**ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № _____**

**об использовании программно-технического комплекса «Банк-Клиент»**

к договору(ам) банковского счета и расчетно-кассового обслуживания

Санкт-Петербург «___» _____ 200__г.

**Открытое акционерное общество «Банк «Петровский»**, именуемый в дальнейшем «Банк», и_____
____
_____
____,
именуемый в дальнейшем «Клиент», в лице _____
_____
____,
действующего на основании _____, с другой стороны,
заключили настоящее соглашение (**далее – Соглашение**) о нижеследующем:

**1. Предмет соглашения**

1.1. Настоящее Соглашение регулирует порядок осуществления электронного документооборота между Банком и Клиентом с использованием автоматизированной технологии обслуживания Клиента и электронной цифровой подписи с целью предоставления услуг по обмену информацией и документами в электронной форме (электронными документами).

1.2. В соответствии с настоящим Соглашением Банк принимает от Клиента электронные документы с применением электронно-цифровой подписи (далее – ЭЦП). При этом стороны признают используемые ими по настоящему Соглашению системы телекоммуникаций, обработки и хранения информации достаточными для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а систему защиты информации, обеспечивающую разграничение доступа, шифрование, контроль целостности и электронную цифровую подпись, достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и разбора конфликтных ситуаций.

1.3. Используемые во взаимоотношениях между Банком и Клиентом документы в электронной форме (электронные документы), подготовленные в соответствии с требованиями Федерального закона по использованию систем защиты информации и заверенные ЭЦП одной из Сторон, признаются другой Стороной как подлинные, эквивалентные соответствующим бумажным документам, и порождают аналогичные им права и обязанности Сторон только в рамках настоящего двустороннего Соглашения.

1.4. Электронный расчетный документ порождает обязательства Сторон по настоящему Соглашению, если он передающей Стороной должным образом оформлен, заверен ЭЦП и передан, а принимающей Стороной получен, проверен и принят. Свидетельством того, что электронный документ получен и принят являются должным образом оформленные и заверенные ЭЦП электронные квитанции о его получении и принятии в обработку соответственно.

1.5. Циркулирующая в системе информация Клиента и Банка, определенная ст. 26 Закона «О банках и банковской деятельности», персональные адреса, идентификационные параметры, регистрационные номера, пароли и ключи обеих Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы согласительной экспертной комиссии по разбору конфликтных ситуаций являются конфиденциальными сведениями. Конфиденциальные сведения не подлежат разглашению Банком и Клиентом (передаче третьему лицу) ни при каких обстоятельствах, кроме установленного законом порядка.

1.6. Счет(-а) Клиента в Банке, по которым будут осуществляться расчеты с использованием системы:

| Номер счёта | Дата и номер договора банковского счёта и расчётно-кассового обслуживания |
|---|---|
| | |
| | |
| | |
| | |
| | |

**2. Термины**

2.1. Термины, применяемые в тексте настоящего Соглашения, используются в следующем значении:

2.1.1. *«Система электронной почты электронных документов» (далее – Система)* – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Соглашению.

2.1.2. *«Электронный документ»* - совокупность информации, предоставленная в электронно-цифровой форме в Системе, соответствующая какому-либо бумажному документу, несущему, сопровождающему и/или подтверждающему финансовые обязательства. Обязательным реквизитом электронного документа является ЭЦП.

2.1.3. *«Электронная цифровая подпись»* – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца подписи, а также установить отсутствие искажения информации в электронном документе.

2.1.4. *«Средства ЭЦП»* - программно-аппаратные средства, обеспечивающие реализацию одной из следующих функций – создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП, подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе.

2.1.5. *«Участник Системы»* - Банк или Клиент.

2.1.6. *«Регистрационный центр – Центр управления ключевыми системами Банка» (далее – Регистрационный центр)* – внутренняя организационная структура Банка, осуществляющая управление ключевой системой в Банке, включая создание ключей ЭЦП, выдачу сертификатов ключей ЭЦП, а также осуществление иных функций удостоверяющего центра, предусмотренных Федеральным законом «Об электронной цифровой подписи».

2.1.7. *«Закрытый ключ ЭЦП»* - уникальная последовательность символов, известная владельцу ЭЦП и предназначенная для создания в электронных документах ЭЦП с использованием средств ЭЦП.

2.1.8. *«Открытый ключ ЭЦП»* - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю Системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности ЭЦП в электронном документе.

2.1.9. *«Владелец ЭЦП»* - лицо, на имя которого Регистрационным центром зарегистрирован сертификат ЭЦП и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).

2.1.10. *«Компрометация закрытого ключа ЭЦП»* - событие, определенное владельцем ЭЦП как ознакомление какими бы то ни было посторонними лицами с его закрытым ключом ЭЦП.

2.1.11. *«Проверка подлинности ЭЦП в электронном документе»* - проверка средствами ЭЦП принадлежности ЭЦП в электронном документе владельцу ЭЦП и отсутствия искажений в электронном документе, подписанном данной ЭЦП.

2.1.12. *«Сертификат открытого ключа ЭЦП»* - документ, включающий в себя открытый ключ ЭЦП, который выдается Регистрационным центром участнику Системы для подтверждения подлинности ЭЦП и идентификации владельца ЭЦП.

**3. Права и обязанности сторон**

3.1. *Банк обязуется:*

3.1.1. Присвоить Клиенту регистрационные идентификационные параметры в системах телекоммуникационной связи и криптографической защиты и зарегистрировать ключи Клиента по его

заявке.

3.1.2. По заявке Клиента в соответствии с действующими Тарифами Банка в предварительно согласованные сроки осуществить установку Системы на оборудовании Клиента.

3.1.3. Своевременно информировать Клиента по Системе о предстоящей смене ключевой информации и передавать ему по его заявке соответствующие сертификаты.

3.1.4. Оказывать консультационные услуги Клиенту по вопросам функционирования Системы, использования средств защиты и передачи/приема информации и технологии ее обработки.

3.1.5. Принимать к исполнению поступившие от Клиента электронные документы, оформленные в соответствии с требованиями действующего законодательства РФ и условиями настоящего Соглашения, заверенные ЭЦП должностных лиц Клиента, при положительном результате проверки подлинности ЭЦП в электронном документе Клиента.

3.1.6. Обработку и исполнение полученных ЭД Клиента осуществлять в строгом соответствии с установленными нормами, техническими требованиями, стандартами, инструкциями ЦБ РФ и другими руководящими документами по подготовке данных, обработке, хранению и передаче информации и выбранным Клиентом тарифным планом.

3.1.7. Электронные документы, оформленные с нарушением условий, указанных в пункте 3.1.6 настоящего Соглашения, Банком к исполнению не принимаются.

3.2. *Банк имеет право*

3.2.1. После предварительного предупреждения отказать в приеме распоряжений на проведение операций по банковскому счёту, подписанных ЭЦП в случае выявления сомнительных операций.

3.2.2. Потребовать от Клиента предоставить в Банк платежный документ на бумажном носителе, оформленный в соответствие с требованиями Банка России, заверенный подписями и печатью, представленными в карточке образцов подписей и оттиска печатей, и не осуществлять платеж до получения указанного документа.

3.2.3. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию электронных документов, в одностороннем порядке приостановить до устранения неисправностей передачу электронных документов. Все платежные документы в этом случае должны представляться в Банк и Клиенту на бумажных носителях в установленном порядке.

3.2.4. Изменить в одностороннем порядке порядок передачи электронных документов, уведомив Клиента средствами Системы.

Уведомление вступает в силу на следующий день после отправки Банком уведомления Клиенту.

3.3. *Банк гарантирует*

3.3.1. Отзыв переданного в Банк электронного документа по письменному заявлению Клиента переданному в Банк (операционному работнику) до акцепта (проведения) документа в Банке.

3.3.2. Блокирование Системой электронных документов от незарегистрированных пользователей и от пользователей, применивших некорректные Средства ЭЦП.

3.4. *Клиент обязуется:*

3.4.1. Организовать внутренний режим функционирования рабочего места Системы таким образом, чтобы исключить возможность его использования неуполномоченными лицами.

3.4.2. Не изготавливать копии Системы, кроме резервных, а также не модифицировать Систему и не использовать ее иначе, чем в рамках Соглашения.

3.4.3. Не передавать третьим лицам предоставленную Банком Систему.

3.4.4. Передать в Банк оформленный в соответствии с Федеральным законом «Об электронной цифровой подписи», Сертификат открытого ключа ЭЦП.

3.4.5. Обеспечить сохранность от посторонних лиц дискет или иных носителей информации с открытыми и закрытыми ключами ЭЦП.

Указанные дискеты или иные носители информации должны храниться исключительно у самих лиц, обладающих правом подписи документов в электронной форме.

3.4.6. Не допускать случаев компрометации закрытых ключей ЭЦП.

3.4.7. В случае компрометации закрытого ключа ЭЦП немедленно известить об этом Банк, потребовав приостановления действия соответствующих сертификатов ключей ЭЦП, и затем произвести смену ключей ЭЦП.

3.4.8. Производить смену ключей ЭЦП не реже одного раза в год, а в случае смены должностных лиц, уполномоченных распоряжаться счетом - немедленно.

3.4.9. Соблюдать положения и требования к средствам криптографической защиты информации (СКЗИ), определяемых эксплуатационной документацией на СКЗИ, а также Федеральных законов и других регламентирующих документов в области создания, эксплуатации и уничтожения СКЗИ.

3.4.10. По первому требованию Банка заверить подписью и печатью принятые Банком с использованием Системы и распечатанные на бумажном носителе проведенные по счету Клиента платежные документы.

3.4.12. Оплачивать услуги Банка в соответствии с Тарифами .

3.5. *Клиент имеет право*

3.5.1. Получать из Банка информацию:

- о состоянии его счетов в форме электронных выписок по мере совершения операций;
- расчетные документы с оттиском штампа Банка:
- справочную информацию о работе Системы.

3.5.2. Передавать в Банк электронные документы в соответствии с п. 3.1.6 настоящего Соглашения.

3.6. *Стороны взаимно обязуются*

3.6.1. Поддерживать в рабочем состоянии установленные на их территории программно-аппаратные средства, используемые при обмене документами по Системе.

3.6.2. Сохранять конфиденциальность информации, связанной с использованием Системы, за исключением случаев, предусмотренных действующим законодательством.

3.6.3. Не предпринимать действий, способных нанести ущерб другой Стороне вследствии использования Системы.

3.6.4. При возникновении разногласий и споров разрешать их в соответствии с порядком, установленным в разделе 6 настоящего Соглашения. При не достижении согласия споры передаются на разрешение в арбитражный суд по месту регистрации Банка.

3.6.5. Поддерживать системное время ПЭВМ, на которой установлена Система, в соответствии с текущим астрономическим временем г. Москвы. Стороны принимают в качестве единой шкалы времени при работе в Системе Московское поясное время.

3.6.6. При осуществлении операций на основании полученных по Системе электронных документов руководствоваться требованиями нормативных документов ЦБ РФ, Российского законодательства и Унифицированных правил и обычаев, сложившихся в международной банковской практике, Договоров (соглашений), заключаемых между Банком и Клиентом, а также правилами и требованиями, установленными технической документацией на Систему.

3.6.7. Обеспечивать целостность, сохранность программных средств, ЭД, протоколов регистрации событий и конфиденциальность действующей парольной и ключевой информации, используемой для доступа в систему, шифрования данных и определения их авторства.

3.6.8. В случае утери своего секретного ключа или возникновении подозрений на несанкционированный доступ к ключам и паролям, немедленно проинформировать противоположную Сторону и прекратить работу до момента генерации новых Сертификатов ключей ЭЦП..

3.6.9. Вести электронные журналы учета отправленных/принятых документов, работы систем телекоммуникаций, а так же соответствующие архивы открытых ключей другой стороны, самих ЭД и квитанций на них с ЭЦП. Журналы и архивы ЭД должны храниться в соответствии с порядком и сроками, установленными для банковских документов, а сертификаты открытых ключей - пока хранятся документы, подписанные на соответствующих им секретных ключах.

**4. Ответственность сторон**

4.1. Ответственность Банка за задержки проведения успешно принятых по Системе электронных документов определяется договором банковского счета и расчетно-кассового обслуживания.

4.2. Банк не несет ответственности в случае невозможности осуществления обмена электронными документами с Клиентом, если это вызвано неисправностями используемых Клиентом программно-аппаратных средств и каналов связи, предоставленных третьими лицами.

4.3. В случае утраты или компрометации закрытых ключей ЭЦП сторона, несвоевременно сообщившая об указанных случаях, несет связанные с этим риски возможных убытков.

4.4. Стороны освобождаются от ответственности за неисполнение (ненадлежащее исполнение) обязательств, явившееся следствием обстоятельств непреодолимой силы. При этом Сторона, для которой создалась невозможность исполнения обязательств, должна известить другую Сторону об этом.

**5. Срок действия соглашения и прочие условия**

5.1. Настоящее Соглашение действует с момента его подписания Сторонами и прекращает

действие с момента закрытия всех счетов клиента, указанных в п.1.6 настоящего Соглашения.

5.2. Клиент имеет право расторгнуть настоящее Соглашение, письменно уведомив Банк за пятнадцать дней до срока предполагаемого расторжения.

5.3. Банк имеет право, уведомив Клиента за пятнадцать дней до даты предполагаемого расторжения, в одностороннем порядке расторгнуть настоящее Соглашение в следующих случаях:

- в случае нарушения Клиентом какого-либо из условий Соглашения;
- в случае, если Клиент не осуществляет операций по системе ЭППД свыше 6-ти месяцев.

5.4. Настоящее Соглашение составлено в 2-х экземплярах, по одному для каждой из Сторон.

Оба имеют равную юридическую силу.

5.5. Все приложения к настоящему Соглашению являются его неотъемлемой частью.

5.6. Стороны признают, что:

- внесение изменений в электронный документ после его подписания ЭЦП является нарушением условий настоящего Соглашения;
- подделка ЭЦП невозможна без использования закрытого ключа ЭЦП.

5.7. Стороны также признают используемую ими систему защиты информации, которая обеспечивает шифрование и контроль целостности ЭЦП, достаточной для защиты от несанкционированного доступа в систему, а также подтверждения авторства и подлинности электронных документов.

5.8. Банк имеет право в целях обеспечения защиты от несанкционированного доступа в систему производить замену средств защиты информации, используемых при обмене электронными документами, о чем уведомляет Клиента не менее чем за 30 дней.

**6. Порядок рассмотрения споров и разногласий**

6.1. Рассмотрение споров и разногласий, которые могут возникнуть в связи с обменом электронными документами, рассматриваются создаваемой Сторонами Согласительной комиссией (далее – Комиссия).

6.2. При возникновении разногласий в связи с обменом электронными документами Сторона, имеющая разногласие (далее Сторона-инициатор), обязана направить другой Стороне заявление о разногласиях, подписанное уполномоченным должностным лицом, с подробным изложением причин разногласий и предложением создать Комиссию с указанием лиц, которые будут представлять ее в Комиссии.

6.3. В состав Комиссии должно входить равное количество представителей каждой Стороны до трех человек. Члены Комиссии от каждой Стороны назначаются приказами соответствующей Стороны.

6.4. Стороны обязуются предоставить Комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена ЭД (АРМ обмена ЭД).

6.5. Комиссией рассматриваются разногласия следующих типов:

1-ый тип разногласий: Сторона-отправитель утверждает, что не направляла электронный документ, а Сторона-получатель утверждает, что электронный документ был получен;

2-ой тип разногласий: Сторона-получатель утверждает, что не получала электронный документ, а Сторона-отправитель утверждает, что электронный документ был направлен;

6.6. При рассмотрении разногласий всех типов первоначально Стороной-инициатором предоставляются Комиссии сертификаты ключей ЭЦП, а Комиссия устанавливает целостность и исправность средств ЭЦП, входящих в систему ЭППД и соответствие представленных открытых ключей ЭЦП открытым ключам ЭЦП, зарегистрированным в Банке. При положительном результате проверки средства ЭЦП и открытые ключи ЭЦП принимаются Комиссией для дальнейшей работы.

6.7. При рассмотрении первого типа разногласий Сторона-получатель представляет электронный документ, оспариваемый Стороной-отправителем.

Если в результате проверки подлинности подписи ЭЦП в представленном электронном документе, проведенной принятыми Комиссией средствами ЭЦП, получен положительный результат, то комиссией принимается решение о том, что Сторона-отправитель направляла электронный документ Стороне-получателю и должна нести за него ответственность.

Если Сторона-отправитель настаивает на том, что данный электронный документ она не отправляла, комиссия может вынести определение о компрометации закрытого ключа ЭЦП Стороны-отправителя, что не снимает ответственности Стороны-отправителя за данный электронный

документ.

Если проверка ЭЦП Стороны-отправителя под оспариваемым электронным документом дает отрицательный результат, то комиссией принимается решение о том, что Сторона-отправитель не направляла электронный документ Стороне-получателю и не должна нести ответственность за его исполнение.

В этом случае ответственность за исполнение данного электронного документа несет Сторона-получатель.

6.8. При рассмотрении разногласий второго типа Сторона-отправитель представляет в виде электронного документа сообщение Стороны-получателя о получении оспариваемого электронного документа, что свидетельствует о получении Стороной-получателем данного электронного документа.

Комиссия осуществляет подтверждение подлинности ЭЦП в данном электронном документе.

Если в результате проверки подлинности подписи, проведенной принятыми Комиссией средствами ЭЦП, получен положительный результат, то Комиссия принимает решение, что Сторона-получатель получила ЭПД и несет за ответственность за его неисполнение.

В случае отрицательного результата проверки ЭЦП или в случае непредставления Стороной-отправителем сообщения от Стороны-получателя на отправленный электронный документ комиссия принимает решение о том, что Сторона-получатель документа не получала и ответственности за его неисполнение не несет.

6.9. По результатам рассмотрения разногласий Комиссией составляется акт, который является основанием для урегулирования Сторонами возникших разногласий в добровольном порядке, а также основанием для передачи спора на рассмотрение арбитражного суда .

6.10. В случае если на предложение Стороны-инициатора о создании комиссии ответ другой Стороны не был получен, или получен отказ от участия в работе комиссии, или другой Стороной чинились препятствия работе комиссии, Сторона-инициатор вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого электронного документа. Указанный акт составляется в двух экземплярах, подписывается уполномоченным должностным лицом, и один экземпляр направляется другой Стороне.

**7. Особые условия**

7.1. Инициатором сеансов связи с Банком всегда является Клиент. Любая просрочка в выполнении Банком своих обязательств, которая произошла из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком, не влечет за собой ответственности Банка.

**8. Юридические адреса и банковские реквизиты сторон**

**БАНК:**

ОАО «Банк «Петровский»:
191186 Санкт-Петербург, Невский пр., дом 26,
к/с 30101810600000000809 в ГРКЦ ГУ Банка России по Санкт-Петербургу, БИК 044030809,
ИНН 7831000179, КПП 783501001, ОКОНХ 96120, ОКПО 09801859, ОГРН 1027800000568
SWIFT:PETRRU2P

**Клиент:**

Наименование
организации_____

Место нахождения _____

ИНН/КИО_____

| **От Банка:** | **От Клиента:** |
|---|---|
| По доверенности №_____ от _____ | _____, |
| _____ | _____ |
| _____ | _____ |
| *(должность, фамилия и инициалы)* | |
| М.П. | М.П. |

Приложение № 1
к Дополнительному соглашению № _____ от _____
об использовании программно-технического комплекса «Банк-Клиент»
к договору(ам) банковского счета и расчетно-кассового обслуживания

**ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ КЛИЕНТА И ОПИСАНИЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОМПЛЕКСА**

1. Технические средства Клиента должны содержать:

- Персональный компьютер класса Pentium с операционной системой Windows 98/NT/2000 XP.
- Установленный на компьютере модем (для создания связи модем-модем)

Возможно соединение через Интернет (через выделенную линию, SKYLINK, и т.п.).

- Обязательное наличие принтера на момент генерации ключей и печати сертификатов и запросов на сертификаты.

2. В Комплексе организована и использована многоуровневая система защиты информации от несанкционированного доступа:

- система электронной подписи и кодирования документов Клиента при отправке в Банк по линиям связи;
- для каждого Клиента устанавливаются уникальные имена и пароль для связи с Банком при помощи программно-технического комплекса «Банк-Клиент»;
- на банковской ЭВМ, осуществляющей связь с Клиентом, ведется протокол работы, который ежедневно контролируется службами Банка.

Система электронной подписи и кодирования использует алгоритм RSA с открытым ключом. Система оперирует парой однозначно взаимосвязанных электронных ключей (открытый и закрытый ключи).

Кодирование и раскодирование документов производится комплексом на основании открытых ключей, которыми обменялись обе стороны настоящего Соглашения.

При установке программно-технического комплекса «Банк-Клиент» для Клиента вводятся:

- имя и пароль для соединения с банковской ЭВМ;
- электронные ключи;

**Для Банка вводится пара электронных ключей, уникальная для каждого Клиента. Банк и Клиент обмениваются открытыми ключами и составляют Акт об обмене электронными ключами (Приложение №2 к настоящему Соглашению**).

| **От Банка:** | **От Клиента:** |
|---|---|
| по доверенности №_____ от _____ | |
| _____ | _____ |
| *должность* | |
| _____ /_____/ | _____ /_____/ |
| *фамилия и инициалы* | |
| м.п. | м.п. |

Приложение №2
к Дополнительному соглашению № _____ от _____
об использовании программно-технического комплекса «Банк-Клиент»
к договору(ам) банковского счета и расчетно-кассового обслуживания

**ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПРИ УСТАНОВКЕ (ПОДКЛЮЧЕНИИ) К СИСТЕМЕ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ**

**1. Порядок взаимодействия при установке (подключении) к системе**

1.1. Клиент получает бланки Дополнительного соглашения с приложениями (в 2-х экземплярах), далее – Дополнительное соглашение.

1.2. Клиент подписывает и передает в ДО БРЦ Дополнительное соглашение (в 2-х экземплярах) и надписанный CD-R (CD-RW) диск для записи на него дистрибутива (при желании).

1.3. Операционный работник в ДО БРЦ, после согласования и подписания Дополнительного соглашения, передает Клиенту под роспись в Карточке учета выдачи выписок из лицевых счетов расчетных, текущих, бюджетных и валютных (далее – Каоточка):

- дискету с конфигурационными файлами (далее – дискета) и пароль к установке (в запечатанном конверте);
- подписанный со стороны Банка экземпляр Дополнительного соглашения;
- CD-R (CD-RW) диск с записанным на него дистрибутивом (при условии его предоставления Клиентом)

1.4. Клиент получает на основании Доверенности:

- дискету и пароль к установке (в запечатанном конверте);
- подписанный со стороны Банка экземпляр Дополнительного соглашения с приложениями;
- CD-R (CD-RW) диск с записанным на него дистрибутивом (при условии его предоставления Клиентом).

1.5. Клиент устанавливает систему Банк-Клиент (один из вариантов):

- скачав дистрибутив программы с сайта Банка **www. petrovskiybank .ru;**
- загрузив дистрибутив с CD-R (CD-RW) диска (при условии его предоставления Клиентом);
- вызвав специалиста службы сопровождения системы Банк-Клиент. Данная услуга оплачивается в соответствии с Тарифами Банка. Для вызова специалиста необходимо связаться со службой сопровождения системы Банк-Клиент.
  Данные для связи (телефон, адрес электронной почты и др.) приведены в инструкции, входящей в состав файлов на дискете, передаваемой Клиенту. При оказании этой услуги подписывается «Акт о выполнении работ по системе электронных платежей «Банк-Клиент».

1.6. Клиент генерирует ключи электронно-цифровой подписи (далее – ЭЦП) и запросы на сертификаты, запрашивает средствами системы Банк-Клиент сертификаты, распечатывает запросы и сертификаты (в 2-х экземплярах).

1.7. Клиент, подписав и проставив печати на запросах и сертификатах (в 2-х экземплярах), передает их в ДО БРЦ .

1.8. Операционный работник в ДО БРЦ после проверки и подписания запросов и сертификатов передает один экземпляр этих документов Клиенту под роспись в Карточке.

1.9. Клиент, получив запросы и сертификаты, проверяет наличие подписи и печати Банка с отметкой «ДЛЯ СЕРТИФИКАТОВ». При их отсутствии возвращает документы в ДО БРЦ .

1.10. Клиент хранит сертификаты в сроки, установленные законодательством РФ.

**2. Порядок действий при замене ключей клиента**

2.1. Замена ключей клиента проводится в связи:

- со сменой должностного лица,

- компрометацией действующего ключа,
- по истечении срока действия ключа.

2.2. При возникновении одной из указанных в п.2.1 причин Клиенту необходимо обратиться в Банк к уполномоченному сотруднику с просьбой осуществить блокировку системы «Банк-Клиент».

2.3. Замена ключей ЭЦП.

2.3.1. В случае смены должностного лица Клиент оформляет в ДО БРЦ карточку образцов подписей и оттиска печати.

2.3.1.1. Операционный работник в ДО БРЦ передает дискету Клиенту под роспись в Карточке.

2.3.1.2. Клиент изменяет файлы конфигурации в клиентской части системы Банк-Клиент.

2.3.2. Клиент генерирует ключи ЭЦП и запросы на сертификаты, запрашивает средствами системы Банк-Клиент сертификаты, распечатывает запросы и сертификаты (в 2-х экземплярах).

2.3.3. Клиент, подписав и проставив печати на запросах и сертификатах (в 2-х экземплярах), передает их в ДО БРЦ .

2.3.4. Операционный работник ДО БРЦ после проверки и подписания запросов и сертификатов передает один экземпляр этих документов Клиенту под роспись в Карточке.

2.3.5. Клиент, получив запросы и сертификаты, проверяет наличие подписи и печати Банка с отметкой «ДЛЯ СЕРТИФИКАТОВ». При их отсутствии возвращает документы в ДО БРЦ .

### 3. Порядок действий при замене конфигурационных файлов (дискета)

3.1. Замена дискеты проводится в связи:

- со сменой должностного лица,
- компрометацией действующего ключа,
- в случае порчи и/или утраты дискеты.

3.2. При возникновении одной из указанных в п.3.1 причин Клиенту необходимо обратиться в Банк к уполномоченному сотруднику с просьбой осуществить блокировку системы «Банк-Клиент».

3.3. Клиент обращается с просьбой о замене дискеты в обслуживающее его ДО БРЦ .

3.4. Получает бланк «Заявки на получение дискеты», далее – Заявка.

3.5. Передает в ДО БРЦ заполненную Заявку с указанием своего кода в системе Банк-Клиент и отметкой причины «замена дискеты».

3.6. Операционный работник в ДО БРЦ, после согласования и подписания Заявки, передает Клиенту под роспись в Карточке:

- дискету (в запечатанном конверте),

3.7. Клиент получает на основании Доверенности:

- дискету (в запечатанном конверте),

Приложение №3
к Дополнительному соглашению № _____ от _____
об использовании программно-технического комплекса «Банк-Клиент»
к договору(ам) банковского счета и расчетно-кассового обслуживания

**ТРЕБОВАНИЯ**
**ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАБОТЕ В СИСТЕМЕ ЭЛЕКТРОННОГО ОБМЕНА ДАННЫМИ С ПРИМЕНЕНИЕМ СРЕДСТВ ШИФРОВАНИЯ**

1. Обмен ЭД должен проводиться на специализированных автоматизированных рабочих местах (АРМ), программное обеспечение которых должно выполнять только функции, определенные данным технологическим процессом
2. Руководство каждой из Сторон своим приказом утверждает список лиц, имеющих доступ к ключевой информации. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.
3. В случае увольнения или изменения функциональных обязанностей сотрудника, имевшего доступ к ключам шифрования, должна быть проведена смена ключей, к которым он имел доступ.
4. Для хранения носителей с ключами шифрования в помещениях должны устанавливаться надежные металлические шкафы (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности или у руководителя).
5. Порядок доступа в помещения, в которых размещается АРМ обмена ЭД, должен быть регламентирован и для обеспечения защиты указанных помещений должны быть реализованы следующие меры:
   - на входные двери должны быть установлены замки и опечатывающие устройства, гарантирующие надежную защиту помещений в нерабочее время, а для контроля за входом в помещения должны быть установлены автоматические замки (электронные, кодовые и т.п.) или другие средства современных систем контроля и регистрации доступа;
   - помещения должны быть (по возможности) оборудованы сигнализацией и по окончании рабочего дня опечатываться и сдаваться под охрану;
6. По окончании рабочего дня, а также вне времени обмена ЭД носители закрытых ключей ЭЦП и шифрования должны храниться в металлических шкафах (сейфах)
7. Запрещается:
   - снимать несанкционированные копии с ключевых носителей;
   - знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;
   - выводить секретные ключи на дисплей (монитор) ПЭВМ или принтер;
   - устанавливать ключевой носитель в считывающее устройство (дисковод) ПЭВМ АРМ обмена ЭД в режимах, не предусмотренных функционированием системы обработки и обмена ЭД с Банком, а также в другие ПЭВМ;
   - записывать на ключевой носитель постороннюю информацию;
   - -хранение ключевой информации на жестких магнитных дисках компьютеров, не оборудованных средствами защиты от несанкционированного доступа;
   - -использование любого локального диска АРМ обмена, в качестве сетевого ресурса;
   - включать ключевую информацию в состав аварийных и других архивов.
8. При компрометации или утере ключа шифрования Сторона, допустившая компрометацию (утрату), немедленно предпринимает все необходимые меры по прекращению любых операций с ЭД с использованием скомпрометированного (утраченного) ключа ЭЦП и оперативно информирует о факте компрометации (утраты) другую Сторону. При этом Стороны в оперативном порядке принимают меры по выводу скомпрометированных (утраченных) ключей ЭЦП или шифрования из действия и организовывают их внеплановую смену
9. Для осуществления антивирусной защиты в АРМ обмена ЭД должны использоваться только лицензированные антивирусные средства.

**От Банка:**
по доверенности №_____ от _____

_____
*должность*
_____ /_____/
*фамилия и инициалы*

м.п.

**От Клиента:**

_____

_____ /_____/

м.п.

Приложение № 4
к Дополнительному соглашению № _____ от _____
об использовании программно-технического комплекса «Банк-Клиент»
к договору(ам) банковского счета и расчетно-кассового обслуживания

**ПОРЯДОК ОБСЛУЖИВАНИЯ БАНКОМ КЛИЕНТОВ ПРИ ПОМОЩИ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА «БАНК-КЛИЕНТ»**

Обслуживание осуществляется по рабочим дням с 9 часов 00 минут до 21 часа 00 минут согласно тарифам комиссионного вознаграждения Банка.

Электронные документы, принятые Банком до 15.00 часов, проводятся по счету клиента датой текущего дня. Электронные документы, принятые Банком после 15.00 часов, проводятся датой следующего рабочего дня.

Полученный Банком от Клиента электронный документ является основанием для списания Банком указанных в документе сумм со счета Клиента в случае прохождения документом проверки и установления подлинности действующего открытого ключа Клиента.

При получении электронных документов от Клиента Банк производит проверку достаточности денежных средств на расчетном счете Клиента для их исполнения и проверку правильности заполнения реквизитов.

Полученный Клиентом от Банка протокол приема платежных документов является подтверждением принятия Банком к исполнению электронных документов Клиента.

В случае неполучения ответа из Банка о проведении электронных документов Клиент обязан выяснить причину у операционного работника, обслуживающего его счета.

Подтверждением исполнения Банком электронных документов является выписка по счету Клиента, предоставляемая не позднее дня, следующего за днем совершения операции.

Отзыв переданного в Банк электронного платежного документа может быть осуществлен самостоятельно или по заявлению, переданному в Банк (операционному работнику):

- не позднее 15.00, в случае проведения платежа текущей датой;
- не позднее 18.00, в случае проведения платежа датой следующего рабочего дня.

**От Банка:**
по доверенности №_____ от _____

_____
*должность*

_____ /_____/
*фамилия и инициалы*

м.п.

**От Клиента:**

_____

_____ /_____/

м.п.

**Дополнительное соглашение к договору банковского счета**

**и расчетно-кассового обслуживания № _____ от «___» _____200__ г.**

Санкт-Петербург «____» _____ 200_ г.

Открытое акционерное общество «Банк «Петровский», именуемое в дальнейшем «Банк» с одной стороны и_____
_____
_____
_____именуемо
е в дальнейшем «Клиент», в лице
_____
_____,
действующего на основании _____, с другой стороны, заключили настоящий договор о нижеследующем:

1. Клиент поручает Банку производить списание денежных средств со своего счета открытого в Банке №_____**по платежным требованиям «без акцепта»**,
выставляемым_____
*( наименование кредитора (получателя средств )*
_____
(дата, номер, пункт основного договора, предусматривающий право безакцептного списания)
_____
*(наименование товаров, работ или услуг)*
_____ .

2. Настоящее дополнительное соглашение является неотъемлемой частью договора банковского счета и расчетно-кассового обслуживания № _____ от «___» _____ 200__ г., составлено в двух экземплярах, имеющих равную юридическую силу, один из которых остается у Банка, а второй у Клиента.

**Реквизиты сторон:**

**БАНК:**
ОАО «Банк «Петровский»:
191186 Санкт-Петербург, Невский пр., дом 26,
к/с 30101810600000000809 в ГРКЦ ГУ Банка России по Санкт-Петербургу, БИК 044030809,
ИНН 7831000179, КПП 783501001, ОКОНХ 96120, ОКПО 09801859, ОГРН 1027800000568
SWIFT:PETRRU2P
**Клиент:**
Наименование организации_____

Место нахождения _____

ИНН/КИО_____

**От Банка:**

По доверенности №_____ от _____
_____
_____
(Должность, фамилия и инициалы)

М.П.

**От Клиента:**

_____,
_____
_____

М.П