверки (включая, но не ограничиваясь): торговое наименование ТСП, наименование юридического лица ТСП, сумма, подлежащая оплате, номер банковского счета. В случае успешной проверки Клиентом предоставленных сведений, Клиент подтверждает распоряжение.
- 2.7. Банк вправе отказать Клиенту в использовании Сервиса в следующих случаях:
 - при отсутствии у Банка технической возможности для работы в Системе быстрых платежей;
 - при отсутствии надлежащей идентификации Клиента в качестве Получателя перевода или Отправителя перевода;
 - при наличии запретов или ограничений на осуществление операций в рамках Системы быстрых платежей Банком России и/или Законодательством;
 - при недостаточности средств на Счете для осуществления перевода и оплаты комиссии Банка, предусмотренной Тарифами;
 - в иных случаях, установленных Договором ДБО и/или Законодательством.
- 2.8. В случае наличия у Банка подозрений и/или информации о несанкционированном характере Операций; при выявлении подозрительных и/или мошеннических операций; при появлении риска нарушения Клиентом Законодательства; в иных, установленных Банком и/или Законодательством, случаях, Банк осуществляет действия в порядке, установленном Договором ДБО, Законодательством.
- 2.9. Лимиты на совершение Переводов предусмотрены законодательством Российской Федерации и Договором ДБО. Банк вправе устанавливать лимиты по Операциям (их количеству, сумме и др.) в рамках Сервиса.
- 2.10. При осуществлении Операции С2С должны быть указаны следующие параметры:
 - Идентификатор Получателя перевода;
 - Сумма перевода;
 - Банк-получателя;
 - иные параметры, установленные Банком.Сумма комиссии (в случае ее наличия) указывается после ввода Клиентом параметров перевода или перед подтверждением Операции Клиентом. Комиссия в рамках Системы быстрых платежей взимается с Отправителя перевода.
- 2.11. При формировании Операции С2В используются следующие параметры: счёт Клиента для списания и сумма оплаты, если она не содержится в QR-коде.
- 2.12. При осуществлении операции Me2Me Pull должны быть указаны следующие параметры:
 - Сумма перевода;
 - Банк Отправителя;
 - иные параметры, установленные Банком.
- 2.13. В целях обеспечения возможности оказания услуги «Система быстрых платежей F.Balance. С2В.Подписки» в сервисе «ФАКТУРА.RU» обеспечена техническая возможность привязки Клиентом к ТСП в мобильном приложении сервиса «ФАКТУРА.RU» счета, с которого будет осуществляться списание средств для осуществления Платежа по СБП С2В, инициированного в платформе ТСП, а также отключения этой привязки счета к ТСП. Клиент может выбрать один счет из тех, по которым для него доступна отправка внешних переводов с использованием сервиса «ФАКТУРА.RU».
- 2.14. После ввода всех параметров для совершения Операции Клиент подтверждает ее путем ввода кода доступа, полученного посредством SMS-уведомления на Номер мобильного телефона Клиента, предоставленного/указанного Банку или посредством PUSH-уведомления через мобильное приложение.
- 2.15. Ответственность за корректность / достаточность указания Номера мобильного телефона Клиента / Получателя перевода и всех иных параметров для совершения Операции возлагается на Клиента.

- 2.16. При совершении Операции по переводу денежных средств Получателю перевода срок зачисления средств Получателю перевода зависит от Банка-получателя.
- 2.17. При зачислении средств Клиенту – Получателю перевода в случае, если Клиент не установил счет в Банке для зачисления денежных средств в рамках Сервиса, Банк производит автоматическое установление Счета. Клиент соглашается и подтверждает право Банка на автоматическое установление Счета.
- 2.18. Клиент несет ответственность за правильность и актуальность указания Банку как своего Номера мобильного телефона, так и Идентификатора Получателя при пользовании услугами в рамках СБП.

3. Иные положения

- 3.1. Признание недействительным какого-либо положения настоящих Условий не влечет недействительности других положений настоящих Условий, если иное не вытекает из признанного недействительным положения.
- 3.2. Клиент проинформирован, что в случае использования Сервиса быстрых платежей для оплаты товаров и услуг спорные вопросы по доставке товаров/оказанию услуг, возврата товара/отмены услуги или их качества рассматриваются между Отправителем и Получателем/Торгово-сервисным предприятием и/или в досудебном/судебном порядке без участия Банка.

**Условия использования счета Клиента в сервисе бесконтактной оплаты (СБПэй) через систему быстрых платежей (СБП) для физических лиц в АО Банк «Развитие-Столица»
(публичная оферта)**

1. ОБЩИЕ УСЛОВИЯ

1.1 Настоящие Условия использования счета Клиента в сервисе бесконтактной оплаты (СБПэй) через систему быстрых платежей (СБП) для физических лиц в АО Банк «Развитие-Столица» (публичная оферта) (далее по тексту – Условия) и являются типовыми для всех Клиентов.

1.2 Присоединение Клиента к настоящим Условиям в порядке ст. 428, 437-438 ГК РФ осуществляется с момента получения согласия Клиента с настоящими Условиями путем совершения Клиентом соответствующих настроек в мобильном приложении Банка или мобильном приложении СБПэй (подтверждение согласия с условиями настоящими Условиями введением кода, полученного из SMS – уведомления, push - уведомления).

1.3 Настоящие Условия размещены в общедоступных источниках информации: в сети Интернет на официальном Сайте Банка и действительны до истечения срока их действия или до момента их отмены Банком.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АО «НСПК» - Акционерное Общество «Национальная система платежных карт» - операционный и платежный клиринговый центр Системы быстрых платежей, обеспечивающий на основании правил СБП информационное и технологическое взаимодействие при формировании, обслуживании и использовании Токена в целях проведения Операций.

Аутентификация – удостоверение правомочности использования Мобильного устройства и дистанционного обращения Клиента в Банк для совершения банковских операций и/или получения информации по Счету, а также совершения иных действий в соответствии с Договором ДБО, с использованием Мобильного устройства.

Банк – АО Банк «Развитие-Столица».

Договор ДБО – договор между Банком и Клиентом, заключенный путем присоединения Клиента к Правилам Дистанционного банковского обслуживания физических лиц.

Договор о предоставлении банковской услуги (Договор) – отдельно заключаемые договоры о предоставлении определенной банковской услуги.

Клиент – физическое лицо, заключившее с Банком договор ДБО.

Мобильное устройство – мобильное персональное устройство Клиента под управлением операционной системы iOS или Android (смарт-часы, смартфон, коммуникатор, планшетный компьютер, и т.п.), имеющее возможность выхода в сеть Интернет, позволяющее установить в свою память СБПэй и проводить Аутентификацию Клиента.

Операция СБП – это финансовая операция, с использованием Счета Клиента при помощи СБПэй, на проведение которой Банком было предоставлено разрешение, а также совершаемая Клиентом путем перевода денежных средств через СБП в пользу ТСП, посредством сканирования QR-кода, считывания данных из NFC-метки или перехода по ссылке, предоставленной ТСП.

Платежная ссылка – ссылка, сгенерированная СБП для возможности осуществления оплаты за товары и услуги ТСП.

Провайдер - юридическое лицо, обеспечивающее на основании правил платежной системы и/или на основании отдельного соглашения с платежной системой информационное и технологическое взаимодействие в целях проведения Операций СБП. Провайдером СБПэй является АО "НСПК".

СБП – сервис быстрых платежей платежной системы Банка России, позволяющий физическим лицам мгновенно (в режиме 24 часа в сутки/7 дней в неделю) переводить денежные средства по Номеру мобильного телефона себе или другим физическим лицам вне зависимости от банка – участника Системы быстрых платежей, обслуживающего Отправителя или Получателя, а также осуществлять платежи в пользу Торгово-сервисных предприятий с использованием QR-кода/Платежной ссылки и получать возвраты денежных средств по проведенным Операциям в случае возврата товаров/ отмены услуг.

Сервис безналичной оплаты (СБПэй) - электронное средство платежа с использованием мобильного приложения СБПэй) для оплаты товаров и услуг в розничных магазинах и сети интернет с использованием всех поддерживаемых в СБП способов оплаты (QR-код, кнопка на сайте и т.д.) с помощью мобильного устройства.

Соглашение – соглашение об использовании Счета, заключаемое между Клиентом и Банком путем присоединения Клиента к настоящим Условиям в целом.

Счет – банковский счет (текущий счет) Клиента.

Тарифы Банка – Тарифы на услуги АО Банк «Развитие-Столица», предоставляемые физическим лицам, в которых указаны размеры, сроки и порядок взимания вознаграждения Банка за совершение операций для Клиентов, правила и порядок оплаты Клиентом расходов Банка, лимиты (максимальные лимиты)

расходования наличных денежных средств, иные сведения и условия. Тарифы АО Банк «Развитие-Столица» размещены в местах обслуживания Клиентов, а также в общедоступных источниках информации: на сайте Банка в сети Интернет – <https://www.dcapital.ru>.

Токен - цифровое представление реквизитов Счета, которое формируется по факту выполнения Клиентом действий, указанных в инструкциях Провайдера, а также в СБПЭй и хранится в зашифрованном виде в специализированной защищенной области СБПЭй, установленное на Мобильное устройство Клиента.

Торгово-сервисное предприятие (ТСП) - юридическое лицо, индивидуальный предприниматель или самозанятое лицо, реализующее (-ий) товары с возможностью их оплаты Клиентом через СБПЭй.

Электронное средство платежа – средство и (или) способ, позволяющие клиенту Банка составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

NFC-метка - чип, который может хранить небольшой объем информации для передачи другому устройству, такому как мобильный телефон. В контексте настоящего Соглашения – чип, на который записана Платежная ссылка.

QR-код – это двухмерный штрих-код, предоставляющий информацию для ее быстрого распознавания с помощью камеры на мобильном телефоне, либо на иных программно-технических устройствах, используемых Банком для проведения операций с использованием данного кода.

3. ПОРЯДОК ФОРМИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ ТОКЕНА

3.1. Для добавления Счета в СБПЭй необходимо следовать инструкциям Провайдера.

3.2. Счет не может быть добавлен и использован в СБПЭй в случаях ограничения его использования Банком.

3.3. Токен не может быть создан без наличия в Банке актуальной информации о зарегистрированном номере мобильного телефона Клиента, на который Банком направляется одноразовый пароль.

3.4. Использование Токена осуществляется в соответствии с настоящими Условиями, законодательством Российской Федерации, правилами платежной системы и требованиями Провайдера.

3.5. Токен используется Клиентом для совершения Операций в ТСП, поддерживающих технологию проведения бесконтактных платежей, а также через сеть Интернет (в интернет - магазинах).

3.6. Клиент уведомлен, понимает и соглашается с тем, что не все ТСП могут обеспечить возможность предоставления QR-кода или NFC-метки для оплаты через СБП, и что платежная система и/или кредитные организации могут вводить ограничения, в том числе по суммам Операций СБП.

3.7. При использовании Токена условия обслуживания Счета, к которому соответствующий Токен сформирован (Тарифы, установленные лимиты и ограничения, информирование по операциям, участие в акциях и иные условия) соответствуют действующей редакции. Операции, совершенные с использованием Токена, приравниваются к операциям, совершенным с использованием Счета, к которому сформирован такой Токен. На отношения между Клиентом и Банком, возникающие в результате использования Токена, распространяются условия Договора ДБО.

3.8. Блокирование Токена или его удаление из памяти Мобильного устройства не прекращает действие Счета, к которому соответствующий Токен сформирован, и не влечет технические ограничения на его использование (не блокирует счет). Если к Счету создано несколько Токенов, при блокировке одного из них, остальные Токены не блокируются.

4. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

4.1. Соглашение заключается на неопределенный срок и прекращает свое действие с момента прекращения действия Токена, который был сформирован в соответствии с Соглашением или с момента расторжения Договора о предоставлении услуги, на основании которого Банком обслуживается Счет, к которому сформирован соответствующий Токен.

4.2. Прекращение действия Соглашения не влияет на юридическую силу и действительность распоряжений о переводе денежных средств, направленных Клиентом в Банк до прекращения его действия.

5. ПЛАТА ЗА ИСПОЛЬЗОВАНИЕ СБПЭй

5.1. Банком не взимается плата за использование СБПЭй. Провайдер, а также иные сторонние организации, в том числе операторы беспроводной связи или поставщики услуг передачи данных, могут взимать плату за услуги в связи с использованием Мобильного устройства или СБПЭй. При этом все комиссии и другие платежи, применимые к Клиенту в соответствии с условиями заключенного Договора, также применяются ко всем операциям, совершенным с использованием СБПЭй.

5.2. Банк, а также СБПЭй или ТСП по своему усмотрению могут устанавливать лимиты на совершение операций.

5.3. До заключения Соглашения Клиент обязан ознакомиться с условиями оказания услуг, установленными СБПЭй, а также иными сторонними организациями.

6. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ МОБИЛЬНОГО УСТРОЙСТВА, НА КОТОРОМ ХРАНИТСЯ ТОКЕН

6.1. Клиент обязан соблюдать следующие меры для защиты Токена:

- не оставлять Мобильное устройство без присмотра;
- не передавать Мобильное устройство третьим лицам;

- обеспечить соответствующий уровень безопасности на Мобильном устройстве, используя антивирусное программное обеспечение (при наличии для данного типа Мобильного устройства), средства Аутентификации, встроенные в Мобильное устройство и предлагаемые Провайдером;
- убедиться, что на Мобильном устройстве не зарегистрированы средства Аутентификации третьего лица;
- не разглашать третьим лицам собственные средства Аутентификации на Мобильном устройстве, являющиеся конфиденциальной информацией;
- удалить все личные данные, финансовую информацию и Токены с Мобильного устройства, использование которого прекращено, или при необходимости передачи устройства в организацию, осуществляющую ремонт;
- обратиться в Банк незамедлительно, в случае подозрений на любое несанкционированное использование Мобильного устройства или размещенного в СБПЭй Токена, а также в случае утраты Мобильного устройства;
- не блокировать любые функции безопасности, предусмотренные на Мобильном устройстве в целях защиты Токена;
- не подвергать Мобильное устройство взлому операционной системы;
- не использовать СБПЭй при подключении к беспроводным сетям общего доступа.

6.2. С целью получения информации о совершенных операциях Клиент обязан предоставлять достоверные сведения, в том числе сведения о номере телефона и адресе электронной почты (при наличии), для получения SMS-сообщений, PUSH-уведомлений и E-mail-уведомлений Банка, а в случае изменения информации для связи с Клиентом, своевременно предоставлять актуальную информацию, согласно условиям Договора.

6.3. Клиент гарантирует, что номер мобильного телефона принадлежит лично ему и третьими лицами не используется.

6.4. Клиент проинформирован, что номер мобильного телефона будет использоваться в качестве его уникального идентификатора, в том числе при обращении в Банк, и для отправки ему SMS-сообщений и PUSH-уведомлений с информацией об операциях СБП с использованием Счета, пароле, для входа в системы дистанционного банковского обслуживания Банка, о кодах подтверждения. Несообщение Банку об изменении (утере) указанного номера является основанием для отказа в совершении операций по Счету, нарушением порядка использования электронного средства платежа и основанием для приостановления использования всех предоставленных Клиенту электронных средств платежа для совершения операций по Счету.

7. ОТВЕТСТВЕННОСТЬ

- 7.1. Ответственность за функционирование СБПЭй несет предоставляющий его Провайдер.
- 7.2. Банк не несет ответственности за возможные проблемы в использовании СБПЭй или отсутствие возможности для Клиента использовать СБПЭй для совершения тех или иных операций СБП.
- 7.3. Банк не несет ответственности за убытки, которые может понести Клиент в результате отказа ТСП в возможности совершения операций СБП с использованием СБПЭй. Банк не несет ответственности за работу Мобильного устройства Клиента.
- 7.4. Банк не несет ответственности за безопасность информации, предоставленной или хранимой Провайдером или другими третьими лицам в связи с использованием СБПЭй. Банк не несет ответственности при нарушении Провайдером правил безопасности, влияющих на любую собранную, сохраненную или отправленную информацию.
- 7.5. Клиент несет ответственность за все операции, совершенные с помощью СБПЭй, вне зависимости от того, свое или третьих лиц использовано при этом Мобильное устройство.
- 7.6. Клиент несет ответственность за все операции, совершенные с помощью Счета\Токена, за исключением случаев, предусмотренных условиями Договора и положениями действующего законодательства РФ.

8. ПРАВА И ОБЯЗАННОСТИ СТОРОН

8.1. Банк вправе:

- в любое время прекратить сотрудничество с Провайдером;
- приостановить возможность использования Счета для совершения операций СБП с использованием СБПЭй. Указанные выше действия Банк вправе предпринять без предварительного уведомления Клиента в случае, если Клиент не выполняет настоящие Условия и/или нарушает условия Договора, а также в иных случаях по усмотрению Банка;
- изменять настоящие Условия в любое время без предварительного уведомления Клиентов. Клиент соглашается со всеми изменениями, если он продолжает использование Счета в СБПЭй. Если Клиент не согласен принять изменения настоящих Условий, он должен удалить все Счета из СБПЭй. Изменения Условий становятся обязательными для сторон в даты их вступления в силу.

8.2. Клиент вправе:

- инициировать формирование Токенов и удалять Токены через СБПЭй;
- обращаться в Банк с заявлениями, в том числе при возникновении споров, связанных с операциями, совершенными с использованием СБПЭй. Заявления Клиента рассматриваются Банком в сроки и в порядке, установленные Договором ДБО;
- в случае необходимости инициировать оформление нового Токена к тому же Счету на ином

Мобильном устройстве.

8.3. Клиент обязан:

- соблюдать положения настоящих Условий, в том числе требования к безопасности использования Мобильного устройства, на котором используется Токен;
- в случае утраты Мобильного устройства или несанкционированного использования Токена Клиент может произвести привязку нового Токена и удалить неиспользуемый (утраченный) Токен посредством новой установки МП Банка на личное мобильное устройство, либо обратиться в Банк для блокирования Токенов, содержащихся на утраченном Мобильном устройстве. Уведомление считается полученным в момент подтверждения Банком факта блокирования Токена.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Заключая Соглашение, Клиент понимает и согласен с тем, что:

- получение услуг осуществляется через сеть Интернет, которая является не безопасным каналом связи;
- Банк не несет ответственности за риски, связанные с подключением мобильных устройств Клиента к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет;
- работоспособность СБПЭй (в том числе при совершении Операций СБП) зависит от Провайдера;
- Банк не контролирует и не влияет на предоставление и использование беспроводных сетей связи;
- Банк не гарантирует конфиденциальность и безопасность хранения и передачи данных через сеть Провайдера, которая находится вне контроля Банка.

9.2. Заключая Соглашение, Клиент соглашается с тем, что Банк вправе собирать, использовать и передавать информацию о Клиенте, в том числе информацию, относящуюся к Счету, Токену и совершению Операций СБП, а также обмениваться данной информацией с Провайдером и платежной системой в следующих целях:

- для подтверждения личности Клиента;
- для формирования / блокирования / разблокирования / удаления Токена;
- для передачи / получения информации о совершенных Клиентом Операциях СБП и осуществления по указанным Операциям СБП расчетов;
- для содействия Провайдеру в повышении безопасности и улучшении работы СБПЭй при выполнении своих обязательств и реализации своих прав в соответствии с соглашениями, заключенными с Провайдером и платежной системой. Банк вправе обобщать информацию о Клиентах или делать ее обезличенной;
- для повышения безопасности оказываемых услуг и предотвращения мошенничества;
- по запросам правоохранительных органов, в случаях предусмотренных законодательством РФ.

9.3. Стороны договорились, что все Операции СБП, совершенные с использованием Токена, не могут быть заявлены Клиентом как совершенные без его ведома и согласия и оспорены им как неправомерные, так как совершение Операций СБП указанным способом неуполномоченным Клиентом лицом является следствием нарушения Клиентом настоящих Условий.

9.4. Информация из аппаратно-программных комплексов платежной системы, Банка и Провайдера может использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

9.5. Отношения, возникающие у Клиентов с Провайдером, операторами услуг беспроводной связи, а также иными лицами, оказывающими услуги, доступные посредством использования СБПЭй, регулируются отдельными и самостоятельными соглашениями.

9.6. Во всем, что не предусмотрено настоящими Условиями (в том числе, в части осуществления расчетов по Операциям СБП, взимания Банком комиссий, предусмотренных Договором), Банк и Клиент руководствуются положениями Договора, а также законодательством Российской Федерации.