Приложение 1
к Соглашению о предоставлении
услуг электронного документооборота
в АО "Промэнергобанк"

Регламент
подключения и использования системы Дистанционного банковского обслуживания

1. Общие положения

1.1. Настоящий регламент является неотъемлемой частью Соглашения о предоставлении услуг электронного документооборота в АО "Промэнергобанк" (далее – Соглашение).
1.2. Электронный документооборот между Банком и Клиентом обеспечивается с помощью Системы дистанционного банковского обслуживания.
1.3. Порядок подключения Клиента к Системе ДБО, порядок обращения со средствами защиты информации, ключами ЭП и паролями, а также порядок передачи и обработки электронных документов устанавливаются настоящим Регламентом.
1.4. Требования настоящего Регламента являются обязательными для выполнения при подключении к системе ДБО и ее эксплуатации.
1.5. Доступ клиента к Системе ДБО осуществляется посредством подключения через сеть Интернет к специализированному сайту Банка с помощью программы-браузера, либо с помощью специального программного обеспечения, загруженного со специализированного сайта Банка и установленного на АРМ Клиента

2. Требования к АРМ клиента

2.1. Компьютер с установленной операционной системой Windows XP или выше, операционной системой семейства Linux.
2.2. Наличие русско-английской клавиатуры и манипулятора мышь, либо аналогичного по функциональности устройства.
2.3. Функционирующий разъем USB для подключения носителей ключевой информации.
2.4. Объем оперативной памяти должен быть достаточен для нормального функционирования операционной системы и веб-браузера.
2.5. Свободное место на жестком диске, достаточное для нормального функционирования операционной системы.
2.6. Установленный веб-браузер (рекомендуемые браузеры: Internet Explorer, Mozilla FireFox, Google Chrome).
2.7. Возможность установки среды выполнения Java (Java Runtime Environment, JRE) версии 7 или выше.
2.8. Канал доступа в сеть Интернет, позволяющий устанавливать соединение с сервером банка по протоколу https и имеющий пропускную способность не менее 128Kbps
2.9. Установленное и функционирующее антивирусное программное обеспечение с регулярно обновляемой базой данных сигнатур.
2.10. Установленный и функционирующий межсетевой экран (брандмауэр), препятствующий бесконтрольному подключению к ресурсам компьютера из локальных сетей и сетей общего пользования.

3. Правила информационной безопасности при использовании Системы

3.1. Клиент обязуется не использовать в качестве АРМ для работы с Системой компьютеры, к которым возможен доступ неуполномоченных лиц.

3.2. Клиент обязан сохранять в тайне от неуполномоченных лиц пароль для доступа в Систему и ключи ЭП. Носители ключевой информации, и пароль должны храниться исключительно у должностных лиц Клиента, уполномоченных распоряжаться счётом.
3.3. Носители ключевой информации должны подключаться к компьютеру только на время работы с системой, в остальное время носители ключевой информации должны храниться в опечатываемом сейфе, исключающем несанкционированный доступ к ним. Носители ключевой информации и сертификат ключа проверки ЭП ни при каких обстоятельствах не должны передаваться неуполномоченным лицам. Ответственность за использование пароля и ключей ЭП неуполномоченными лицами полностью несёт Клиент, вне зависимости от обстоятельств, при которых пароль, ключи ЭП оказались у неуполномоченных лиц.
3.4. При утере носителя ключевой информации, компрометации ключей или паролей Клиент обязан незамедлительно оповестить об этом факте Банк. Порядок действий при компрометации определяется разделом 7 настоящего Регламента
3.5. Клиент обязан сообщать Банку обо всех ошибках при совершении переводов средств и о несанкционированных переводах средств по телефону немедленно после их обнаружения по телефону, а затем в письменном виде. Под ошибкой понимается, но не ограничивается этим:
- неверный перевод средств со счёта Клиента;
- неправильное указание суммы перевода или получателя платежа в выписке по счёту Клиента;
- Наличие в выписке по счету Клиента платежей, не совершавшихся Клиентом.

3.6. В целях предотвращения угрозы несанкционированного использования Системы ДБО Клиент обязан регулярно проводить проверки АРМ средствами антивирусного программного обеспечения. В случае обнаружения вредоносного кода Клиент обязан приостановить использование системы на данном АРМ до полной очистки АРМ от вредоносного кода и восстановления его работоспособности.
3.7. В целях минимизации риска компрометации ключей ЭП Клиент и Банк проводят плановую замену ключей ЭП не реже 1 раза в год. Плановая замена ключей проводится в порядке, предусмотренном разделом 8 Регламента.
3.8. В соответствии с Положением Банка России от 09.06.2012 г. №382-П, в целях минимизации риска несанкционированного доступа к Системе ДБО и несанкционированного списания средств с расчетных счетов Банк рекомендует Клиенту выполнять меры защиты информации, приведенные в Приложении 8 к настоящему Соглашению.

4. Порядок подключения к Системе ДБО

Для подключения к Системе ДБО Клиент производит следующие действия:
4.1. Подключается к сайту Банка, загружает с него средства защиты информации и устанавливает их на своем АРМ;
4.2. Подготавливает нужное количество носителей ключевой информации;
4.3. Подключается к системе ДБО непосредственно через веб-браузер на специализированном сайте Банка (ДБО онлайн), либо установив программное обеспечение, загруженное со специализированного сайта Банка (ДБО оффлайн).
4.4. Проводит регистрацию в Системе ДБО, вводя следующие реквизиты:
- ИНН, наименование, юридический адрес организации;
- телефон и адрес электронной почты для отправки оповещений;
- контактную информацию сотрудника-пользователя Системы (ФИО и телефон);
- блокировочное слово (для блокирования ключа в случае его компрометации);
- информацию об уполномоченных лицах - владельцах ключа ЭП (ФИО, должность и паспортные данные);

4.5. После ввода регистрационных данных Системой производится генерация ключей ЭП и ключей проверки ЭП в соответствии с введенными данными об их владельцах; ключи ЭП ключи сохраняются на подготовленных носителях, ключи проверки передаются Системой в Банк для регистрации.
4.6. По сгенерированным ключам проверки ЭП Системой формируются сертификаты ключей проверки ЭП по форме Приложения 2 к Соглашению. Клиент распечатывает сертификаты и заверяет их подписями владельцев ключей ЭП, подписью руководителя и печатью Клиента, при ее наличии.
4.7. Клиент передает в Банк полученные сертификаты ключей проверки ЭП и Заявление о присоединении к Соглашению.
4.8. Банк рассматривает Заявление о присоединении к Соглашению и, не позднее чем через 3 рабочих дня, обеспечивает подключение Клиента к Системе ДБО, либо уведомляет его об отказе в подключении. Уведомление о подключении либо отказе в подключении производится по электронной почте в соответствии с указанными при регистрации реквизитами.

5. Работа в Системе ДБО

5.1. Клиент осуществляет работу в Системе ДБО в соответствии с Руководством пользователя, размещенном на сайте Банка.
5.2. Посредством Системы Клиент имеет возможность передать в Банк следующие виды электронных документов:
- Рублевое платежное поручение
- Поручение на перевод валюты
- Поручение на продажу валюты
- Поручение на покупку валюты
- Документы, подлежащие валютному контролю: Паспорт сделки, справка о валютных операциях, справка о поступлении валюты РФ, справка о подтверждающих документах
- Запрос на формирование выписки
- Письмо в банк с вложением в произвольном формате (файл)

5.3. Посредством Системы Банк передает клиенту следующие виды документов:
- Выписка по счету Клиента
- Расшифровка списаний и поступлений по счету Клиента – электронные документы, входящие в выписку по счету Клиента.
- Письмо с вложением в произвольном формате (файл)

5.4. Клиент имеет возможность подключаться к Системе ДБО круглосуточно.
5.5. Отправленные Клиентом электронные документы, поступившие на сервер в течение времени, установленного Банком для обслуживания Клиентов, принимаются к исполнению в тот же день. Электронные документы, поступившие на сервер Банка в прочее время, принимаются к исполнению Банком на следующий рабочий день. Информация о времени обслуживания Клиентов и порядке приема расчетных документов доводится до сведения Клиента путем размещения на информационных стендах в офисах Банка и сайте Банка в сети Интернет.
5.6. Электронный документ, поступивший на сервер Банка посредством Системы, не может быть отозван Клиентом средствами системы. При необходимости отмены документа после отправки его в Банк клиент должен обратиться в Банк по телефону для определения возможности отзыва документа. В случае если отзыв документа возможен – Клиент направляет в банк заявление на отзыв в письменном виде либо в виде электронного письма через Систему.
5.7. Окончательные выписки по счетам клиента за день в электронном виде формируются сервером Банка на следующий рабочий день в период с 8:30 до 9:00 по московскому времени.

5.8. Для получения Клиентом информации о текущем состоянии счета и движениям по счету за текущий день Клиент может отправить посредством системы запрос на выписку. Запрос выписки обрабатывается сервером Банка в течение не более чем 15 минут, по результатам обработки Клиенту передается выписка по счету на текущий момент, включающая расшифровку списаний и поступлений по счету.

5.9. Для информирования клиента о ходе обработки электронного документа каждый документ в Системе ДБО имеет набор статусов. Статус зависит от стадии обработки документа в системе:

- **Новый**. Присваивается при создании и сохранении нового документа, при редактировании и сохранении существующего документа, а также при импорте документа из файла. Документ со статусом Новый банк не рассматривает и не обрабатывает.
- **Подписан**. Присваивается в случае, если документ подписан, но число подписей под документом меньше необходимого. После подписания документа всеми необходимыми подписями ему присваивается статус Доставлен. При внесении изменений в документ с таким статусом и его последующем сохранении статус документа меняется на Новый.
- **Требует подтверждения**. Присваивается платежному поручению после получения необходимого количества подписей в случае использования в банке дополнительных мер защиты документа.
- **Доставлен**. Присваивается документу, когда число подписей под документом соответствует необходимому для рассмотрения документа банком. Документы в данном статусе поступают на обработку на сервер банка.
- **На обработке**. Присваивается документу после прохождения всех автоматических проверок при его выгрузке в автоматизированную банковскую систему. Для рассмотрения специалистом Банка
- **На исполнении**. Присваивается, когда документ проверен специалистом Банка и принят к исполнению.
- **Исполнен**. Присваивается документу при его исполнении Банком.
- **Отвергнут**. Присваивается документу, не принятому к исполнению по результатам автоматического контроля или проверки специалистом Банка. Клиент может или отредактировать и сохранить документ (статус изменится на **Новый**), или удалить документ (статус изменится на Удален).
- **Удален**. Присваивается документу, удаленному Клиентом. Удалению подлежат только документы в статусе Новый, Подписан или Отвергнут.

6. Дополнительные средства защиты от несанкционированного доступа при работе в Системе ДБО

6.1. В целях снижения риска несанкционированного доступа в Системе ДБО могут использоваться дополнительные средства защиты: ограничение возможности подключения Клиента к системе только с указанного IP адреса; информирование Клиента о факте подключения к Системе (входа в Систему) и/или о получении сервером Системы электронных платежных документов посредством отправки sms или e-mail сообщений.

6.2. Для использования/изменения/отмены использования фиксированного IP-адреса при работе с Системой ДБО Клиент предоставляет в Банк заявление по форме Приложения 7 к Соглашению.

6.3. Для подключения/изменения параметров/отключения информирования Клиента о фактах входа в Систему и/или о поступлении электронных платежных документов Клиент предоставляет в Банк заявление по форме Приложения 4 к Соглашению.

7. Порядок действий при компрометации ключей/паролей ЭП Клиента

7.1. При утере носителя ключевой информации, компрометации ключей ЭП или паролей Клиент обязан незамедлительно оповестить об этом факте Банк любым доступным способом, а затем, не позднее следующего рабочего дня, в письменном виде по форме Приложения 6 к Соглашению для блокировки ключей проверки ЭП. При извещении Банка по телефону для идентификации клиента используется блокировочное слово.

7.2. При получении устного сообщения Клиента о компрометации ключа ЭП и/или пароля Банк временно приостанавливает действие соответствующего ключа (ключей) проверки ЭП Клиента. При получении Заявления о компрометации ключа ЭП/пароля по форме Приложения 6 к Соглашению Банк незамедлительно блокирует ключ проверки ЭП указанных уполномоченных лиц - владельцев ключей ЭП. Ключи проверки ЭП блокируются окончательно и не могут быть использованы в дальнейшем. Изготовление и регистрация новых ключей производится в соответствии с п.9.3 настоящего Регламента.

8. Порядок плановой замены ключей ЭП

8.1. Для плановой смены ключей электронной подписи Клиент осуществляет следующие действия:

8.1.1. Клиент самостоятельно вводит регистрационную информацию о новых владельцах ключей электронной подписи в соответствии с Руководством пользователя Системы.

8.1.2. После ввода регистрационных данных Системой производится генерация ключей ЭП и ключей проверки ЭП в соответствии с введенными данными об их владельцах; ключи ЭП ключи сохраняются на подготовленных носителях, ключи проверки передаются Системой в Банк для регистрации.

8.1.3. По сгенерированным ключам проверки ЭП Системой формируются сертификаты ключей проверки ЭП по форме Приложения 2 к Соглашению. Клиент распечатывает сертификаты и заверяет их подписями владельцев ключей ЭП, подписью руководителя и печатью Клиента, при ее наличии.

8.1.4. Клиент передает в Банк полученные сертификаты ключей.

8.2. Банк проводит проверку предоставленных Клиентом сертификатов ключей проверки ЭП и, не позднее через 3 рабочих дня, производит регистрацию новых ключей проверки ЭП в Системе ДБО с одновременной блокировкой старых ключей проверки ЭП. О факте регистрации Банк уведомляет Клиента по электронной почте в соответствии с указанными при регистрации реквизитами.

9. Порядок изменения списка лиц, обладающих правом подписи электронных документов

9.1. Состав уполномоченных лиц - владельцев ключей ЭП, обладающих правами подписи электронных документов, должен соответствовать карточке образцов подписей Клиента, хранящейся в банке. При внесении изменений в карточку образцов подписей требуется внести соответствующие изменения в Систему.

9.2. При внесении изменений в карточку образцов подписей Клиента Банк проверяет соответствие списка уполномоченных лиц - владельцев ключей ЭП, зарегистрированных в Системе, карточке и блокирует ключи проверки ЭП ответственных лиц, исключенных из карточки.

Для обеспечения непрерывной работы в Системе Клиенту рекомендуется осуществить генерацию ключей ЭП новых уполномоченных лиц по п. 9.3 до внесения изменений в карточку образцов подписей и предоставить документы по п.9.5 в Банк одновременно со сменой карточки образцов подписей.

9.3. Для добавления уполномоченных лиц - владельцев ключей электронной подписи, либо для генерации уполномоченном лицам новых ключей взамен ранее заблокированных Клиент производит следующие действия:

9.3.1. Клиент самостоятельно вводит регистрационную информацию о новых владельцах ключей электронной подписи в соответствии с Руководством пользователя Системы.

9.3.2. После ввода регистрационных данных Системой производится генерация ключей ЭП и ключей проверки ЭП в соответствии с введенными данными об их владельцах; ключи ЭП ключи сохраняются на подготовленных носителях, ключи проверки передаются Системой в Банк для регистрации.

9.3.3. По сгенерированным ключам проверки ЭП Системой формируются сертификаты ключей проверки ЭП по форме Приложения 2 к Соглашению. Клиент распечатывает сертификаты и заверяет их подписями владельцев ключей ЭП, подписью руководителя и печатью Клиента, при ее наличии.

9.3.4. Клиент передает в Банк полученные сертификаты ключей и Заявление об изменении состава уполномоченных лиц - владельцев ключей ЭП по форме Приложения 5 к Соглашению.

9.4. В случае исключения уполномоченных лиц - владельцев ключей ЭП Клиент предоставляет в Банк Заявление об изменении состава уполномоченных лиц - владельцев ключей ЭП по форме Приложения 5 к Соглашению.

9.5. Банк рассматривает Заявление и предоставленные Клиентом сертификаты ключей проверки ЭП и, не позднее чем через 3 рабочих дня, проводит изменение перечня владельцев ЭП Клиента в Системе ДБО, либо уведомляет его об отказе в изменении параметров. Уведомление об изменении перечня владельцев ключей ЭП либо об отказе в изменении направляется по электронной почте в соответствии с указанными при регистрации реквизитами.

10. Порядок изменения перечня счетов, подключенных к Системе ДБО

10.1. Для подключения или отключения расчетных счетов в Системе ДБО Клиент предоставляет в Банк Заявление об изменении состава счетов, обслуживаемых посредством Системы ДБО по форме Приложения 3 к Соглашению.

10.2. Банк рассматривает Заявление и, не позднее чем через 3 рабочих дня, проводит изменение перечня счетов Клиента, подключенных к Системе ДБО, либо уведомляет его об отказе. Уведомление о произведенных изменениях либо об отказе напарвляется по электронной почте в соответствии с указанными при регистрации реквизитами.

11. Разбор конфликтных ситуаций

11.1. В данном разделе описан порядок разрешения конфликтов между Банком и Клиентом, связанных с подлинностью электронных документов. Электронный документ считается подлинным, если он был с одной стороны надлежащим образом оформлен, подписан электронной подписью и передан средствами Системы, а с другой - получен, проверен и принят к исполнению.

11.2. Настоящий раздел регламентирует процедуры, связанные с конфликтными ситуациями

- по факту передачи Клиентом Банку электронного документа;
- по дате передачи Клиентом Банку электронного документа;
- содержания переданного Клиентом Банку Электронного документа.

11.3. В случае несогласия Клиента с действиями Банка, Клиент подает в Банк письменное заявление с изложением спорной ситуации, указав детально суть конфликта, а также представляет документы и информацию, имеющие отношение к предмету спора.

11.4. На основании изучения материалов, предоставленных Клиентом, и имеющихся в распоряжении Банка, Банк в течение 5 рабочих дней со дня получения заявления выносит письменное заключение о правомерности и обоснованности претензии. Согласие или несогласие Клиента с выводами Банка оформляется письменно в форме заключения.

11.5. В случае несогласия Клиента с заключением Банка, Клиент и Банк («Стороны») в течение 5 банковских дней от даты выражения Клиентом несогласия формируют согласительную комиссию численностью не более 6 человек из числа представителей обеих Сторон. По договоренности Сторон в согласительную комиссию дополнительно могут быть включены независимые эксперты числом не более 3 человек.

11.6. Создание согласительной комиссии утверждается протоколом, подписываемым обеими Сторонами, в котором указываются Ф.И.О. членов комиссии от каждой Стороны и независимые эксперты, а также описывается регламент работы комиссии и график заседаний.

11.7. В случае уклонения Клиента или его представителей от создания согласительной комиссии или участия в ее работе Банк вправе сформировать комиссию самостоятельно, включив в состав комиссии в качестве представителей Клиента не более 3 независимых экспертов.

11.8. Согласительная комиссия осуществляет свою работу на территории Банка, с использованием сертификатов ключей проверки электронной подписи, участвующих в конфликте Сторон.

11.9. Согласительная комиссия запрашивает у Клиента и Банка необходимые материалы, относящиеся к спорной операции, в том числе материалы, находящиеся в юридическом деле Клиента; заявления Клиента о проведении спорной операции, электронные документы Системы ДБО в виде файлов и на бумажном носителе, пояснения работников Банка по сути спорной операции, документы бухгалтерского учета, подтверждающие факт проведения операции.

11.10. По результатам работы согласительной комиссии составляется соответствующий Акт, который является окончательным и не может быть оспорен Сторонами. Возражения членов согласительной комиссии, не согласных с выводами, изложенными в Акте, оформляются в письменном виде и прилагаются к Акту как его неотъемлемая часть.

11.11. Акт комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта.

11.12. Акт комиссии может являться доказательством при дальнейшем разбирательстве конфликта в судебно-арбитражных органах.