

УСЛОВИЯ
ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ПО БАНКОВСКИМ
СЧЕТАМ ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ,
ЛИЦ, ЗАНИМАЮЩИХСЯ ЧАСТНОЙ ПРАКТИКОЙ В ООО «ЗЕМСКИЙ БАНК»

1. ОПРЕДЕЛЕНИЯ

1.1. Для целей настоящих Условий, в дополнение к Правилам комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк» используются указанные ниже определения:

1.1.1. **Договор на дистанционное банковское обслуживание (далее по тексту настоящих Условий - Договор)** - общие положения Правил, настоящие Условия, Тарифы и Заявление о предоставлении КБО, надлежащим образом заполненное и подписанное Клиентом, составляющие в совокупности Договор на дистанционное банковское обслуживание, заключаемый между Банком и Клиентом;

1.1.2. **Система** - электронная банковская система, позволяющая Клиенту передавать в Банк в электронном виде расчетные (платежные) и иные документы, отслеживать текущий статус этих документов, а также получать из Банка выписки по Счетам, сообщения и иные документы с использованием сети «Интернет» с использованием средств электронной подписи, с целью предоставления Клиенту услуг по Договору.

1.1.3. **«Электронный документ»** (далее по тексту - ЭД)- документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

1.1.4. **«Электронный платежный документ»** (далее по тексту - ЭПД) - документ, являющийся основанием для совершения операций по Счетам, открытым в Банке, подписанный ЭП (или содержащий КА) и имеющий равную юридическую силу с платежными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати Клиента.

1.1.5. **«Электронная подпись»** (далее по тексту - ЭП) - реквизит ЭД, добавляемый к ЭД, полученный в результате криптографического преобразования информации, который позволяет получателю ЭД удостовериться в его авторстве и неизменности его содержания, в том числе в отсутствии подделки или искажения ЭД со стороны получателя или третьих лиц. Процедуры создания и проверки ЭП на базе асимметричного криптографического алгоритма с применением функции хэширования выполнены в соответствии с требованиями ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.

1.1.6. **«Владелец сертификата открытого ключа ЭП»** (Клиент) - уполномоченное лицо Клиента, осуществляющее от имени Клиента работу в Системе, на имя которого оформлен Сертификат открытого ключа ЭП, и которое владеет соответствующим закрытым ключом ЭП. Владелец ключа ЭП должен обладать правом подписи расчетных (платежных) документов в соответствии с карточкой с образцами подписей и оттиска печати по Счету Клиента. Если в действующей карточке с образцами подписей и оттиска печати, оформленной по форме установленной Банком, в поле «Подписи второй группы» указаны лица, обладающие правом подписи, то Владельцев ключей ЭП Клиента должно быть не менее двух - по одному лицу, указанному в карточке с образцами подписей и оттиска печати в полях «Подписи первой группы», «Подписи второй группы» соответственно. В этом случае Банк принимает к исполнению только ЭД, подписанные двумя ЭП.

1.1.7. **«Ключ ЭП»** (далее по тексту - «Ключ») - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всех возможных для данного алгоритма преобразований. Ключ состоит из открытого и закрытого ключей, которые связаны между собой с помощью особого математического соотношения.

1.1.8. **«Открытый ключ ЭП»** - криптографический ключ (уникальная последовательность символов, соответствующая закрытому ключу ЭП), известный помимо Владельца ключа другим пользователям Системы и предназначенный для проверки подлинности ЭП. Открытый ключ ЭП позволяет установить авторство и неизменность содержания ЭД, но не позволяет вычислить закрытый ключ ЭП. Открытый ключ ЭП считается принадлежащим Клиенту, если такой ключ был зарегистрирован в Каталоге открытых ключей Центра регистрации ключей (далее по тексту «ЦРК») Банка (Зарегистрированный ключ ЭП).

1.1.9. **«Закрытый ключ ЭП»** - криптографический ключ (уникальная последовательность символов), известный только Владельцу ключа (Клиенту или Банку соответственно) и хранимый Владельцем в тайне. Закрытый ключ ЭП используется для формирования ЭП.

1.1.10. **«Каталог открытых ключей ЭП»** - база данных Банка, элементами которой являются: наименования/ Ф.И.О. Клиентов - пользователей Системы, действующие открытые ключи ЭП Клиентов и идентификаторы открытых ключей ЭП Клиентов.

1.1.11. **«Сертификат открытого ключа ЭП»** - документ, содержащий информацию об открытом ключе ЭП Клиента: собственно открытый ключ ЭП и его идентификатор. Сертификаты открытого ключа ЭП оформляются и подписываются Клиентом (уполномоченным лицом Клиента) и заверяются его печатью (при наличии). По одному экземпляру сертификата открытого ключа ЭП хранится в Банке и у Клиента.

1.1.12. **«Подтверждение подлинности электронной подписи в электронном документе»** - положительный результат проверки, соответствующим сертифицированным средством ЭП, с использованием криптосистемы «Агава-С», принадлежности ЭП в ЭД Клиенту (Владельцу сертификата открытого ключа ЭП) и отсутствия искажений в подписанном данной ЭП ЭД;

1.1.13. **«Компрометация ключа»** - событие, связанное с утратой доверия к тому, что используемый ключ (пара ключей) обеспечивает безопасность информации. К событиям, связанным с компрометацией ключа (пары ключей), относятся, в том числе, следующие события:

- утрата (в том числе хищение) носителя, на котором записан Закрытый ключ ЭП;
- утрата носителя, на котором записан Закрытый ключ ЭП, с последующим обнаружением;
- увольнение (перевод на другую работу) сотрудника, имевшего доступ к Закрытому ключу ЭП;
- нарушение правил хранения Закрытого ключа ЭП;
- несанкционированное копирование Закрытого ключа ЭП;
- случаи, когда нельзя достоверно установить, что произошло с Закрытым ключом ЭП (в том числе случаи, когда Закрытый ключ ЭП вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

1.1.14. **«Блокировочное слово»** - слово, которое Клиент указывает Банку при регистрации в Системе, запоминает и использует в качестве пароля при обращении по телефону в Банк для временного блокирования работы Клиента в Системе в случае компрометации ключа ЭП.

1.1.15. **Условия** – Условия дистанционного банковского обслуживания по банковским счетам юридических индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк»

1.1.16. **Пароль** – набор (комбинация) букв, цифр, специальных символов созданный Клиентом самостоятельно, используемый для идентификации Клиента и предоставляющий доступ к Системе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Условия определяют порядок осуществления Банком дистанционного банковского обслуживания Счетов Клиента (ДБО) с использованием Системы с доступом через сеть Интернет с предоставлением Клиенту следующих услуг:

- Прием от Клиента ЭПД, подписанных ЭП, на выполнение операций по Счетам Клиента, указанным в Заявлении о предоставлении КБО;
- Предоставление Клиенту информации об операциях, совершенных по Счету, в виде ЭД, подписанных ЭП;
- Обмен информацией (служебные документы, информационные сообщения, переписка) в виде ЭД, подписанных ЭП.

2.2. Проведение операций по Счету на основании ЭПД Клиента осуществляется в порядке и на условиях, установленных Правилами.

2.3. Заключение сторонами Договора не препятствует (не запрещает) проведению операций по Счету Клиента на основании Распоряжений Клиента или третьих лиц, составленных на бумажном носителе.

2.4. Использование ЭПД, подписанных ЭП, не изменяет содержания установленных законодательством и Договором банковского счета прав и обязанностей участников расчетов, содержания платежных документов и правил заполнения их реквизитов.

2.5. Настоящие Условия являются приложением и неотъемлемой частью Правил комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк».

В части, не урегулированной Условиями и не противоречащей им, Стороны руководствуются Общими положениями Правил, опубликованными на официальном Сайте Банка.

Условия являются типовыми для всех Клиентов и определяют в совокупности с Правилами комплексного банковского обслуживания положения Договора на дистанционное банковское обслуживание, заключаемого между Банком и Клиентом.

2.6. Заключение Договора осуществляется в порядке, предусмотренном Правилами.

2.7. Банк с целью ознакомления Клиентов с Условиями и Тарифами размещает указанные Условия и Тарифы в порядке, предусмотренном Правилами.

3. СОГЛАШЕНИЯ СТОРОН

3.1. Стороны при обмене ЭД посредством Системы применяют средства криптозащиты и ЭП в соответствии со стандартами ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.

3.2. Клиент признает, что получение Банком ЭД, подписанных корректной ЭП Клиента, равнозначно получению документов на бумажном носителе, подписанных подписью уполномоченных лиц и заверенных оттиском печати Клиента.

3.3. Банк признает, что получение Клиентом ЭД, подписанных корректной ЭП Банка, равнозначно получению документов на бумажном носителе, подписанных подписью уполномоченных лиц и заверенных оттиском штампа Банка.

3.4. Стороны признают, что при произвольном изменении ЭД (изменение, добавление или удаление символов документа), заверенного ЭП, ЭП становится некорректной, то есть подтверждение подлинности ЭП в ЭД дает отрицательный результат.

3.5. Стороны признают, что подделка ЭП Клиента, то есть подтверждение подлинности ЭП в ЭД от имени

Клиента, практически невозможна без знания закрытого ключа ЭП Клиента.

3.6. Стороны признают, что ЭД, подписанные ЭП Клиента, юридически эквивалентны соответствующим подлинным документам на бумажном носителе, заполненным в соответствии с действующим законодательством Российской Федерации, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами при одновременном соблюдении следующих условий:

- Сертификат открытого ключа, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания ЭД при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭП в ЭД;
- ЭП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

ЭД без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.7. Стороны признают, что ЭД с ЭП Клиента, создаваемые Системой в Банке, являются доказательным материалом для решения спорных вопросов. ЭД, не имеющие ЭП, при наличии спорных вопросов, не являются доказательным материалом.

3.8. Стороны признают, что открытый ключ ЭП Клиента, указанный в заверенном подписью уполномоченного лица Банка Сертификате открытого ключа ЭП Клиента, принадлежит Клиенту.

3.9. Стороны признают в качестве единой шкалы времени при работе с Системой местное поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.10. Стороны установили, что моментом получения ЭД принимающей Стороной в Системе является текущее время по системным часам принимающей Стороны в момент помещения информации в архив входящих сообщений принимающей Стороны.

3.11. Банк исполняет поступившие от Клиента ЭД в пределах операционного времени Банка по месту ведения Счета и в сроки, установленные Федеральным законом «О национальной платежной системе».

3.12. Подлинность ЭП и идентификация владельца закрытого ключа ЭП подтверждается Сертификатом открытого ключа.

3.13. Стороны обеспечивают сохранность архивов ЭД на срок, установленный для хранения соответствующих документов.

3.14. Стороны признают, что используемая Сторонами система защиты информации, которая реализует подписание ЭП и шифрование ЭД, достаточна для обеспечения конфиденциальности, а также подтверждения авторства и контроля целостности ЭД.

3.15. Каждая Сторона несет полную ответственность за обеспечение безопасности и сохранность своих закрытых ключей ЭП, а также за действия своего персонала.

3.16. Стороны признают, что для доступа к Системе, а так же к информации, находящейся в Системе используются многозначные пароли.

3.17. Стороны признают, что через доступ к Системе, полученный Клиентом после ввода Пароля, последний получает доступ к информации об остатках денежных средств на его расчетном счете (счетах), сведений о расчетном счете (счетах), информации об осуществленных операциях по расчетному счету (счетам).

4. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

4.1. С целью предоставления Услуг Банк:

- передает Клиенту на время действия Договора соответствующее программное обеспечение для работы с ЭД и неисключительные (ограниченные) права (простая (неисключительная) лицензия) на использование программного обеспечения;
- подключает программное обеспечение Системы;
- регистрирует Клиента в качестве пользователя Системы.

4.2. До заключения Договора Клиент проинформирован Банком об условиях использования ЭП, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования ЭП. Памятка пользователя Системы по информационной безопасности размещена на Сайте Банка.

4.3. По окончании работ по подключению к Системе Стороны оформляют Акт готовности к эксплуатации Системы (Приложение №5.1.). Дата подписания указанного Акта является датой ввода Системы в действие и является основанием для проведения расчетов между Сторонами.

4.4. Ключи ЭП (закрытый и открытый) подписывающей стороны становятся действующими только после завершения процедур регистрации открытых ключей и ввода в действие закрытых ключей. Ключи являются действующими на момент подписания, если они зарегистрированы и не отозваны подписывающей стороной.

4.5. Ключи со стороны Банка хранятся в вычислительной системе на ресурсе со строго ограниченным доступом.

4.6. Ключи со стороны Клиента сохраняются на стороне Клиента (на съемном носителе информации) в файле с Хранилищем ключей.

4.7. Смена ключей может быть произведена в любой момент по желанию Клиента. Клиент обязан произвести смену принадлежащих ему ключей по требованию Банка. При этом документооборот по Системе временно приостанавливается. Документооборот по Системе восстанавливается после регистрации новых ключей Клиентом и активизации их Банком.

4.8. Подпись документа ЭП производится в Системе автоматически при подготовке документа для другой стороны к отправке.

4.9. Проверка достоверности ЭП производится автоматически при приеме документа.

4.10. При получении ЭД от Клиента Банк производит подтверждение подлинности ЭП в ЭД Открытым ключом ЭП Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность

возникновения дебетового сальдо на расчётном счёте Клиента. В случае отбраковки ЭД Банком не принимается.

4.11. Банк информирует Клиента о совершенных по Счету операциях с использованием ЭП, по крайней мере одним из следующих способов:

- путем присвоения вида и/или описания состояния ЭПД в Системе на «проведен», при этом обязанность Банка по информированию Клиента о совершении операции с использованием ЭП считается исполненной, а Клиент - уведомленным о совершении операции с использованием ЭП с момента присвоения такого вида и/или описания. Стороны условились считать надлежащим доказательством уведомления Клиента о совершенной с применением ЭП операции изготовленную Банком выписку, содержащую полное либо сокращенное наименование либо фамилию, имя и отчество Клиента, его ИНН, дату совершения операции, а также реквизиты платежного документа, на основании которого была совершена операция, а также дату совершения операции и дату присвоения платежному документу в АБС вида и/или описания «проведен», которую Стороны определили датой уведомления о совершенной операции.

- путем отправки уведомлений в электронном виде на электронный почтовый адрес (E-Mail) Клиента, указанный в Заявлении о предоставлении КБО, при этом обязанность Банка по информированию Клиента о совершении операции с использованием ЭП считается исполненной, а Клиент - уведомленным о совершении операции с использованием ЭП с момента отправки Банком уведомления. Стороны условились, что при использовании способа уведомления путем отправки уведомления на электронный почтовый адрес Клиента в случае возникновения спорных ситуаций доказательством надлежащего уведомления Банком Клиента о совершенной операции является выписка, изготовленная Банком на бумажном носителе на основе информации автоматизированной базы данных Банка, содержащая полное либо сокращенное наименование либо фамилию, имя и отчество Клиента, его ИНН, а также текст переданного на электронный почтовый адрес сообщения Клиенту о совершенной операции, при этом Клиент считается уведомленным независимо от того, прочитал ли он сообщение электронной почты, обеспечил ли он проверку указанного в Заявлении о предоставлении КБО почтового ящика e-mail и/или его соединение с сетью интернет для обеспечения приема сообщения Банка, обеспечил ли он иным образом возможность получения направленного Банком электронного письма с уведомлением о совершенной операции;

В случае возникновения споров, связанных с достоверностью ЭП Клиента, корректностью реквизитов и иных споров, связанных с операциями, совершенными с использованием ЭП, Стороны условились считать доказательством уведомления Клиента о совершенной операции любую из указанных в настоящем пункте Условий выписку за подписью Главного бухгалтера Банка (дополнительного офиса) или его заместителя.

4.12. Использование Клиентом ЭП может быть приостановлено или прекращено Банком на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования ЭП в соответствии с настоящими Условиями, а также в иных случаях, предусмотренных настоящими Условиями.

Приостановление или прекращение использования Клиентом ЭП не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

4.13. При выходе из строя аппаратных или программных средств Системы или их элементов, а также в иных случаях невозможности предоставления (получения) Услуг и, соответственно, приостановлении использования Системы, Сторона обязана в течение трех часов известить другую Сторону любым доступным способом, а в течение суток дать письменное сообщение о готовности и сроках возобновления обмена ЭД. На период приостановления использования Системы обмен ЭД между Сторонами осуществляется на бумажных носителях.

4.14. При компрометации или подозрении на компрометацию закрытого ключа ЭП и (или) его использование без согласия Клиента Клиент направляет Банку уведомление об утрате ЭП и (или) его использовании без согласия Клиента и о прекращении действия соответствующего ключа ЭП, предоставив указанное уведомление непосредственно в Банк или отправив Почтой России заказным письмом с обратным уведомлением незамедлительно после обнаружения факта утраты ЭП и (или) его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, при этом факт уведомления устанавливается по правилам, изложенным в п.4.11. настоящих Условий.

4.15. С момента уведомления Стороны выводятся из действия соответствующий открытый ключ ЭП. Скомпрометированные ключи уничтожаются Стороной у которой они находятся.

4.16. Сторона, получившая уведомление о прекращении действия соответствующего ключа ЭП, выводит соответствующий Открытый ключ ЭП из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения уведомления.

4.17. При замене действующего ключа ЭП Клиента по другим причинам, Стороны составляют Акт о завершении действия открытого ключа ЭП Клиента.

4.18. Банк рассматривает заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его ЭП, за исключением уведомлений о прекращении действия соответствующего ключа ЭП в течение 30 (тридцати) календарных дней со дня получения заявления Клиента, а также в течение 60 (шестидесяти) календарных дней со дня получения заявления в случае использования ЭП для осуществления трансграничного перевода денежных средств. О результатах рассмотрения заявления Клиента Банк информирует Клиента передачей электронного служебно-информационного документа по Системе либо в письменной форме по требованию Клиента, в сроки, установленные Условиями для рассмотрения заявлений Клиента.

Правила, установленные настоящим пунктом Условий, не подлежат применению к заявлениям, предусмотренным п.4.14. настоящих Условий.

5.1. Банк обязан:

5.1.1. Передать на время действия Договора программное обеспечение для работы с ЭД и неисключительные (ограниченные) права (простая (неисключительная) лицензия) на использование программного обеспечения.

5.1.2. Обеспечить подключение Клиента к Системе в соответствии с порядком, установленным разделом 4 Условий.

5.1.3. Принимать к исполнению поступившие от Клиента ЭПД, оформленные и переданные в Банк в соответствии с Условиями и подписанные корректной ЭП Клиента.

5.1.5. Не исполнять поступившие от Клиента ЭПД, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных документов Банка России и Условий, а также при отсутствии или некорректности ЭП Клиента.

5.1.6. Предоставлять информацию о совершенных операциях по Счету с использованием ЭП в порядке, установленном Условиями.

5.1.7. Сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе, если это затрагивало ЭД Клиента.

5.1.8. При установлении возможности нарушения безопасности Системы, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы и оповестить Клиента.

5.1.9. По требованию Клиента блокировать в Системе существующий открытый ключ ЭП Клиента и зарегистрировать новый Открытый ключ ЭП Клиента.

5.1.10. По телефонному звонку Клиента с применением блокировочного слова впредь до письменного уведомления временно блокировать работу Клиента в Системе.

5.1.11. В случае блокирования или удаления Открытого ключа ЭП Клиента оповестить его об этом.

5.1.12. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и Условиями.

5.1.13. Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых файлов с ЭД и ЭП на аппаратных средствах Системы в течение не менее тридцати дней после их получения, а в случае возникновения споров - до их разрешения. Обеспечить сохранность архивов переданных и принятых файлов, подписанных ЭП, открытых ключей ЭП Клиента, а также системных журналов в течение срока, установленного действующим законодательством Российской Федерации.

5.1.14. Заверять, в случае необходимости, на основании письменного заявления Клиента в срок не позднее 3 рабочих дней подписями должностных лиц Банка и оттиском штампа Банка распечатанные на бумажном носителе копии ЭД, принятых Клиентом по Системе, подписанных корректной ЭП Банка.

5.1.15. Организовать внутренний режим функционирования установленных по месту нахождения Банка рабочих мест таким образом, чтобы исключить возможность использования Системы и ключей ЭП лицами, не имеющими допуска к работе с Системой.

5.2. Банк имеет право:

5.2.1. В целях обеспечения безопасности при совершении Клиентом платежей с использованием технологии дистанционного обслуживания отказать Клиенту в приеме Распоряжения, подписанного аналогом собственноручной подписи. При этом Клиент может представить непосредственно в Банк аналогичный платежный документ на бумажном носителе, подписанный в соответствии с образцом подписей, имеющимся в карточке с образцами подписей.

5.2.2. Затребовать от Клиента оформления подлинника документа на бумажном носителе, заполненного в соответствии с действующим законодательством Российской Федерации и не производить исполнения ЭД, сообщив об этом Клиенту через Систему или иным способом.

5.2.3. По своему усмотрению без уведомления Клиента блокировать открытый ключ ЭП Клиента, и потребовать от Клиента смены закрытого и соответствующего ему открытого ключей ЭП Клиента.

5.2.4. Отказывать Клиенту после предварительного предупреждения в приеме от него ЭПД на проведение операции по Счету, подписанных корректной ЭП, в случае выявления сомнительных операций Клиента. При этом Банк принимает от Клиента только надлежащим образом оформленные платежные документы на бумажном носителе.

5.2.5. В случаях выявления Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, Банк обязан приостановить предоставление услуг с использованием Систем (приостановить использование Клиентом электронного средства платежа), а также до осуществления списания денежных средств с банковского счета Клиента приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, а также:

- предоставить клиенту информацию о приостановлении Банком исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента и о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия клиента;

- незамедлительно запросить у клиента подтверждение возобновления исполнения распоряжения.

О приостановлении исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, Банк информирует Клиента по телефонам, которые предоставлены Клиентом при заключении и исполнении Договора.

Клиент обязан предоставить подтверждение возобновления исполнения распоряжения по счету в письменном виде на бумажном носителе в срок не позднее 2 (двух) рабочих дней со дня получения запроса, либо предоставить в Банк письменное заявление на бумажном носителе об отзыве распоряжения по счету в срок не позднее 2 (двух) рабочих дней со дня получения запроса от Банка на подтверждение возобновления исполнения

распоряжения по счету.

При получении от Клиента подтверждения возобновления исполнения распоряжения Банк обязан незамедлительно возобновить предоставление услуг с использованием Системы (возобновить использование Клиентом электронного средства платежа) и исполнение Распоряжения.

При неполучении от Клиента подтверждения возобновления исполнения Распоряжения Банк возобновляет предоставление услуг с использованием Системы (возобновляет использование Клиентом электронного средства платежа) и исполнение Распоряжения по истечении двух рабочих дней после дня совершения им действий, предусмотренных настоящим пунктом Условий.

5.2.6. Вводить ограничения или полностью прекратить предоставление Клиенту Услуг в случае выявления попыток сканирования, атак информационных ресурсов Банка, а также иных признаков нарушения безопасности с использованием программно-аппаратных средств Клиента.

5.2.7. Вводить ограничения или полностью прекратить предоставление Клиенту Услуг, включая отказ в приеме ЭПД Клиента о совершении операции по банковскому счету, в случае совершения Клиентом операций с использованием ДБО, имеющих признаки, при наличии которых Банк России рекомендует кредитным организациям уделять повышенное внимание таким операциям.

5.2.8. Блокировать использование ключей ЭП Клиента после окончания срока их действия.

5.2.9. Требовать от Клиента замены (формирования) ключей ЭП при проведении периодической плановой замены ключей ЭП, истечении полномочий и смене лиц, уполномоченных распоряжаться Счетами, компрометации или подозрении на компрометацию закрытых ключей ЭП, нарушении требований по обеспечению безопасности в процессе эксплуатации Системы, а также в случае необходимости проведения регламентных работ по обслуживанию программно-аппаратных средств Системы.

5.2.10. В одностороннем порядке вводить новые, изменять и дополнять действующие Тарифы на услуги Банка, порядок и сроки взимания платы. Информация о действующих тарифах размещается Банком в местах обслуживания Клиента, а также в Интернете на сайте Банка.

5.2.11. Разрабатывать новые версии и предоставлять Клиенту путем передачи по Системе для последующего подключения, обновления программного обеспечения, инструкций по безопасности и использованию Системы.

5.2.12. Привлекать сторонние организации для оказания Клиенту услуг, связанных с подключением и эксплуатацией Системы. В этом случае Банк несет ответственность за качество оказания данными организациями указанных услуг.

5.2.13. Вносить в одностороннем порядке изменения в Систему в случае использования иных сертифицированных средств криптографической защиты, программного обеспечения, предназначенного для вычисления значения хэш-функции и для подтверждения авторства и целостности ЭД, подписанных ЭП, программно-аппаратного комплекса для подключения к защищенной корпоративной VPN-сети, а также порядок применения средств Системы с письменным уведомлением Клиента не позднее, чем за 30 (тридцать) календарных дней до вступления в действие указанных изменений. При не поступлении от Клиента в указанный выше срок заявления в письменной форме о расторжении Договора изменения считаются принятыми.

6. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

6.1. Клиент имеет право:

6.1.1. Получать из Банка следующую информацию:

- справки по остаткам на Счетах Клиента;
- выписки по Счетам;
- справочную информацию, имеющуюся в Системе ;

6.1.2. Пересылать в Банк ЭПД.

6.1.3. Клиент имеет право досрочно прекратить действие своего Открытого ключа ЭП и потребовать от Банка заблокировать этот Открытый ключ ЭП Клиента.

6.1.4. По своему усмотрению создавать новые Закрытые ключи ЭП и соответствующие им Открытые ключи ЭП Клиента и регистрировать в Банке новые Открытые ключи ЭП Клиента.

6.1.5. Позвонив по телефону 8 (8464) 986767, 987825 в Банк впредь до письменного уведомления временно заблокировать свою работу в Системе с применением Блокировочного слова.

6.1.6. В случае возникновения у Клиента претензий, связанных с принятием или непринятием и/или исполнением или неисполнением Банком ЭД, требовать от Банка проведения технической экспертизы в соответствии с разделом 8 Условий.

6.1.7. В любое время производить замену Ключей ЭП Клиента.

6.1.8. Выбрать и определить по своему усмотрению на основании заявления (Приложение №5.5.) , подписанного уполномоченными на распоряжение счетом лицами и скрепленного печатью и переданного нарочно в Банк, предоставляемую Банком возможность, в виде самоограничительных технических пределов и ограничений, границ операций, которые могут осуществляться Клиентом с использованием Системы (далее - самоограничительные технические пределы операции), а именно:

- на максимальную сумму перевода денежных средств за одну операцию;
- на общую сумму переводов денежных средств фактически отправленных за календарную дату;
- времени отправки платежных документов в банк, с указанием периода начала и окончания обслуживания;
- mac-адреса.

Распоряжения по операциям, выходящим за установленные Клиентом самоограничительные пределы (параметры) операций, Банком в Систему не принимаются, отбраковываются и не обрабатываются системой АБС

банка по данным операциям, в связи с чем не требуется и не осуществляется какая-либо дополнительная проверка Банком, в том числе по признакам осуществления перевода денежных средств без согласия клиента Банка России. В этом случае документ Клиента получает статус «Не принят», «Ошибка реквизитов».

Указанные самоограничительные технические пределы операций не являются признаками необычных операций, в т.ч. для целей выявления платежей без согласия клиента в соответствии с п.5.1. статьи 8, п.9.1. статьи 9 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе».

6.1.9. Отозвать ранее переданный ЭПД, имеющий корректную ЭП Клиента, путем направления в Банк по Системе соответствующего уведомления в виде электронного служебно-информационного документа, защищенного ЭП, при условии, что Банк к моменту получения уведомления Клиента не произвел списание со Счета Клиента денежных средств во исполнение ранее полученного от Клиента ЭПД.

6.1.10. Приостановить на срок до шести месяцев предоставление Услуг путем направления не менее, чем за 5 (пять) рабочих дней письменного уведомления с указанием даты начала и срока приостановки предоставления услуг, заверенного руководителем Клиента и оттиском печати Клиента. При этом плата за обслуживание Клиента в Системе за указанный период не взимается.

6.2. Клиент обязан :

6.2.1. Предоставлять рабочие площади на своей территории, необходимые для подготовки к работе Системы, обеспечить необходимые условия и соблюдение сроков проведения работ в соответствии с Условиями.

6.2.2. Заполнять ЭД в соответствии с действующим законодательством Российской Федерации.

6.2.3. Создавать Закрытый ключ ЭП и соответствующий ему Открытый ключ ЭП Клиента на лиц, которым предоставлено право распоряжаться денежными средствами в соответствии с карточкой с образцами подписей и оттиска печати по Счету Клиента. Если в действующей карточке с образцами подписей и оттиска печати, оформленной по форме, предусмотренной Банком, в поле «Подписи второй группы» указаны лица, обладающие правом подписи, то Владелец ключей ЭП Клиента должно быть не менее двух - по одному лицу, указанному в карточке с образцами подписей и оттиска печати в полях «Подписи первой группы», «Подписи второй группы» соответственно. В этом случае Банк принимает к исполнению только ЭД, подписанные двумя ЭП.

6.2.4. Немедленно уведомить Банк о кадровых перестановках лиц, связанных с использованием Системы.

6.2.5. При продлении полномочий представителей – владельцев ЭП создать новый закрытый и соответствующий ему открытый ключ ЭП Клиента и зарегистрировать новый Открытый ключ ЭП Клиента в Банке.

6.2.6. По требованию Банка создать новый закрытый и соответствующий ему открытый ключ ЭП Клиента и зарегистрировать новый Открытый ключ ЭП Клиента в Банке.

6.2.7. В случае проведения плановой регенерации Ключей ЭП по инициативе Клиента проинформировать об этом Банк по Системе за одну неделю до предполагаемой даты регенерации.

6.2.8. Немедленно сообщать Банку об обнаружении попытки несанкционированного доступа к Системе.

6.2.9. В случае внедрения Банком новой версии Системы Клиент обязан исполнить поручение Банка по подключению новой версии в оговоренные сроки.

6.2.10. Оплачивать услуги Банка в порядке и сроки, предусмотренные Условиями.

6.2.11. Хранить в секрете и не передавать третьим лицам (обеспечить конфиденциальность) пароль и носитель с Закрытым ключом ЭП Клиента, используемые в Системе, информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и Условиями.

6.2.12. При установлении возможности нарушения безопасности Системы, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы и оповестить об этом Банк незамедлительно в письменном виде.

6.2.13. Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых файлов с ЭД и ЭП на собственных аппаратных средствах в течение не менее 30 (тридцати) календарных дней после их получения, а в случае возникновения споров - до их разрешения. Обеспечить сохранность архивов переданных и принятых файлов, подписанных ЭП, открытых ключей ЭП Банка, а также системных журналов в течение срока, установленного действующим законодательством Российской Федерации.

6.2.14. Организовывать внутренний режим функционирования рабочих мест уполномоченных лиц таким образом, чтобы исключить возможность использования Системы и ключей ЭП лицами, не имеющими допуска к работе с Системой.

6.2.15. Соблюдать требования и обязательства Клиента по выполнению правил безопасной работы при использовании Системы (Приложение 5.2. к настоящим Условиям).

6.2.16. Производить замену Ключей ЭП уполномоченных лиц в случаях, предусмотренных п.5.2.7. Условий.

6.2.17. Передать Банку в срок не позднее следующего рабочего дня с даты его обращения распечатанную на бумажном носителе и заверенную подписями уполномоченных лиц Клиента и оттиском печати Клиента копию ЭД, принятого Банком от Клиента по Системе, подписанного корректной ЭП уполномоченного лица Клиента.

6.2.18. Предоставить подтверждение возобновления исполнения распоряжения по счету в письменном виде на бумажном носителе в срок не позднее 2 (двух) рабочих дней со дня получения запроса, либо предоставить в Банк письменное заявление на бумажном носителе об отзыве распоряжения по счету в срок не позднее 2 (двух) рабочих дней со дня получения запроса от Банка на подтверждение возобновления исполнения распоряжения по счету.

6.2.19. Использовать предоставленные в соответствии с Договором документацию и инструкции по Системе и программные средства, без права их отчуждения и/или передачи в пользование другим физическим

и/или юридическим лицам, за исключением случаев, прямо предусмотренных действующим законодательством Российской Федерации.

6.2.20. Обеспечивать возможность контроля со стороны уполномоченных Органов за соблюдением требований и условий осуществления лицензируемой деятельности по техническому обслуживанию сертифицированных уполномоченными органами шифровальных средств, используемых в Системе.

6.2.21. В случае утраты ЭП и (или) его использования без согласия Клиента Клиент обязан направить соответствующее уведомление Банку любым доступным для Клиента способом незамедлительно после обнаружения факта утраты ЭП и (или) его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции.

6.3. Клиенту рекомендуется обеспечить информационную безопасность клиентского рабочего места для работы Системы:

6.3.1. Организовать выделенную рабочую станцию, предназначенную исключительно для работы с Банком;

6.3.2. Взаимодействие рабочей станции необходимо ограничить только с необходимым доверенным перечнем IP-адресов;

6.3.3. Подключение рабочей станции к сети Интернет организовать со статического IP-адреса;

6.3.4. Использовать лицензионное программное обеспечение в операционную систему;

6.3.5. Регулярно устанавливать обновления безопасности программного обеспечения операционной системы;

6.3.6. Использовать лицензионное средство защиты от воздействий вредоносного кода и регулярное его обновление;

6.3.7. применять лицензионный персональный межсетевой экран;

6.3.8. произвести перед использованием Системы настройку безопасности операционной системы, а также ограничить права доступа пользователей системы и организовать парольную защиту.

7. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ

7.1. За ДБО, осуществляемое Банком при помощи Системы, Клиент уплачивает Банку плату (вознаграждение) в размере, предусмотренном Тарифами. Оплата услуг Банка осуществляется Клиентом помимо (сверх) платы, установленной соответствующим Договором банковского счета.

7.2. Оплата Услуг по Договору производится Клиентом в порядке, предусмотренном Правилами.

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. Стороны в рабочем порядке урегулируют все споры, возникающие между ними в ходе работы в Системе, за исключением споров, указанных в п. 8.2. Условий.

8.2. Споры Сторон по поводу авторства и неизменности содержания ЭД рассматриваются Экспертной комиссией, формируемой сторонами (далее по тексту - «Комиссия»).

8.3. Претензия предъявляется соответствующей Стороной в письменной форме путем официального вручения под расписку другой Стороне или направления по почте телеграммой либо заказным письмом с уведомлением о вручении.

8.4. Получив претензию, соответствующая Сторона официально в письменной форме информирует другую Сторону о результатах ее рассмотрения в течение 30 (тридцать) календарных дней со дня получения претензии, а также в течение 60 (шестьдесят) календарных дней со дня получения претензии в случае использования ЭП для осуществления трансграничного перевода денежных средств.

8.5. Сторона, предъявившая претензию, в течение 10 (десяти) рабочих дней после получения результатов рассмотрения претензии от другой Стороны должна рассмотреть представленные объяснения и письменно уведомить другую Сторону о снятии претензии или о несогласии с представленными объяснениями.

8.6. Если Сторона не согласна с представленными объяснениями, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты уведомления о несогласии сформировать Комиссию для рассмотрения и разрешения указанного спора по существу.

8.7. До передачи спора на рассмотрение Комиссии Сторонам следует удостовериться, что причиной возникновения спора не является нарушение целостности программного обеспечения, произошедшее в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет, и т.п. В этом случае Стороны руководствуются п. 8.1. Условий.

8.8. В состав Комиссии включается равное количество представителей Банка и Клиента. При необходимости в состав Комиссии могут быть включены независимые эксперты, в частности, представители компании - разработчика Системы. Максимальное количество членов Комиссии не должно превышать 6 (Шести) человек.

8.9. Полномочия представителей Сторон для участия в Комиссии должны подтверждаться оформленными надлежащим образом доверенностями.

8.10. Заседание Комиссии проводится не позднее 5 (Пяти) рабочих дней со дня ее формирования.

8.11. При рассмотрении спора об авторстве и неизменности содержания ЭД Комиссия устанавливает следующие факты:

- предмет спора Сторон;
- перечень ЭД, относящихся к предмету спора;
- идентичность созданного Клиентом ЭД документу на бумажном носителе, распечатанному Банком и хранящемуся в документах дня Банка;

- принадлежность ЭП ЭД Клиенту.
- 8.12. При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:
- данные имеющегося в Банке архива отправленных/принятых ЭД;
 - сертификат(ы) открытого ключа ЭП Клиента, подписанный(ые) Клиентом и хранящийся (хранящиеся) в Банке (Эталонный(е) сертификат(ы)).
- 8.13. Разрешение споров осуществляется на основании результатов проверки ЭП Клиента в спорном ЭД.
- 8.14. Комиссия осуществляет свою работу на территории Банка с использованием персонального компьютера, свободного от вирусов и программных закладок, с установленными на нем эталонными DLL-библиотеками СКЗИ, предоставляемыми R-Style.
- 8.15. Для рассмотрения спора Комиссией Администратор ЦРК Банка предоставляет Эталонный(е) сертификат(ы).
- 8.16. Клиент для рассмотрения спора Комиссией предоставляет сертификат(ы) открытого ключа ЭП Клиента, хранящийся (хранящиеся) у Клиента.
- 8.17. Если инициатором рассмотрения спора является Клиент, Комиссией устанавливается актуальность открытых ключей ЭП Клиента на момент передачи ЭД, являющегося объектом спора. Открытые ключи ЭП Клиента считаются актуальными, если они были зарегистрированы в Каталоге открытых ключей и действовали в момент, когда спорный ЭД был передан Клиентом в Банк.
- 8.18. Принимая во внимание математические свойства алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения сертифицированной ЭП любым лицом, не обладающим закрытым ключом ЭП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания ЭД заключается в доказательстве принадлежности ЭП конкретного ЭД конкретной Стороне.
- 8.19. В целях формирования Протокола проверки ЭП Администратор Центрального абонентского сервера Банка (далее - ЦАС Банка) в присутствии Комиссии осуществляет следующие действия:
- выводит на печать Сертификат открытого ключа ЭП Клиента из Каталога открытых ключей, используя АРМ Клиента
 - сравнивает распечатанный Сертификат открытого ключа ЭП Клиента из Каталога открытых ключей с Эталонным сертификатом, предоставленным Комиссии Администратором ЦРК Банка, а также с аналогичным сертификатом, хранящимся у Клиента и представленным Комиссии Клиентом. Значения открытого ключа ЭП Клиента, содержащиеся в Каталоге открытых ключей, в Эталонном сертификате и в хранящемся у Клиента сертификате, должны совпасть. В случае их несовпадения верным признается Эталонный сертификат;
 - с помощью АРМ Клиента находит спорный документ и, формирует результат проверки ЭП, в котором указываются идентификаторы ключей ЭП, участвовавшие в подписи документа, авторство которого оспаривается;
 - выводит на печать документ со списком идентификаторов подписавших его ключей ЭП. В случае, если спорный ЭД был подписан несколькими ЭП, данная процедура повторяется применительно к каждой ЭП.
- 8.20. Принадлежность ЭП Клиенту и авторство ЭД считается установленным, если идентификаторы открытых ключей ЭП, содержащихся в списке идентификаторов, подписавших ЭД, и Эталонном сертификате совпадают, в Документе сформирована запись «ЭП Корректна», и распечатанный Сертификат открытого ключа ЭП Клиента из Каталога открытых ключей совпадает с Эталонным сертификатом.
- 8.21. Заключение Комиссии оформляется письменно в двух экземплярах - по одному для каждой из Сторон - и подписывается всеми членами Комиссии.
- 8.22. Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.
- 8.23. Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда в соответствии с Условиями Комиссия должна быть создана, возникший спор передается на рассмотрение и разрешение по существу в судебном порядке.
- 8.24. Все иные споры Сторон, связанные с обменом ЭД по Системе, также передаются на рассмотрение в судебном порядке.

9. ОТВЕТСТВЕННОСТЬ СТОРОН

- 9.1. Банк не несёт ответственности за ущерб, причинённый Клиенту, в результате использования третьими лицами закрытого ключа ЭП Клиента.
- 9.2. Банк не несет ответственности за правильность заполнения и оформления Клиентом платежных документов и иных документов.
- 9.3. Банк не несет ответственности за неисполнение платежных документов Клиента в случае возникновения технических неисправностей на стороне Клиента или в коммуникационных системах третьих лиц.
- 9.4. Банк не несет ответственности за состояние технических средств Клиента, правильность установки и настройки системного и прикладного программного обеспечения, а также за их антивирусную защиту.
- 9.5. Банк не несет ответственности за наступившие негативные последствия для Клиента, в случае несвоевременного прочтения полученных им информационных сообщений, переданных Банком через Систему.
- 9.6. Банк не несет ответственности за ущерб, возникший вследствие разглашения уполномоченными лицами Клиента собственного закрытого ключа ЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.
- 9.7. Банк не несет ответственности за последствия исполнения ЭПД, защищенного корректной ЭП Клиента, в т.ч. в случае использования ключей ЭП и программно-аппаратных средств клиентской части Системы

неуполномоченным лицом.

9.8. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к Системе, установленной у Клиента, и криптографическим ключам Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

9.9. При расторжении Договора Стороны несут ответственность по всем ЭД с ЭП Клиента, сформированным в системе, в соответствии с действующим законодательством Российской Федерации.

9.10. Клиент несет ответственность за передачу третьим лицам Пароля доступа к Системе, а равно информации, содержащейся в системе.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Договор заключается на неопределенный срок.

10.2. Стороны вправе расторгнуть Договор в одностороннем порядке путем предупреждения до даты предполагаемого расторжения за один месяц.

10.3. Договор прекращает свое действие в случае расторжения Договоров банковского счета по которым предоставляется Услуга ДБО. В случае, если Договором регулируются правоотношения, связанные с обслуживанием нескольких Договоров банковского счета, то Договор прекращает свое действие только в отношении расторгнутого Договора банковского счета.

10.4. При отсутствии средств на Счете Клиента более двух месяцев, а также в случае отсутствия операций по Счету Клиента более двух месяцев, Банк вправе прекратить ДБО Клиента по Системе и расторгнуть Договор в одностороннем порядке, как в отношении одного из Счетов, так и в отношении всех Счетов Клиента.

11. ПРИЛОЖЕНИЯ

- №5.1. «Акт готовности к эксплуатации Системы»;
- №5.2. «Требования и обязательства Клиента по выполнению правил безопасной работы при дистанционном банковском обслуживании»;
- №5.3. «Заявление о блокировочном слове»;
- №5.4. «Заявления на регистрацию новых Ключей ЭП»;
- №5.5. «Заявление на дополнительные услуги по специальным мерам защиты ЭПД по переводам денежных средств в Системе».

к Условиям дистанционного банковского обслуживания по банковским счетам юридических лиц, индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк»

Акт готовности к эксплуатации Системы

г. Сызрань

года

Общество с ограниченной ответственностью «Земский банк», именуемое в дальнейшем «БАНК», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «КЛИЕНТ», в лице _____, действующего на основании _____, с другой стороны, составили настоящий акт о нижеследующем:

1. В соответствии с Договором на дистанционное обслуживание клиента по Системе № _____ от _____ года, БАНК произвел окончательную регистрацию КЛИЕНТА в Системе, а также передал КЛИЕНТУ программное обеспечение на сменном носителе, а КЛИЕНТ принял указанную работу БАНКА и программное обеспечение.

2. С момента подписания сторонами настоящего акта БАНК считается исполнившим свои обязательства по окончательной регистрации КЛИЕНТА в Системе и передаче необходимого для работы программного обеспечения в полном объеме.

3. Настоящий акт является неотъемлемой частью Договора на дистанционное обслуживание клиента по Системе № _____ от _____ года, составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из сторон.

4. Стороны полностью готовы к началу осуществления операций по Счету с использованием Системы.

5. Начало проведения операций по Счету с использованием Системы: _____ г.

 _____ (_____)
 МП

 МП

к Условиям дистанционного банковского обслуживания по банковским счетам юридических лиц, индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк»

Требования и обязательства Клиента по выполнению правил безопасной работы при дистанционном банковском обслуживании направленные на снижение рисков осуществления переводов денежных средств без согласия Клиента

Настоящим подтверждаю, что ознакомлен до заключения Договора с требованиями и обязательствами по соблюдению безопасности при работе в Системе, мне известны последствия несоблюдения вышеуказанных мер безопасности, и я полностью беру на себя ответственность за такие последствия в случае нарушения мною требований и обязательств по соблюдению безопасности при работе в Системе включая, но не ограничиваясь следующими:

1. Выполнение правил выбора пароля доступа к Системе

-Пароль выбирается самостоятельно;

-Если пароль записан на бумаге, то хранится в месте, недоступном для посторонних лиц;

-Пароль подлежит обязательной смене, если он стал известен постороннему лицу;

-В качестве пароля не используются простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в других системах. Пароль не должен являться копией других паролей пользователя, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете); пароль не должен содержать последовательность одинаковых символов и групп символов (например, не должны применяться пароли, состоящие из одинаковых цифр или из одинаковых букв). Пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.) или распространенным (словарным) словом (например, password, default, admin, guest – это ненадежный пароль). Пароль должен соответствовать следующим требованиям:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛИБС, USER и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

-При возникновении подозрений в осуществлении несанкционированных операций в Системе либо при компрометации пароля на вход в Систему или Средства подтверждения/Ключа ЭП необходимо последовательно выполнить следующие действия:

- Выйти из Системы с помощью кнопки «Выход»;

- Заблокировать устройства, используемые для работы в Системе (в том числе выключить/перевести в режим гибернации (сна) компьютер);

- Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе, аннулирования действия Сертификата/Ключа ЭП. Это можно сделать в офисе Банка, а также по звонку в Банк 8 (8464) 986767, 987825 с последующим оформлением в Банке соответствующих письменных заявлений.

- В письменном заявлении описать обстоятельства компрометации пароля, ключей электронной подписи или несанкционированного доступа либо другую информацию по фактам, вызвавшим Ваши подозрения

2. Исключение доступа посторонних лиц к носителям ключевой информации (дискета, CD, flash-карта, OTP-устройство, USB-токен, смарт-карта, жесткий диск)

-Носители ключевой информации и пароли доступа к ним необходимо хранить в недоступном для окружающих месте отдельно друг от друга;

-По завершении работы в Системе или перерыва в работе носитель ключевой информации извлекается из устройства;

-Хранение носителя ключевой информации осуществляется в условиях, исключающих возможность несанкционированного использования третьими лицами;

-Носитель ключевой информации используется только для подписания ЭД или многофакторной аутентификации;

-Ключ ЭП запрещается копировать или передавать третьему лицу;

- Запрещено осуществлять хранение Ключа ЭП на жестком диске компьютера, в памяти иного устройства, с использованием которого осуществляется выход в Интернет, а также иным способом, делающим данную информацию доступной для третьих лиц;

-В случае смены ответственного лица, осуществляющего подпись ЭД, утере носителя ключевой информации, а также о любом подозрении на компрометацию ключа ЭП незамедлительно сообщается в Банк для блокировки ключа ЭП.

3. Требования к рабочим местам, с которых осуществляется работа с ПО Системы (далее «Рабочие места Системы»):

- Для работы в Системе использовать выделенный персональный компьютер;

- Исключить работу в Системе на персональном компьютере со свободным доступом (Интернет-кафе, бесплатный Wi-Fi и пр.);

- Запрещено использовать системы удалённого управления персональным компьютером, а также привлекать для администрирования и обслуживания данного персонального компьютера ИТ-персонал на условиях предоставления ему удаленного доступа;

- Право доступа необходимо предоставлять лицам, непосредственно осуществляющим работу в Системе;

- Рабочие места Системы запрещается оставлять без контроля (при кратковременном отсутствии средствами операционной системы блокировать Рабочее место Системы).

4. Настройка “доверенной среды” и исключение несанкционированного изменения программного обеспечения на Рабочих местах Системы:

-Используется только лицензионное программное обеспечение;

-Устанавливаются все обновления системы безопасности, рекомендуемые производителем операционной системы, установленной на компьютере;

-Отключается учетная запись для гостевого входа (Guest);

- Использовать для доступа в Систему отдельную учетную запись пользователя компьютера. Доступ к этой учетной записи должен быть защищен паролем, неизвестным любым третьим лицам, включая сотрудников Банка и родственников, удовлетворяющий требованиям п.1 настоящих обязательств;

-Для защиты от несанкционированного доступа из внешней или локальной сети используется и своевременно обновляется специализированное ПО для защиты информации – антивирусное ПО с регулярно обновляемыми базами, персональные межсетевые экраны, средства защиты от несанкционированного доступа и другие технические средства защиты;

-При подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы, работа в Системе немедленно прекращается, а об инциденте сообщается в Банк.

- Не оставлять устройство с активной Системой без присмотра.

- Обязательно осуществлять выход из Системы при необходимости на любое, даже непродолжительное время оставить вне контроля (поля зрения) устройство, на котором осуществляется работа в Системе, и/или устройство.

- После окончания работы в Системе необходимо в обязательном порядке закрыть окно Системы с помощью кнопки «Выход», а также извлечь из компьютера носитель, на котором хранится Сертификат/Ключ ЭП, если операции осуществлялись с его использованием.

-На устройстве, используемом для доступа к Системе, не должно быть установлено программное обеспечение удаленного управления, в том числе TeamViewer, RAdmin, VNC и иное подобное программное обеспечение.

5. Соблюдение правил безопасной работы в сети Интернет на Рабочих местах Системы:

- Не допускается открывать сайт Системы по ссылкам (особенно баннерным или полученным через электронную почту);

- Не допускается отвечать на подозрительные письма с просьбой выслать Закрытый ключ ЭП, пароль и другие конфиденциальные данные Системы;

- Не допускается сохранять на персональный компьютер подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные на форумах;

- Не допускается устанавливать на персональный компьютер и запускаются программы, полученные от недостоверных источников;

- Исключить посещение сайтов сомнительного содержания и любых других Интернет-ресурсов непромышленного характера (социальные и пиринговые сети, конференции и чаты, телефонные сети и т.п.).

- При каждом сеансе работы с Системой через браузер, проверить подлинность соединения, для чего убедиться, что: включен защищенный режим SSL, то есть в адресной строке браузера web-адрес начинается с символов «https://», на зеленом фоне и в окне web-браузера отражается символ «закрытый замок».

- Соединение установлено именно с сервером ООО «Земский банк», то есть в адресной строке интернет-страницы указан точный адрес: <https://ib1.zemsky.ru/RSPortal/StartHTML/example.htm> (не допускается никаких отличий в написании web-адреса, вплоть до любого знака);

- В сертификате сайта в строке «Кем выдан» указано точное значение «zemsky.ru».

- До начала проведения операций в Системе проверить историю входов в Систему на предмет соответствия действительным входам в Систему пользователем, отсутствия в ней сведений о входах с IP-адресов, неизвестных пользователю, а также на предмет отсутствия какой-либо истории, которая может свидетельствовать о нахождении на сайте злоумышленника, а не Банка.

- Необходимо обращать пристальное внимание на неанонсированные Банком изменения страниц входа в Систему и работы с ней (интерфейс Системы), особенно касающиеся безопасности. При возникновении подозрений в подмене злоумышленником страниц Интернет-банка запрещено звонить по номеру телефона, указанному на подозрительной странице, а необходимо незамедлительно связаться с Банком по телефонам 8 (8464) 986767, 987825.

6. Действия в случае возникновения подозрений в осуществлении несанкционированных операций:

При возникновении подозрений в осуществлении несанкционированных операций в Системе либо при компрометации пароля на вход в Систему или Средства подтверждения/Ключа ЭП необходимо последовательно выполнить следующие действия:

- Выйти из Системы с помощью кнопки «Выход»;

- Заблокировать устройства, используемые для работы в Системе (в том числе выключить/перевести в режим гибернации (сна) компьютер);

- Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе, аннулирования действия Сертификата/Ключа ЭП. Это можно сделать в офисе Банка, а также по звонку в Банк 8 (8464) 986767, 987825 с последующим оформлением в Банке соответствующих письменных заявлений.

- В письменном заявлении описать обстоятельства компрометации пароля, ключей электронной подписи или несанкционированного доступа либо другую информацию по фактам, вызвавшим Ваши подозрения;

- Возобновление доступа в систему и возобновление действия Сертификата/Ключа ЭП производится в офисе Банка при личном обращении клиента.

О проявлении злоумышленных действий в Системе, требующих незамедлительного обращения в Банк, могут свидетельствовать следующие факты:

- В истории поручений в Системе указаны поручения, которые Вы не совершали;

- Подозрительная активность на компьютере, с которого осуществляется работа с Системой (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.);

- Входящий звонок от лиц, представляющихся работниками ООО «Земский банк», уведомляющих Вас о регламентных/восстановительных работах в Системе или Банке;

- Получение сообщения о блокировке/разблокировке доступа в Систему;

- Изменение адреса в адресной строке браузера при работе с Системой;

- Наличие в истории входов в Систему информации о входе в Систему с незнакомого IP-адреса; 6.9. невозможность получения доступа к Системе по причине несовпадения пароля при введении заведомо верного пароля;

- Изменение интерфейса или настроек безопасности Системы без предварительного уведомления на сайте Банка.

ООО «Земский банк»

от _____

Для исполнения договора на дистанционное банковское обслуживание
№ _____ от _____
сообщает блокировочное
_____ (наименование организации) _____
слово _____¹⁵

Руководитель

Главный бухгалтер

МП.

¹⁵ Данное заявление вложить в конверт, заклеить и поставить оттиск печати организации на нем.

ООО «Земский банк»

от _____

Прошу Вас дать указание на регистрацию в базе открытых ключей ЭП, используемой для проверки подписи электронных документов, направляемых из (наименование организации) в ООО «Земский банк», в соответствии с договором № _____ от _____ г., следующих уполномоченных сотрудников:

1. _____
2. _____

Подписи следующих сотрудников просим исключить из базы открытых ключей ЭП:

- 1 _____
- 2 _____

Приложение: Сертификат открытого ключа ЭП¹⁶.

(наименование Клиента, должность)

(подпись)

(ФИО)

« ____ » _____ 20__ г.

МП.

¹⁶ Сертификат открытого ключа ЭП предоставляется на каждого сотрудника, имеющего право подписи.

**Заявление на дополнительные услуги по специальным мерам защиты ЭПД по переводам
денежных средств в Системе**

Клиент _____
(наименовании организации)

р/ _____
(наименовании организации)

настоящим определяет по своему усмотрению, в виде самоограничительных технических пределов и ограничений, границ операций, которые могут осуществляться Клиентом с использованием Системы (далее - самоограничительные технические пределы операции) , в связи с чем просит определить пределы (параметры) операций с использованием Системы:

Ограничение на максимальную сумму перевода денежных средств за одну операцию, на сумму _____ руб. 00 коп.

Ограничение на общую сумму переводов денежных средств фактически отправленных за календарную дату, на сумму _____ руб. 00 коп., за день.

Ограничение на временной период (в часах), в который могут быть совершены переводы денежных средств с использованием Системы, с указанием периода начала и окончания обслуживания с _____ до _____.

Ограничение по мас-адресам _____, _____.

Распоряжения по операциям, выходящим за установленные Клиентом самоограничительные пределы (параметры) операций, Банком в систему не принимаются, отбраковываются и не обрабатываются системой АБС банка по данным операциям, в связи с чем не требуется и не осуществляется какая-либо дополнительная проверка Банком, в том числе по признакам осуществления перевода денежных средств без согласия клиента Банка России. В этом случае Клиента документ получает статус «Не принят», «Ошибка реквизитов». Указанные самоограничительные технические пределы операций не являются признаками необычных операций, в т.ч. для целей выявления платежей без согласия клиента в соответствии с п.5.1. статьи 8, п.9.1. статьи 9 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе».

Клиент: _____ / _____ /

М.П.

ОТМЕТКИ БАНКА

Реквизиты Клиента указаны верно, соответствуют представленным документам.

Подпись Клиента проверена по карточке образцов подписей и соответствует оригиналу.

(должность сотрудника Банка)

(подпись)

(наименование офиса)

М.П.