СОГЛАШЕНИЕ

о расчетном обслуживании с использованием системы

дистанционного банковского обслуживания “Банк+”

г. Казань «___»_____201__г.

«Банк Заречье» (Акционерное общество), именуемый в дальнейшем «БАНК», в лице _____ _____ с одной стороны, и

_____
(полное наименование юридического лица
_____, именуемое (-ый) в дальнейшем «КЛИЕНТ»,
или индивидуального предпринимателя)
в лице _____, действующего на основании
(должностное лицо юридического лица)
_____, с другой стороны, совместно именуемые «Стороны»,
(основание полномочий)
заключили настоящее соглашение о расчетном обслуживании с использованием системы дистанционного банковского обслуживания “Банк+” (далее по тексту – «соглашение») о нижеследующем:

1. Предмет соглашения

1.1. Настоящее соглашение устанавливает порядок предоставления КЛИЕНТОМ БАНКУ документов в электронном виде (далее по тексту – «электронные документы»), которые формируются, подписываются электронной цифровой подписью и передаются в БАНК с использованием системы дистанционного банковского обслуживания «Банк+» (далее по тексту – «Система»).

Стороны установили, что настоящее соглашение распространяется на правоотношения Сторон, возникшие из договоров на расчётное и кассовое обслуживание (в рублях и иностранной валюте), заключенных между Сторонами как до момента подписания настоящего соглашения, так и в период его действия (далее по тексту – «договоры банковского счета»).

1.2. Электронные документы, формируемые с использованием Системы, по своей юридической силе тождественны расчетным документам, составленным в письменной форме, и являются основанием для проведения операций по счету КЛИЕНТА при условии, если электронные документы:

- надлежащим образом оформлены в соответствии с требованиями законодательства и банковских правил;
- заверены электронными цифровыми подписями лиц, уполномоченных распоряжаться денежными средствами, находящимися на соответствующем счете КЛИЕНТА в БАНКЕ;
- переданы КЛИЕНТОМ и получены БАНКОМ;
- проверены на соответствие и приняты ответственным специалистом БАНКА к исполнению.

1.3. Стороны признают, что используемая Система является достаточной для обеспечения надежной и эффективной работы при передаче, приеме, обработке и хранении информации, а система защиты, обеспечивающая разграничение доступа, шифрование, контроль целостности и соответствия электронной цифровой подписи, является достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, а также для разрешения спорных ситуаций.

1.4. Стороны уведомлены о том, что в целях обеспечения безопасной работы в Системе при первом запуске клиентской части Системы программное обеспечение определяет и регистрирует уникальный идентификатор компьютера КЛИЕНТА. При последующих запусках Системы программное обеспечение проверяет текущий уникальный идентификатор компьютера КЛИЕНТА на соответствие идентификатору, зарегистрированному при первом запуске системы. В случае несовпадения идентификаторов доступ в Систему блокируется. Для смены идентификатора компьютера, с которого разрешен доступ в Систему, КЛИЕНТУ необходимо обратиться в БАНК. Для работы в Системе с других компьютеров КЛИЕНТУ также необходимо обратиться в БАНК. В случае обращения КЛИЕНТА в БАНК по телефону (в этом и в иных случаях) идентификация КЛИЕНТА осуществляется по кодовому слову. Кодовое слово указывается КЛИЕНТОМ в момент заключения настоящего соглашения в Регистрационной карточке клиента для подключения к Системе «Банк+» (**Приложение №1** к настоящему Соглашению**)**.

1.5. В целях безопасности проведения платежей КЛИЕНТУ может быть подключён сервис SMS-информирования. Для подключения к сервису SMS-информирования КЛИЕНТ должен проставить соответствующую отметку в Регистрационной карточке КЛИЕНТА для подключения к Системе «Банк+» (**Приложение №1** к настоящему Соглашению) и указать номер телефона, который будет использоваться БАНКОМ для SMS-информирования КЛИЕНТА. В рамках сервиса SMS-информирования Банком осуществляется оповещение КЛИЕНТА о фактах передачи в БАНК платёжных документов, файлов информационного характера и о входе КЛИЕНТА в Систему.

1.6. По письменному заявлению КЛИЕНТА, подписанного полномочным представителем КЛИЕНТА переданного Банку через сотрудника, обслуживающего счёт могут быть установлены параметры операций, проводимых в Системе (Приложение №5 к Соглашению). В целях выявления фальсифицированных электронных сообщений, поступивших через Систему, Банк вправе совершить телефонный звонок Клиенту для уточнения реквизитов распоряжения. При отрицательном результате проверки установленных КЛИЕНТОМ параметров операций, проводимых в Системе, Система не принимает распоряжение КЛИЕНТА в обработку и уведомляет об этом КЛИЕНТА в установленный законодательством РФ срок.

1.7. Перечень банковских счетов КЛИЕНТА, обслуживаемых с использованием Системы на момент заключения настоящего Соглашения, приведен в Регистрационной карточке клиента для подключения к Системе

«Банк+» (**Приложение №1** к настоящему Соглашению). При необходимости КЛИЕНТ может обратиться в БАНК с целью подключения/отключения открытых в БАНКЕ счетов к Системе.

1.8. БАНК приостанавливает (блокирует) работу КЛИЕНТА в Системе при неуплате КЛИЕНТОМ стоимости предоставленного КЛИЕНТУ программного обеспечения и услуг БАНКА по сопровождению Системы за текущий месяц; замены подписи и (или) изменения фамилии, имени, отчества лица, указанного в карточке с образцами подписей и оттиска печати; утрате, хищении или возникновении у КЛИЕНТА подозрений на несанкционированный доступ к секретным ключам КЛИЕНТА или клиентской части программного обеспечения; утрате КЛИЕНТОМ паролей доступа к секретным ключам.

Возобновление расчетного обслуживания с использованием Системы осуществляется БАНКОМ после оплаты КЛИЕНТОМ стоимости предоставленного КЛИЕНТУ программного обеспечения и услуг БАНКА по сопровождению Системы, генерации ключей и совершения БАНКОМ действий, предусмотренных подпунктом 2.1.2. пункта 2.1. настоящего Соглашения.

1.9. Использование КЛИЕНТОМ Системы может быть приостановлено или прекращено БАНКОМ на основании полученного от КЛИЕНТА уведомления или по инициативе БАНКА при нарушении КЛИЕНТОМ порядка использования СИСТЕМЫ в соответствии с настоящим договором.

1.10. Приостановление или прекращение использования КЛИЕНТОМ Системы не прекращает обязательств КЛИЕНТА и БАНКА, возникших до момента приостановления или прекращения указанного использования.

1.11. Стороны подтверждают, что до заключения настоящего Соглашения БАНК проинформировал КЛИЕНТА об условиях использования Системы, в том числе о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы.

2. Обязанности Сторон

2.1. БАНК обязуется:

2.1.1. Предоставить уполномоченному представителю КЛИЕНТА программное обеспечение клиентской части Системы, которое позволяет осуществлять:

- формирование электронных документов с соблюдением всех требований, установленных действующим законодательством и банковскими правилами, включая нормативные акты Центрального банка Российской Федерации;
- проставление в электронных документах электронных цифровых подписей лиц, уполномоченных распоряжаться денежными средствами, находящимися на соответствующем счете КЛИЕНТА в БАНКЕ;
- передачу электронных документов по электронным каналам связи в БАНК и хранение электронных документов в банковской части Системы;
- доступ к электронным документам, сформированным БАНКОМ для КЛИЕНТА и помещенным в базу данных банковской части Системы;

2.1.2. Зарегистрировать карточку открытого ключа КЛИЕНТА, заверенную собственноручными подписями уполномоченных лиц. Порядок генерации ключей описан в инструкции, передаваемой уполномоченному представителю КЛИЕНТА вместе с программным обеспечением клиентской части Системы. Форма Карточки открытого ключа приведена в **Приложении №2** к настоящему Соглашению.

БАНК исполняет обязанности, указанные в подп.2.1.1 п.2.1 настоящего Соглашения, в течение 10 (десяти) рабочих дней, следующих за днем его заключения Сторонами.

2.1.3. Консультировать сотрудников КЛИЕНТА, осуществляющих формирование электронных документов и работающих с предоставленным программным обеспечением, по всем вопросам его использования.

2.1.4. Производить регистрацию в Системе новых открытых ключей КЛИЕНТА при их утрате, хищении или возникновении подозрений на несанкционированный доступ к действующим секретным ключам КЛИЕНТА или клиентской части программного обеспечения.

2.1.5. Исполнять принятые БАНКОМ электронные документы в пределах имеющегося на момент их поступления в БАНК остатка денежных средств на соответствующем счете КЛИЕНТА в следующие сроки:

<u>по электронным расчетным документам в рублях Российской Федерации:</u>

- в течение текущего операционного дня, если они поступили в БАНК до 15 часов 00 минут московского времени (данное условие действует для БАНКА, его допофисов, филиалов и их внутренних структурных подразделений);
- в течение следующего операционного дня, если они поступили в БАНК в 15 часов 00 минут московского времени и позднее (данное условие действует для БАНКА, его допофисов, филиалов и их внутренних структурных подразделений);

<u>по электронным расчетным документам в долларах США:</u>

по текущим расчетам

- в течение текущего операционного дня, если они поступили в БАНК до 14 часов 00 минут московского времени (для допофисов, филиалов БАНКА и их внутренних структурных подразделений – до 13 часов 45 минут московского времени);
- в течение следующего операционного дня, если они поступили в БАНК в 14 часов 00 минут московского времени и позднее (для допофисов, филиалов БАНКА и их внутренних структурных подразделений – в 13 часов 45 минут московского времени и позднее);

<u>по электронным расчетным документам в Евро и других иностранных валютах:</u>

по текущим расчетам

- в течение текущего операционного дня, если они поступили в БАНК до 14 часов 00 минут московского времени (для допофисов, филиалов БАНКА и их внутренних структурных подразделений – до 13 часов 45 минут московского времени);
- в течение следующего операционного дня, если они поступили в БАНК в 14 часов 00 минут московского времени и позднее (для допофисов, филиалов БАНКА и их внутренних структурных подразделений – в 13 часов 45 минут московского времени и позднее).

Другие электронные документы считаются принятыми в работу специалистом, обслуживающим счёт, специалистом Отдела учёта ценных бумаг и валютных операций учётно-операционного управления Банка, специалистом валютного контроля Банка/филиала соответственно:

- текущим рабочим днём, если электронный документ поступил в Банк до 16 часов 00 минут московского времени (в ВСП/филиал Банка – до 15 часов 45 минут московского времени);
- следующим рабочим днём, если электронный документ поступил в Банк в 16 часов 00 минут московского времени и позднее (в ВСП/филиал Банка – в 15 часов 45 минут московского времени и позднее).

2.1.6. Предоставить КЛИЕНТУ возможность получения электронной выписки о проведенных по счету операциях.

2.1.7. Обеспечить защиту банковской части Системы от несанкционированного доступа, сохранять банковскую тайну о счетах и об операциях КЛИЕНТА и не разглашать указанные сведения третьим лицам за исключением случаев, предусмотренных действующим законодательством.

2.1.8. Сообщать КЛИЕНТУ об обнаружении попытки несанкционированного доступа к Системе, если это затрагивает счета и операции КЛИЕНТА, в течение 1 (одного) рабочего дня с момента обнаружения указанного факта.

2.1.9. Информировать КЛИЕНТА о совершении КЛИЕНТОМ каждой операции с использованием Системы путем направления КЛИЕНТУ уведомления. Уведомления направляются посредством Системы и отражаются в разделе «Уведомления о переданных в банк документах» Системы. Уведомление считается полученным КЛИЕНТОМ в день направления уведомления БАНКОМ.

2.1.10. Передавать КЛИЕНТУ по Системе и/или нарочно документы и информацию, связанную с расчетным обслуживанием с использованием Системы.

2.1.11. Рассматривать заявления КЛИЕНТА, связанные с расчетным обслуживанием с использованием Системы, в течение 30 (тридцати) календарных дней со дня поступления заявления в БАНК, а в случае поступления заявления, связанного с расчетным обслуживанием с использованием Системы для осуществления трансграничного перевода денежных средств, – в течение 60 (шестидесяти) календарных дней. Ответы на заявления КЛИЕНТА направляются БАНКОМ через Систему. Если КЛИЕНТ в заявлении потребовал ответить в письменной форме на заявление, БАНК направляет письменный ответ на заявление по адресу я КЛИЕНТА, указанному в настоящем Соглашении.

2.1.12. По заявлению КЛИЕНТА возместить ему сумму операции, совершенную без согласия КЛИЕНТА после получения уведомления в порядке, установленном подп.2.3.13 п.2.3 настоящего Соглашения. Сумма операции не возмещается БАНКОМ в том случае, если БАНК исполнил обязанность, предусмотренную подп.2.1.9 п.2.1 настоящего Соглашения, а КЛИЕНТ не исполнил обязанность, предусмотренную подп.2.3.13 п.2.3 настоящего Соглашения.

2.2. БАНК вправе:

2.2.1. До момента осуществления операции по счету (счетам) КЛИЕНТА потребовать от последнего представления расчетных документов, составленных в письменной форме в случае, если у БАНКА возникли какие-либо подозрения (сомнения) в отношении полученных электронных документов (их подлинности, отправки самим КЛИЕНТОМ и др.);

2.2.2. Производить опрос и разъяснительные беседы с КЛИЕНТОМ для определения уровня риска, возникающего при расчетном обслуживании с использованием Системы.

2.2.3. Расторгнуть настоящее Соглашение, если присвоенный КЛИЕНТУ уровень риска, влечет за собой использование Системы с ненадлежащим уровнем информационной безопасности деятельности КЛИЕНТА, связанной с работой в Системе.

2.3. КЛИЕНТ обязуется:

2.3.1. Передавать в БАНК надлежащим образом оформленные документы и на следующий рабочий день, после проведения операции, с использованием Системы получать из БАНКА выписки по счету за предыдущий рабочий день, подтверждающие прохождение платёжных документов КЛИЕНТА в БАНКЕ.

2.3.2. Обеспечить выполнение требований по обеспечению информационной безопасности при работе в Системе «Банк+» и следовать всем рекомендациям БАНКА при комплектации рабочего места Системы аппаратными и программными средствами (**Приложение №6** к настоящему Соглашению).

2.3.3. Ответственно относиться к программному обеспечению, полученному от БАНКА на время действия настоящего Соглашения, и эксплуатировать его согласно предоставленному руководству пользователя.

2.3.4. Производить копирование предоставленного БАНКОМ программного обеспечения только в целях создания резервных копий для восстановления Системы.

2.3.5. В случае сбоев и иных технических неполадок программного обеспечения передавать в БАНК расчетные документы и иные документы в обычном порядке, предусмотренном соответствующим договором банковского счета.

2.3.6. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность несанкционированного использования, взлома, модификации, копирования и перенастройки программного обеспечения, предоставленного БАНКОМ, а также возможность использования паролей доступа и ключей для формирования электронных цифровых подписей.

2.3.7. В случае утраты, хищения, в том числе осуществления операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента или несанкционированного доступа к ключам и паролям, изменения целостности программного обеспечения немедленно проинформировать БАНК и прекратить работу с Системой до момента ее возобновления в согласованном с БАНКОМ порядке.

2.3.8. Контролировать правильность оформления всех необходимых реквизитов своих электронных документов, соответствие суммы платежа и остатка на соответствующем счете в БАНКЕ и осуществлять платежи только в пределах этого остатка, если иное не предусмотрено соглашением Сторон.

2.3.9. Не менее чем за 1 (один) рабочий день до смены номера телефона, используемого БАНКОМ для SMS-информирования КЛИЕНТА, письменно уведомлять об этом БАНК.

2.3.10. До момента установки клиентской части Системы произвести подключение, настройку и проверку всех необходимых аппаратных и программных средств (компьютер, коммуникационное оборудование, подключение к сети Интернет), которые будут использоваться для осуществления связи с БАНКОМ.

2.3.11. Предоставлять необходимую информацию, участвовать в разъяснительных беседах, опросе, проводимых БАНКОМ, позволяющих определить уровень информационной безопасности деятельности КЛИЕНТА, связанной с работой в Системе.

2.3.12. Ежедневно заходить в Систему и проверять наличие или отсутствие уведомлений БАНКА о совершенных КЛИЕНТОМ операциях с использованием Системы.

2.3.13. В случае утраты Системы по каким-либо причинам или использовании Системы без согласия КЛИЕНТА, незамедлительно после обнаружения факта утраты Системы и (или) её использования без согласия КЛИЕНТА, но не позднее дня, следующего за днем получения от БАНКА уведомления о совершенной операции, сообщить об этом БАНКУ, одним из следующих способов:

1) в рабочие дни с 8 часов 00 минут до 17 часов 00 минут (обед с 12 часов 30 минут до 13 часов 30 минут) телефонограммой по одному из следующих телефонов: (843) 557-59-88, 557-59-74 с обязательным указанием кодового слова;

2) путем направления в любое время (24 часа в сутки 7 дней в неделю) на адрес электронной почты: dbo@zarech.ru уведомления (**Приложение №3** к настоящему Соглашению);

3) путем передачи оригинала уведомления (**Приложение №3** к настоящему Соглашению) нарочно специалисту, обслуживающему счет;

4) путем направления оригинала уведомления заказным письмом по адресу: 420032, г.Казань, ул.Лукницкого, д.2.

После направления уведомления в порядке, указанном в литерах 1 - 2 настоящего подпункта КЛИЕНТ обязан в течение 3 (трех) календарных дней передать оригинал уведомления одним из способов, указанных в литерах 3 - 4 настоящего подпункта.

5) В течение 3 (трех) рабочих дней, следующих за днем, когда БАНКУ станет известно о том, что КЛИЕНТ не направлял уведомление об утрате Системы или использовании Системы без согласия КЛИЕНТА, написать заявление в свободной письменной форме о том, что КЛИЕНТ не направлял уведомление БАНКУ.

2.3.14. Незамедлительно инициировать перегенерацию ключей электронно-цифровой подписи в случае смены лиц, уполномоченных распоряжаться денежными средствами, находящимися на соответствующем счете КЛИЕНТА в БАНКЕ.

2.4. КЛИЕНТ вправе:

2.4.1. Направлять в адрес БАНКА заявления по вопросам, расчетного обслуживания с использованием Системы одним из следующих способов:

1) нарочно, специалисту обслуживающему счет;

2) путем направления заказного письма по адресу: 420032, г.Казань, ул.Лукницкого, д.2;

3) на адрес электронной почты: dbo@zarech.ru;

2.4.2. Требовать от БАНКА ответа на заявление в письменной форме в сроки, указанные в подп.2.1.11 п.2.1 настоящего Соглашения.

2.4.3. Требовать от БАНКА возмещения суммы операции, совершенной без согласия КЛИЕНТА, с учетом положений подп.2.1.12 п.2.1 настоящего Соглашения.

3. Ответственность Сторон

3.1. КЛИЕНТ несет полную ответственность за доступ к переданному ему БАНКОМ программному обеспечению, к индивидуальному рабочему месту работника (представителя) КЛИЕНТА, осуществляющего формирование электронных документов с использованием Системы, а также к накопителям (носителям) информации (дискетам, флэш-картам и др.) с записанными на них уникальными секретными ключами для проставления в электронных документах электронных цифровых подписей уполномоченных лиц.

3.2. БАНК не несет ответственности:

1) за сбои в работе Системы по причине изменений, вносимых КЛИЕНТОМ в клиентскую часть переданного ему программного обеспечения (изменение настроек конфигурации, занесение «вирусов» и т.д.), а также вследствие неисправностей в линиях связи;

2) за ошибочно переданные КЛИЕНТОМ электронные документы, если эти документы надлежащим образом оформлены и переданы в БАНК;

3) за правомерность и правильность надлежащим образом оформленных электронных документов, а также за убытки, понесенные КЛИЕНТОМ вследствие отзыва им электронных документов, в случае, если данные электронные документы уже исполнены БАНКОМ, и у БАНКА не имеется возможности отменить их исполнение;

4) за нарушение или ненадлежащее исполнение Клиентом требований по обеспечению информационной безопасности при работе в Системе «Банк+»;

5) за ущерб, возникший вследствие утери или разглашении Клиентом информации, касающейся ключей электронно-цифровой подписи, аутентификационной и идентификационной информации, используемой Клиентом для доступа к Системе «Банк+».

3.3. В случае неисполнения и/или ненадлежащего исполнения КЛИЕНТОМ обязанностей, установленных подп.подп.2.3.6 и 2.3.7 п.2.3 настоящего Соглашения, БАНК имеет право приостановить расчеты с КЛИЕНТОМ с использованием Системы до урегулирования отношений.

3.4. Инициатором сеансов связи с БАНКОМ всегда является КЛИЕНТ. Любая просрочка исполнения БАНКОМ своих обязательств, которая произошла из-за отсутствия инициативы КЛИЕНТА в установлении связи с БАНКОМ, не влечет за собой ответственности БАНКА.

3.5. БАНК несет ответственность за несоблюдение сроков проведения расчетных операций по счету КЛИЕНТА на основании надлежащим образом оформленных и своевременно поступивших электронных документов КЛИЕНТА в соответствии с действующим законодательством и соответствующим договором банковского счета.

3.6. Во всех остальных случаях неисполнения или ненадлежащего исполнения обязательств по настоящему соглашению Стороны несут ответственность в соответствии с законодательством.

3.7. Сторона может быть освобождена от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему соглашению, если докажет, что надлежащее исполнение обязательства оказалось невозможным вследствие возникновения и/или действия обстоятельств непреодолимой силы, а именно: пожаров, наводнений, землетрясений или иных стихийных бедствий,

технологических катастроф, забастовок, террористических актов, массовых беспорядков, войны, военных действий, издания нормативных правовых или иных актов органов государственной власти и управления, препятствующих или делающих невозможным надлежащее исполнение Стороной своих обязательств, и других чрезвычайных и непредотвратимых при данных условиях обстоятельств.

3.8. При наступлении указанных в пункте 3.7 настоящего Соглашения обстоятельств Сторона, для которой возникла невозможность надлежащего исполнения обязательств, обязана при первой возможности составить письменное уведомление о возникновении указанных обстоятельств, подписать его, скрепить оттиском печати и передать другой Стороне по факсу и/или электронной почте с последующим представлением подлинника уведомления с приложением документов, подтверждающих наступление (прекращение) этих обстоятельств.

4. Порядок разрешения споров Сторон

4.1. В случае возникновения споров между Сторонами по предмету настоящего Соглашения совместным решением обеих Сторон создается согласительная экспертная комиссия (далее по тексту – «комиссия») из равного количества представителей от каждой Стороны. Комиссия должна быть создана в течение 7 (семи) календарных дней, следующих за днем получения одной из Сторон письменной претензии от другой Стороны.

4.2. Комиссия рассматривает споры по электронным документам, которые были сформированы и переданы с использованием Системы, не ранее, чем за 35 (тридцать пять) календарных дней до даты поступления письменной претензии от соответствующей Стороны.

4.3. При рассмотрении комиссией спора о подлинности, наличии или отсутствии документа, созданного с использованием Системы или подписанного электронной цифровой подписью, каждая Сторона обязана доказать лишь то, что она своевременно и надлежащим образом исполнила обязанности по настоящему Соглашению.

4.4. Комиссия рассматривает, в частности, споры следующих типов:

а) Сторона-получатель документа утверждает, что получила от Стороны-отправителя корректно подписанные электронные документы, а Сторона-отправитель отрицает факт отправки этих документов. В этом случае Сторона-получатель предъявляет комиссии открытый ключ подписи Стороны-отправителя в электронном виде и файл, содержащий спорные электронные документы, подписанный электронно-цифровой подписью Стороны-отправителя. На специально выделенном компьютере устанавливается программное обеспечение для проверки корректности электронно-цифровой подписи под документами. С помощью программы проверки электронной цифровой подписи проверяется корректность электронной цифровой подписи файла, содержащего оспариваемые электронные документы. В том случае, если корректность электронно-цифровой подписи подтверждается программой, виновной признается Сторона-отправитель документов, в противном случае виновной признается Сторона-получатель документов.

б) Сторона-отправитель документов утверждает, что корректно подписанные ею электронные документы были получены Стороной-получателем, а Сторона-получатель отрицает факт получения этих документов. В этом случае Сторона-отправитель предъявляет комиссии открытый ключ подписи Стороны-получателя в электронном виде и файл, содержащий подтверждение получения электронных документов Стороной-получателем. На специально выделенном компьютере устанавливается программное обеспечение для проверки корректности электронно-цифровой подписи под документами. С помощью программы проверки электронной цифровой подписи проверяется корректность электронной цифровой подписи файла, содержащего подтверждение получения электронных документов. В том случае, если корректность электронно-цифровой подписи подтверждается программой, виновной признается Сторона-получатель документов, в противном случае виновной признается Сторона-отправитель документов.

4.5. Споры Сторон, возникшие в связи с исполнением настоящего соглашения и не урегулированные комиссией, разрешаются арбитражным судом в порядке, установленном действующим законодательством.

5. Срок действия Соглашения и другие условия

5.1. Программное обеспечение, лицензия на право использования средств криптографической защиты информации и техническая документация, необходимая для функционирования Системы, предоставляется КЛИЕНТУ во временное пользование на срок действия настоящего Соглашения и не может быть передано им третьему лицу без предварительного письменного согласия БАНКА.

5.2. Каждая из Сторон при подписании электронных документов электронными цифровыми подписями применяет свои секретные ключи, а при проверке подписей – открытые ключи другой Стороны, являющиеся действующими на момент подписания и передачи данного документа.

5.3. Оплата стоимости предоставленного КЛИЕНТУ программного обеспечения и услуг БАНКА по сопровождению Системы производится КЛИЕНТОМ в соответствии с установленными БАНКОМ Тарифами на расчетное и кассовое обслуживание юридических лиц и индивидуальных предпринимателей. Порядок расчетов регулируется соответствующими договорами банковского счета, заключенными между БАНКОМ и КЛИЕНТОМ.

5.4. Настоящее Соглашение вступает в силу (считается заключенным) с момента его подписания Сторонами (их полномочными представителями) со скреплением оттисками круглых печатей Сторон и действует до момента прекращения всех договоров банковского счета (в российских рублях и иностранной валюте), заключенных между Сторонами как до момента подписания настоящего Соглашения, так и в период его действия, если иное не предусмотрено Соглашением Сторон.

Действие настоящего Соглашения не распространяется на правоотношения Сторон, возникшие из отдельного договора банковского счета (в российских рублях или в иностранной валюте) в случае достижения Сторонами об этом взаимного согласия. В этом случае Стороны заключают дополнительное соглашение к настоящему Соглашению, обмениваются письмами или иными документами, в которых однозначно выражено намерение Сторон, направленное на нераспространение действия настоящего Соглашения на правоотношения Сторон по соответствующему договору банковского счета.

В случае распространения действия настоящего Соглашения на правоотношения Сторон, возникшие из отдельного договора банковского счета (в российских рублях или в иностранной валюте), заключенного в период действия настоящего Соглашения, настройка БАНКОМ программного обеспечения клиентской части Системы осуществляется исключительно по заявлению КЛИЕНТА, представленному в БАНК в письменной форме.

5.5. Настоящее Соглашение может быть изменено, дополнено или прекращено до истечения срока его действия по соглашению Сторон, за исключением случаев, предусмотренных действующим законодательством.

Все изменения и дополнения к настоящему Соглашению (за исключением изменений размера абонентской платы за предоставление и сопровождение программного обеспечения Системы) считаются действительными, если они выполнены в письменной форме, подписаны Сторонами (их полномочными представителями) и скреплены оттисками круглых печатей Сторон.

Изменения и/или дополнения в настоящее Соглашение в части размера абонентской платы за предоставление и сопровождение программного обеспечения Системы могут быть внесены БАНКОМ в одностороннем порядке следующим образом. Информация о вносимых в настоящее Соглашение изменениях и/или дополнениях доводится БАНКОМ до КЛИЕНТА путем ее размещения на информационных стендах в помещениях БАНКА или его внутренних структурных подразделениях, в помещении филиала БАНКА и внутренних структурных подразделениях филиала. При непоступлении от КЛИЕНТА возражений на вносимые в Соглашение изменения (дополнения) в течение 15 (пятнадцати) операционных дней, следующих за днем размещения информации на стендах, изменения (дополнения) считаются принятыми КЛИЕНТОМ и являются неотъемлемой частью Соглашения.

5.6. Настоящее Соглашение может быть расторгнуто по заявлению одной из Сторон, оформленному письменно и направленному другой Стороне не менее, чем за 5 (пять) календарных дней до даты расторжения. В случае соблюдения срока направления заявления, настоящее Соглашение считается расторгнутым с даты, указанной в заявлении Стороны, в противном случае настоящее Соглашение считается расторгнутым по истечении 5 (пяти) календарных дней, следующих за днем получения Стороной заявления другой Стороны о расторжении Соглашения.

При этом если инициатором расторжения является БАНК, то с даты, указанной в его заявлении, БАНК прекращает принимать от КЛИЕНТА электронные документы и проводит операции по счету КЛИЕНТА только на основании документов в письменной форме в обычном порядке, предусмотренном соответствующим договором банковского счета.

5.7. Условия настоящего Соглашения являются конфиденциальными и составляют коммерческую тайну Сторон. Каждая из Сторон обязуется не предоставлять информацию о них третьему лицу (лицам) без предварительного письменного согласия другой Стороны за исключением случаев, предусмотренных законодательством и письменным соглашением Сторон.

5.8. Взаимоотношения Сторон, не урегулированные в настоящем Соглашении, регулируются действующим законодательством и соответствующим договором банковского счета.

5.9. Стороны установили, что с момента вступления в силу настоящего Соглашения все ранее заключенные между Сторонами договоры (дополнительные соглашения к договору на расчетное и кассовое обслуживание), имеющие тот же предмет, прекращают свое действие.

5.10.При прекращении действия настоящего Соглашения, в том числе в случае его расторжения, КЛИЕНТ обязан вернуть Банку по Акту приема-передачи программное обеспечение, лицензию на право использования средств криптографической защиты информации и техническую документацию, необходимую для функционирования Системы, полученные им в соответствии с п. 5.1. настоящего Соглашения в течение 1 (одного) рабочего дня с момента прекращения действия настоящего Соглашения.

5.11. Настоящее Соглашение составлено в 2 (двух) идентичных экземплярах, имеющих одинаковую юридическую силу, один из которых передается КЛИЕНТУ, а второй – остается у БАНКА.

Приложения №№1 – 6 являются неотъемлемой частью настоящего Соглашения.

6. Местонахождение и реквизиты Сторон

БАНК:	**КЛИЕНТ:**
«Банк Заречье» (АО); ОГРН 1021600000586, ИНН 1653016664;	_____ОГРН:__ _____, ИНН_____
420032, г. Казань, ул. Лукницкого, 2;	местонахождение:_____
к/счет № 30101810900000000772	р/счет № _____
в Отделении - НБ Республика Татарстан;	в банке:_____
БИК 049205772.	БИК_____

7. Подписи Сторон

От БАНКА:	**От КЛИЕНТА:**
_____	_____
_____/_____/	_____/_____/
м.п.	м.п.
Главный бухгалтер	Главный бухгалтер
_____/Н.Н. Архипович/	_____/_____/

Приложение № 1
к Соглашению о расчетном обслуживании
с использованием Системы «Банк+»

РЕГИСТРАЦИОННАЯ КАРТОЧКА КЛИЕНТА
для подключения к Системе «Банк+»

Наименование КЛИЕНТА	
Кодовое слово	

☐ Подключить сервис SMS-информирования[1].

Для направления SMS-сообщений просим Банк использовать номер мобильного телефона:

Номер телефона (указывается в международном формате, с кодом страны, например: 79061234567)	**Ф.И.О. владельца телефона**

Перечень счетов КЛИЕНТА, обслуживаемых в Системе «Банк+»

№ п\п	Номер счёта:	Полный доступ к счёту	Получение информации по счёту
1.		☐	☐
2.		☐	☐
3.		☐	☐
4.		☐	☐
5.		☐	☐

Просим предоставить доступ для работы в Системе следующим лицам:

№ п\п	Ф.И.О. (полностью) пользователей Системы[2]	Роль в Системе *(подпись, пользователь)*	Номер логин-конверта *(заполняется сотрудником Банка)*
1.			
2.			
3.			
4.			
5.			

Средства аутентификации (логин-конверты) получены.

КЛИЕНТ: _____ (_____) «____» _____ 20___г.
подпись уполномоченного лица *Ф.И.О.*

Заполняется Банком

Документы приняты в ВСП Банка _____
в _____ часов _____ минут «____»_____ 20___г.

Специалист, обслуживающий счет: _____ (_____)

[1] При подключении сервиса SMS-информирования осуществляется оповещение клиента о фактах передачи в банк платёжных документов, файлов информационного характера и о входе клиента в Систему.
[2] Лица, указанные в карточке с образцами подписей и оттиска печати, а также лица, действующие от имени КЛИЕНТА на основании доверенности по представлению интересов КЛИЕНТА во взаимоотношениях с Банком.

Приложение № 2
к Соглашению о расчетном обслуживании
с использованием Системы «Банк+»

КАРТОЧКА ОТКРЫТОГО КЛЮЧА

Владелец:

Организация:

Тип подписи:

Дата создания: Начало действия:
Окончание действия:
Тип ключа:

Открытый ключ:

Содержание открытого ключа

Владелец ключа: Дата _____.

_____/_____/

Представитель БАНКА ключ принял: Дата _____.

_____/_____/

Приложение № 3
к Соглашению о расчетном обслуживании
с использованием Системы «Банк+»

Уведомление Клиента об утрате системы дистанционного банковского обслуживания «Банк+» или проведения операции с использованием Системы без согласия Клиента

_____
(наименование организации, Ф.И. О. Индивидуального предпринимателя, ИНН, номер расчетного счета)

в лице _____,

действующей (-го) на основании _____
(наименование и реквизиты документа)

сообщает, что _____
(причина направления уведомления)

_____

_____

_____

_____ _____/_____
(дата) (подпись, расшифровка подписи)

Приложение № 4
к Соглашению о расчетном обслуживании
с использованием Системы «Банк+»

АКТ № _____

приема-передачи лицензии на право использования средств криптографической защиты информации, к Соглашению от _____

г. Казань «___» _____ 201_г.

Мы, нижеподписавшиеся, «Банк Заречье» (АО) в лице _____
_____,
действующего на основании _____,
(далее – Банк), с одной стороны, и
Клиент в лице _____
_____,
(должность, фамилия, имя, отчество (полностью) руководителя организации (филиала организации))

действующего на основании _____
_____,
(наименование учредительного документа, номер, дата, при наличии доверенности дата, номер (если присвоен))
с другой стороны, составили настоящий Акт о том, что Банк передал, а Клиент принял 1 (одну) лицензию на право использования СКЗИ «КриптоПро CSP» версии 3.6 на одном рабочем месте MS Windows.

Подписи Сторон

От БАНКА:	**От КЛИЕНТА:**
_____	_____
_____	_____
_____	_____
_____ _____	_____ _____
(подпись, расшифровка подписи)	*(подпись, расшифровка подписи)*
«____» _____ 201_г.	«____» _____ 201_г.
М.П.	М.П.

Приложение № 5

к Соглашению о расчетном обслуживании

с использованием Системы «Банк+»

Председателю Правления «Банка Заречье» (АО)

Н.В. Девятых

_____

наименование клиента

ЗАЯВЛЕНИЕ

Клиент просит « Банк Заречье» (АО) установить следующие параметры операций, проводимых в Системе «Банк+» начиная со следующего рабочего дня после даты приема Заявления:

	виды параметров операций	**условие**
☐	максимальная сумма перевода денежных средств с использованием Системы за одну операцию и (или) за определенный период времени (день/месяц) в рублях	Максимальная сумма за одну операцию: _____ Максимальная сумма за один операционный день: _____ Максимальная сумма за текущий календарный месяц: _____
☐	получатели денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием Системы либо БИК (банка-получателя) и лицевой счет получателя (20 знаков) и ИНН, либо БИК (банка-получателя) и лицевой счет получателя (20 знаков), либо ИНН	_____ _____
☐	временной период, в который могут быть переданы документы в Банк с использованием Системы по операциям в рублях и иностранной валюте (доллары США/Евро)[3]	С 8.00 до 17.00 (рабочие дни)

Клиент уведомлен, что при отрицательном результате проверки установленных КЛИЕНТОМ параметров операций, проводимых в Системе, Система не принимает распоряжение КЛИЕНТА в обработку

КЛИЕНТ: _____ (_____) «____» _____ 20___г.

подпись уполномоченного лица *Ф.И.О.*

[3] В случае если КЛИЕНТ не выбрал данный пункт документы с помощью Системы могут быть направлены в БАНК круглосуточно.

Приложение № 6

к Соглашению о расчетном обслуживании

с использованием Системы «Банк+»

Риски клиентов при работе в системе дистанционного банковского обслуживания «Банк+» (далее – «Система»)

За последнее время в ряде российских банков участились случаи хищения денежных средств с расчетных счетов корпоративных клиентов путем совершения платежей с использованием системы дистанционного банковского обслуживания.

Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

1. как работающими, так и уволенными ответственными сотрудниками предприятия, имевшими доступ к паролю доступа, секретным ключам, к компьютерам, с которых осуществлялась работа по системе дистанционного банковского обслуживания;
2. как работающими, так и уволенными ИТ-сотрудниками организации, а так же нештатными, приходящими по вызову, ИТ-специалистами, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютерах, с которых осуществляется работа по системе дистанционного банковского обслуживания;
3. злоумышленниками путем заражения вредоносными программами компьютеров клиентов в связи с уязвимостью системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением секретных ключей и паролей.

Как правило, действия злоумышленников направлены:

1. на похищение секретных ключей;
2. на похищение паролей доступа к Системе;
3. на передачу в банк электронных платежных документов, заверенных похищенным ключом.

Документы, направляемые злоумышленниками с использованием действующих секретных ключей клиентов, могут не вызывать подозрений у сотрудников банков, поскольку такие документы имеют корректную электронную подпись, вполне обычные реквизиты получателей и типовое назначение платежа. Благодаря этому, полученные платежные документы признаются банками поступившими от клиента – владельца расчетного счета, и банки обязаны их исполнять. Таким образом происходит хищение злоумышленниками денежных средств с расчетных счетов клиентов. **При этом вся ответственность за убытки безусловно и полностью возлагается на клиентов как единственных владельцев секретных ключей.**

В целях повышения безопасности при работе с системой дистанционного банковского обслуживания «Банк+» АКБ «Заречье» (ОАО) представляет комплекс требований и рекомендаций, выполнение которых позволит снизить указанные выше риски при работе в Системе.

Требования по обеспечению информационной безопасности при работе в Системе «Банк+»

В целях обеспечения информационной безопасности при работе в Системе Клиент наделяется следующими обязанностями:

1. Разрешено использовать программное обеспечение системы ДБО «Банк+» только скачанное с официального сайта «Банка Заречье» (АО) (www.zarech.ru).

2. Ключи электронной подписи (далее по тексту – ЭП) разрешено хранить только на внешнем носителе информации в недоступном для посторонних лиц месте (персональный сейф, металлический шкаф). Запрещено копирование ключей ЭП на жесткий диск компьютера, с которого осуществляется работа в Системе «Банк+».

3. Запрещено использовать в качестве пароля:

- последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
- последовательности повторяющихся букв или цифр;
- идущие подряд в раскладке клавиатуры или в алфавите символы;
- имена и фамилии;
- ИНН или другие реквизиты клиента.

4. Пароль должен:

- быть не менее 6 символов;
- содержать цифры, строчные и заглавные буквы;
- содержать хотя бы 1 символ, не являющийся буквой или цифрой.

5. Пароль пользователя в операционной системе, а также в системе ДБО «Банк+» необходимо менять не реже одного раза в квартал.

6. Пароль доступа к ключу ЭП необходимо хранить отдельно от ключа ЭП. Запрещено записывать пароль доступа к секретному ключу на этикетке внешнего носителя.

7. Разрешено подключать внешний носитель, содержащий ключ ЭП, только в момент подписания электронных документов. Запрещено оставлять внешний носитель, содержащий ключ ЭП, постоянно подключенным к компьютеру.

8. Использовать внешний носитель, содержащий ключ ЭП, только для подписания электронных документов.

9. Запрещено использовать внешний носитель, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с системой ДБО «Банк+».

10. Запрещено копировать содержимое внешнего носителя, содержащего ключ ЭП, и не передавать его никому даже на короткое время.

11. Закончив работу в системе ДБО «Банк+» или прервав её (даже на несколько минут), необходимо извлечь внешний носитель, содержащий ключ ЭП, и убрать его в недоступное другим лицам место.

12. Необходимо применять на рабочем месте средства защиты от вредоносного кода, позволяющее блокирование несанкционированного удаленного доступа к компьютеру по сети Интернет, с возможностью автоматического обновления баз данных сигнатур вредоносного кода.

13. Необходимо своевременно обновлять ПО системы ДБО «Банк+». Обновление системы ДБО «Банк+» разрешено через меню системы ДБО «Банк+» («Операции» - «Обновление программы»).

14. Запрещается работать с системой ДБО «Банк+» с компьютеров, которые располагаются в общественных местах (Интернет-кафе, салонах, киосках и т.д.).

15. Необходимо осуществлять постоянный контроль отправляемых платежных документов при работе с системой ДБО «Банк+», а также за состоянием своего расчетного (банковского) счета.

16. В случае выявления признаков компрометации ключей ЭП или выявления вредоносного кода в компьютере, используемом для работы в системе ДБО «Банк+», необходимо немедленно извлечь ключ ЭП, выключить компьютер и уведомить Банк по телефонам: **(843) 557-59-74, (843) 557-59-88 с 8 часов 00 минут до 17 часов 00 минут (в рабочие дни)**, либо лично явиться в Банк с целью блокирования скомпрометированных закрытых ключей ЭП с последующей их заменой.

17. К событиям, связанным с компрометацией ключей ЭП, в том числе, относятся:

- утеря (утрата) носителя ЭП, в том числе, с последующим его обнаружением;
- обнаружение факта или угрозы использования (копирования) ключей ЭП и/или пароля доступа к ключам ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе системы ДБО «Банк+», в том числе, возникающих в связи с попытками нарушения информационной безопасности;
- увольнение ответственного сотрудника, имевшего доступ к закрытому ключу ЭП ДБО «Банк+».

18. Необходимо блокировать встроенные локальные учетные записи «Администратор» и «Гость» в операционной системе Windows.

19. При обнаружении несанкционированных платежных операций или утрате системы ДБО «Банк+» немедленно проинформировать руководство, обязательно уведомить Банк и написать уведомление об утрате Системы или использовании Системы без согласия Клиента в порядке, установленном Соглашением о расчетном обслуживании с использованием системы дистанционного банковского обслуживания “Банк+”, а также обратиться с соответствующим заявлением в правоохранительные органы.

20. Запрещено восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с системой ДБО «Банк+» разрешено проводить только на новом компьютере после смены всех ключей ЭП клиента.

21. Необходимо отключить службу «Telnet» и её автоматический запуск операционной системе Windows.

22. Необходимо использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.

23. Необходимо отключить возможность терминального соединения к компьютерам, используемым для работы в Системе, заблокировать 3389 (RDP Remote desktop). Запрещено использование сторонних приложений, позволяющих осуществление удаленного доступа к компьютерам, используемым для работы по Системе (таких как ‘Team Viewer’, ‘Radmin’ и т.п.).

24. Необходимо включить в операционной системе журнал безопасности Windows.

25. Разрешено использовать подключение к сети Интернет на компьютерах, используемых для работы в Системе, исключительно для работы в Системе. Необходимо запретить доступ к социальным сетям и развлекательным ресурсам сети Интернет.

Помимо указанных выше требований рекомендуется также:

1. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).

2. Обеспечить возможность своевременного обновления системного и прикладного ПО.

3. Выделить стационарный компьютер только для работы с системой ДБО «Банк+».

4. Доступ в помещение, где размещен компьютер с системой ДБО «Банк+», рекомендуется предоставлять только уполномоченным лицам.

5. Компьютер, с которого осуществляется подготовка и отправка электронных документов в Банк, рекомендуется выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети клиента Банка.

6. С целью обеспечения безопасности платежей рекомендуется использовать услугу SMS–информирования.

7. Исключить доступ к компьютерам, используемым для работы по Системе, посторонним лицам и персоналу предприятия, не уполномоченному на работу по Системе и/или обслуживание компьютеров.

8. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.

9. Оборудовать устройство, с которого осуществляется перевод денежных средств, средством защиты информации, позволяющим осуществлять контроль конфигурации устройства (Аккорд-АМДЗ и т.п.).