##### ДОГОВОР ОБ ОБСЛУЖИВАНИИ

**банковского счета с**

**использованием документов в электронной форме**

 г. \_\_\_\_\_\_\_\_\_\_\_ «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ года

Акционерное общество Банк «Тамбовкредитпромбанк», именуемый в дальнейшем "Банк" в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем "Клиент", в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, далее совместно именуемые Стороны, заключили настоящий Договор о нижеследующем:

**1. ПРЕДМЕТ ДОГОВОРА**

1.1. Банк обязуется обслуживать указанные в Заявке на изготовление сертификата (приложение № 3 к настоящему договору, являющиеся его неотъемлемой частью) банковские счета Клиента с помощью корпоративной системы обмена электронными документами (именуемой в дальнейшем «Система») - программно–аппаратного комплекса, позволяющего осуществлять посредством глобальной компьютерной сети Интернет обмен электронными (в том числе электронными расчетными) документами в соответствии с Договором банковского счета.

Электронные документы (именуемые в дальнейшем «документы») – документы, в которых информация представлена в электронной форме и заверена электронной подписью.

1.2. На основании настоящего Договора Клиент вправе с использованием Системы осуществлять расчетные операции по своему банковскому счету, а также осуществлять обмен электронными документами между участниками Системы.

К участникам Системы относятся оператор, осуществляющий информационное и технологическое обслуживание Банка в Системе, Банк, Клиент.

**2. ОБЩИЕ УСЛОВИЯ СОВЕРШЕНИЯ РАСЧЕТОВ В ЭЛЕКТРОННОМ ВИДЕ**

2.1. Электронные документы передаются с использованием средств Системы, при этом обмен документами на бумажных носителях сторонами не производится, кроме случаев, предусмотренных настоящим Договором, в частности при возникновении обстоятельств непреодолимой силы или возможных нарушениях работы Системы.

В качестве электронных расчетных и иных документов, являющихся основанием для осуществления Клиентом операций по счету (далее «расчетные документы»), стороны используют форматы документов, установленные Банком и/или Системой с учетом требований действующего законодательства, Банка России.

Стороны признают, что полученные с помощью Системы расчетные документы, заверенные электронной подписью, юридически эквивалентны документам, составленным на бумажном носителе, подписанным собственноручной подписью Клиента или лица, уполномоченного доверенностью распоряжаться банковским счетом, и являются основанием проведения операций по счету Клиента.

2.2. Электронная подпись представляет собой реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать Клиента, а также установить отсутствие искажения информации в документе.

Закрытый ключ – уникальная последовательность символов, известная Клиенту, и предназначенная для создания в документах электронной подписи.

Электронная подпись представляет собой уникальную последовательность символов, соответствующую закрытому ключу, доступную любому участнику Системы и предназначенную для подтверждения подлинности электронной подписи в электронном документе.

2.3. Стороны признают, что способы защиты информации и средства аутентификации, используемые при передаче электронных документов, достаточны для подтверждения авторства и подлинности документов и обязуются выполнять режим обеспечения безопасности, установленный правилами Системы. К исполнению документы принимаются только при их аутентификации в соответствии с правилами Системы.

2.4. Стороны также признают, что:

2.4.1. при любом изменении электронного документа, совершенном после подписания такого документа электронной подписью одной из Сторон, электронная подпись становится некорректной;

2.4.2. знание информации, которая передается между Сторонами по каналу связи Системы, не приводит к компрометации секретных ключей подписи Сторон;

2.4.3. подделка одной Стороной электронной цифровой подписи другой Стороны, т.е. создание корректной электронной подписи, невозможна без знания секретного ключа Стороны;

2.4.4. созданный в единственном экземпляре в рамках настоящего Договора секретный ключ Клиента уникален, создание дубликата секретного ключа возможно только Клиентом или при нарушении Клиентом условий хранения и/или при нарушении условий использования секретного ключа, предусмотренных настоящим Договором;

2.4.5. каждая Сторона несет ответственность за сохранение в тайне своих секретных ключей подписи, за правильность заполнения и оформления электронных документов и за действия своего персонала, уполномоченных лиц при работе с Системой.

2.4.6. заключая настоящий Договор и проводя операции с использованием Системы, Клиент соглашается с тем, что привлечение Банком оператора и удостоверяющего центра к осуществлению операций с использованием Системы (в частности, при формировании и передаче документов через процессинговый центр оператора) не является нарушением Банком банковской тайны.

**3. ПОРЯДОК АККРЕДИТАЦИИ КЛИЕНТА В СИСТЕМЕ**

3.1. Аккредитация в Системе представляет собой предоставление Клиенту права использовать Систему для обмена электронными документами с Банком и иными участниками Системы.

3.2. Аккредитация Клиента осуществляется Банком и заключается в:

3.2.1. проверке полномочий лиц, уполномоченных Клиентом распоряжаться денежными средствами на счете, и документов, подтверждающих полномочия;

3.2.2.создании ключевой информации Клиента (открытого и секретного ключей электронной подписи);

3.2.3. передаче Клиенту Сертификата ключа подписи – электронного документа, выдаваемого удостоверяющим центром для подтверждения подлинности электронной цифровой подписи и идентификации участника Системы, удостоверенного электронной цифровой подписью удостоверяющего центра (в дальнейшем «Сертификат»).

3.3. Основанием для аккредитации Клиента в Системе и создания удостоверяющим центром Сертификата Клиента является заявка, составляемая Клиентом по форме Приложение № 3 к настоящему договору, являющиеся его неотъемлемой частью. Заявка составляется в письменной форме на бумажном носителе, подписывается собственноручной подпис*ь*ю Клиента или представителя Клиента, имеющего право подписывать платежные документы, и предоставляется в Банк.

Клиент обязан предоставить копии паспорта лица, ответственного за работу с системой «Интернет-банк», лица, уполномоченного на получение ключа электронной подписи, и лица, на которого изготовляется Сертификат ключа.

При передаче Клиенту Сертификата, созданного удостоверяющим центром, Клиент или представитель Клиента, имеющий право подписывать платежные документы, подписывает собственноручной подписью Акт о признании электронной подписи к настоящему договору (приложение № 2 к настоящему договору).

3.4. Передаваемый Банком Клиенту Сертификат содержит следующие реквизиты:

* уникальный идентификатор (DN) владельца Сертификата (Клиента или физического лица, уполномоченного от имени Клиента распоряжаться вкладом/средствами на счете),
* даты начала и окончания срока действия Сертификата,
* фамилию, имя, отчество владельца Сертификата ключа подписи,
* наименование средств электронной цифровой подписи, с которыми используется открытый ключ электронной цифровой подписи,
* открытый ключ электронной цифровой подписи,
* уникальный серийный номер Сертификата, присвоенный удостоверяющим центром,
* идентификатор (DN) создавшего Сертификат удостоверяющего центра,
* наименование и место нахождения удостоверяющего центра.

3.5. Информация о выданных удостоверяющим центром Сертификатах содержится в реестре сертификатов ключей подписей. Обеспечение актуальности реестра и возможности свободного доступа к нему Клиента осуществляется удостоверяющим центром.

3.6. Банк в течение 15 рабочих дней с момента подачи Клиентом заявки предоставляет Клиенту секретный ключ, а также предоставляет Клиенту в электронной форме необходимую документацию о порядке работы Системы и осуществления операций с ее помощью.

3.7. Аккредитация Клиента подтверждается выдачей Клиенту Сертификата, с момента получения которого Клиент вправе осуществлять операции с использованием Системы.

3.8. Срок действия Сертификата составляет один календарный год с даты начала действия Сертификата. Продление срока действия Сертификата на новый срок оформляется выдачей нового Сертификата с обязательной сменой ключей не позднее 15 дней до момента окончания срока действия Сертификата.

Процедура продления срока действия сертификата может быть осуществлена:

* самостоятельно Клиентом, при этом он обязан сообщить Банку уникальный номер запроса, назначаемый в процессе продления;
* путем обращения в Банк, при этом Клиент предоставляет в Банк заявку, ключевой носитель и пин-код для доступа к нему.

По результатам продления составляется Акт о признании электронной подписи, который должен быть подписан обеими сторонами.

**4. ПОРЯДОК СОВЕРШЕНИЯ РАСЧЕТОВ В ЭЛЕКТРОННОМ ВИДЕ**

4.1. Банк обязан осуществлять платежи на основании расчетных документов в электронной форме при условии соответствия этих документов требованиям законодательства РФ, договора банковского счета, форматам, установленным Банком и/или Системой, наличия корректной электронной подписи.

Осуществление операций с использованием Системы возможно при наличии у Клиента доступа в Интернет, подключение к которому оформляется Клиентом самостоятельно.

4.2. В случае несоответствия электронного расчетного документа требованиям, предусмотренным п.п. 4.1., угрозы несанкционированного доступа к счетам Клиента (поступления поврежденных документов) Банк отказывает в приеме документов, уведомив об этом Клиента в электронном виде с указанием причины отказа.

4.3. Прием электронных документов производится Банком круглосуточно. Исполнение документов осуществляется Банком в течение операционного времени ежедневно с 9-00 до 16-00 за исключением выходных и праздничных дней. Документы, поступившие в Банк после окончания операционного дня, считаются поступившими и подлежат исполнению в следующий операционный день.

4.4. Прием документов подтверждается электронным извещением Банка с указанием времени приема документа.

При возникновении разногласий в правильности указания времени приема документа Стороны признают, что временем приема документов является текущее время по системным часам аппаратных средств Банка.

Банк информирует клиента об исполнении каждого электронного документа путем направления клиенту соответствующего извещения (протокола операции) с использованием Системы.

Документальным подтверждением факта совершения операции с использованием Системы является протокол проведения операции в Системе, подтверждающий корректную идентификацию и аутентификацию Клиента и совершение операции.

4.5. Клиент обязан получать заверенную электронной подписью Банка выписку по счету, самостоятельно связываясь с Банком. Движение средств по счету считается подтвержденным, если Клиент не представил свои замечания в течение 10 дней с даты совершения операции.

4.6. Клиент имеет право отозвать документ в день его отправки. Отзыв принимается Банком только в случае неисполнения документа до момента получения отзыва и наличия технологической возможности отменить исполнение документа.

4.7. По отдельным документам Банк вправе запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе либо иным образом в день получения документа. В этом случае документ принимается после получения требуемого подтверждения.

4.8. Любая из Сторон предоставляет другой Стороне по первому обоснованному требованию подписанные собственноручной подписью Клиента/уполномоченного лица распечатанные документы, принятые от нее по Системе и заверенные ее электронной подписью.

4.9. При смене лица, обладающего правом подписи электронных документов, изменении данных, идентифицирующих Клиента/уполномоченного лица, смене ключей подписи, в иных случаях, прекращающих действие Сертификата, Сертификат подлежит замене.

Смена ключей должна быть произведена немедленно в случае угрозы несанкционированного доступа к счету Клиента, изменений состава лиц, имеющих доступ к Системе (обладающих правом использования секретного ключа).

**5. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

5.1. Клиент обязан реализовать перечень мероприятий согласно Требованиям по обеспечению информационной безопасности, изложенных в приложении 6. Документальным подтверждением выполнения этих требований служит проведённая Клиентом самостоятельная оценка в соответствии с Приложением 7, которая впоследствии утверждается и предоставляется в Банк. Банк вправе отказать Клиенту в подключении к Системе при неудовлетворительном результате оценки (до момента достижения положительной оценки).

Клиент обязан предоставлять в Банк документальное подтверждение выполнения Требований по обеспечению информационной безопасности при заключении Договора, при ежегодном продлении срока действия Сертификата, а также по запросу Банка.

5.2 Клиент обязан немедленно уведомить Банк любым доступным способом в случае несанкционированного доступа к Системе, в случае утери материального носителя, содержащего секретный ключ, изменения состава лиц, обладающих правом использования секретного ключа, ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности, но не позднее дня, следующего за днем получения от Банка извещения о совершенной операции.

Любое устное уведомление должно быть подтверждено письменным сообщением клиента по форме Приложения № 5 к Договору или в произвольной форме.

После получения уведомления Клиента Банк обязан возместить Клиенту сумму операции, совершенной без согласия Клиента после получения указанного уведомления.

В случае если Банк не исполняет обязанность по информированию Клиента о совершенной операции в соответствии с п.4.4 настоящего договора, Банк обязан возместить Клиенту сумму операции, о которой Клиент не был проинформирован и которая была совершена без его согласия.

В случае если Банк исполняет обязанность по информированию Клиента о совершенной операции в соответствии с п.4.4 настоящего договора и Клиент не направил Банку соответствующее уведомление, Банк не обязан возмещать Клиенту сумму операции, совершенной без согласия Клиента.

Бремя доказывания надлежащего исполнения обязательств, установленных настоящим пунктом, лежит на Клиенте.

При обнаружении Банком признаков (фактов) нарушения безопасности Системы Банк немедленно приостанавливает прием электронных документов и любым доступным способом извещает Клиента.

5.3. В случаях выхода из строя аппаратных или программных средств Системы или их элементов, в иных случаях невозможности осуществления электронных платежей на основании электронных документов Стороны обязаны в течение трех часов известить друг друга любым доступным способом, при этом Клиент вправе осуществлять платежи в иной форме в соответствии с договором банковского счета. Стороны должны известить друг друга о готовности и сроках возобновления проведения расчётов в электронном виде.

5.4. В течение срока действия настоящего Договора Клиент вправе в любое время прекратить передачу электронных документов, а Банк обязан прекратить прием документов с момента поступления соответствующего требования от Клиента. Требование может быть направлено Клиентом с использованием Системы.

Стороны определили, в течение срока действия настоящего Договора допускается временное приостановление Банком, оператором работы Системы не более, чем на четыре часа в сутки.

5.5. Банк обязуется формировать и поддерживать архивы:

* всех входящих/исходящих электронных документов в принятом/в исходном виде с электронной подписью;
* извещений (в электронном виде с электронной подписью) о приеме электронных документов;
* сообщений свободного формата, подписанных электронной подписью;
* электронных протоколов сеансов обмена информацией;
* средств проверки подлинности электронной подписи;

и несет ответственность за их целостность и достоверность. Порядок формирования и поддержания архивов определяется Банком. Необходимость формирования и поддержания архивов Клиентом определяется им самостоятельно.

Сроки хранения электронных расчетных документов должны соответствовать срокам хранения, установленным для хранения расчетных документов на бумажных носителях. Иные архивы поддерживаются Банком в течение не менее трех лет (а в случае возникновения споров – до их разрешения).

5.6. Клиент вправе обращаться в Банк за получением бесплатных консультаций, связанных с эксплуатацией Системы, по телефону в течение всего срока действия настоящего Договора.

5.7. Банк в праве, руководствуясь действующим законодательством, после предварительного предупреждения в письменной форме отказывать Клиенту в приеме от него распоряжений на проведение операций по банковскому счету, переданных в Банк с использованием системы «Интернет-Банк».

5.8. По истечении срока действия сертификата Банк вправе в одностороннем порядке приостановить прием распоряжений Клиента на проведение операций по банковскому счету, переданных в Банк с использованием системы «Интернет-Банк» вплоть до получения от него подписанного Акта о признании обновленной электронной подписи.

5.9. Банк в праве:

 - запрашивать от клиента документы и сведения, необходимые Банку для осуществления функций, предусмотренных действующим законодательством Российской Федерации и нормативными актами Банка России;

 - после предварительного предупреждения в письменной форме, **отказать** Клиенту в приеме от него распоряжений на проведение операций по банковскому счету, переданных в Банк с использованием системы «Интернет-Банк», **приостановить обслужива**ние клиента с использованием системы «Интернет-Банк» в случае, если у Банка возникают подозрения, что операции осуществляются Клиентом с целью легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

- возобновить обслуживание Клиента с использованием системы «Интернет-Банк», при условии удовлетворения требований, предусмотренных действующим законодательством, при условии:

а) личного обращения в кредитную организацию физического лица, исполняющего функции единоличного исполнительного органа клиента;

б) после предоставления Клиентом документов и сведений, запрошенных Банком.

 - в одностороннем порядке приостановить прием распоряжений Клиента на проведение операций по банковскому счету, переданных в Банк с использованием системы «Интернет-Банк», по истечении срока действия сертификата, вплоть до получения от него подписанного Акта о признании обновленной электронной подписи.

5.10. Клиент обязан предоставлять документы и сведения, необходимые Банку для осуществления функций, предусмотренных действующим законодательством Российской Федерации и нормативными актами Банка России, в том числе:

сведений о клиенте, представителе клиента, выгодоприобретателе, бенефициарном владельце, документов с расчетом сумм НДФЛ, исчисленных и удержанных им в качестве налогового агента, как минимум, за последний отчетный период, документов (в том числе в виде выписок с банковских счетов, открытых клиенту в других кредитных организациях), подтверждающих исполнение клиентом своей обязанности по уплате налогов или других обязательных платежей в бюджетную систему Российской Федерации, оплату коммунальных услуг, арендных платежей за недвижимое имущество и иных платежей, связанных с деятельностью клиента, документов по определению источников происхождения денежных средств и (или) иного имущества клиента, договора, (контракты) и (или) иные документы.

5.11. Клиент имеет право, в случае отказа/приостановления в приеме от него распоряжений на проведение операций по банковскому счету, переданных в Банк с использованием системы «Интернет-Банк» предоставить в Банк надлежащим образом оформленный расчетный документ на бумажном носителе, который исполняется Банком в соответствии с действующим законодательством и договором банковского счета.

5.12. В случае возникновения у Банка подозрений, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма Банком реализуется право, предусмотренное п. 5.2 и 11 статьи 7 Федерального Закона от 07.09.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

**6. ОТВЕТСТВЕННОСТЬ СТОРОН**

6.1. Банк не несёт ответственности за ущерб, возникший вследствие неправильного оформления Клиентом расчетных документов, за срывы и помехи в работе используемой Клиентом линии связи, приводящих к невозможности передачи в Банк документов, в случаях воздействия на программно-аппаратные комплексы вредоносных программ, неправомерного доступа к программно-аппаратным комплексам Клиента, несанкционированного использования электронной подписи неуполномоченными на это Клиентом лицами.

6.2. Банк не несет ответственности в случаях финансовых потерь и других негативных последствий, возникших в связи с нарушением и (или) ненадлежащим исполнением Клиентом требований по обеспечению информационной безопасности (Приложение 6).

6.3. В случае возникновения форс-мажорных обстоятельств (стихийных бедствий; аварий; пожаров; массовых беспорядков; повреждений линий связей; забастовок; военных действий; противоправных действий третьих лиц; вступления в силу законодательных актов, постановлений и распоряжений государственных органов власти, препятствующих выполнению Сторонами своих обязательств по настоящему Договору), а также других обстоятельств, не зависящих от воли Сторон, Стороны приостанавливают обмен финансовыми документами на все время действия форс-мажорных обстоятельств и обязуются в разумно короткий срок с момента наступления таких обстоятельств уведомить друг друга об их наступлении любым возможным видом связи.

**7. Конфиденциальность.**

7.1. К конфиденциальной информации относятся сведения об остатках и операциях по счетам, контрагентах, технических и технологических особенностях удаленного обслуживания, методах обеспечения безопасности информации, персональные данные физических лиц.

7.2. Стороны обязуются:

* обеспечить конфиденциальность полученной информации и не использовать её для своей собственной выгоды или выгоды третьих лиц;
* в целях обеспечения безопасности конфиденциальной информации принимать все необходимые меры, в том числе меры по предотвращению утечки, хищения, утраты, искажения, подделки, а также несанкционированной обработки;
* не раскрывать и не передавать конфиденциальную информацию какой-либо третьей стороне, а также не предпринимать каких-либо действий, результатом которых может стать её разглашение, за исключением случаев исполнения договорных обязательств, требований законодательства РФ или запросов государственных органов.
* незамедлительно сообщать другой стороне о допущенном либо ставшем известном факте или угрозы разглашения, незаконном получении или использовании конфиденциальной информации.

7.3. Стороны несут ответственность за разглашение или несанкционированное использование полученной Конфиденциальной информации.

**8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ**

8.1. При возникновении разногласий и споров, связанных с исполнением Сторонами настоящего Договора, Стороны обязуются решать их путем переговоров. На время разрешения спорной ситуации, связанной с исполнением Банком поручения Клиента, Банк имеет право приостановить действие настоящего Договора в одностороннем внесудебном порядке с последующим уведомлением Клиента.

8.2. Если одна из Сторон предъявляет другой Стороне претензию по документу, а также подтверждение другой Стороны о получении такого документа, а другая Сторона не может представить архивную копию спорного документа вследствие ненадлежащего хранения архива, виновной признается Сторона, не представившая архивную копию спорного документа.

8.3. Споры, по которым не достигнуто соглашение Сторон, разрешаются в суде в соответствии с действующим законодательством Российском Федерации.

8.4. При возникновении споров, связанных с принятием или неприятием и/или с исполнением или неисполнением документа в электронной форме, Стороны обязаны соблюсти порядок разрешения спорных ситуаций, изложенный в Приложении №1, являющемся неотъемлемой частью настоящего Договора.

**9.** **ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ**

9.1 Настоящий Договор является неотъемлемой частью и действует в течение срока действия договора банковского счета № \_\_\_ от «\_\_» \_\_\_\_ 20\_\_ г., заключенного между Сторонами при открытии счета, номер которого указан в Заявке на изготовление сертификата (приложение № 3 к настоящему договору, являющиеся его неотъемлемой частью).

9.2. Исполнение сторонами обязательств по Договору приостанавливается с момента окончания срока действия Сертификата и до момента оформления Клиенту нового Сертификата. В течение этого срока стороны не вправе проводить в Системе какие-либо операции, а Банк прекращает прием электронных документов.

Если по истечении 30 календарных дней с даты окончания срока действия Сертификата Клиент не обратился в Банк за оформлением нового Сертификата, настоящий Договор прекращается без дополнительного уведомления Банком Клиента.

9.3. Настоящий Договор подлежит прекращению в случае прекращения действия Договора банковского счета.

9.4. Любая Сторона вправе расторгнуть настоящий Договор в одностороннем порядке досрочно, предупредив другую Сторону в письменной форме не менее чем за 30 (тридцать) дней до предполагаемой даты расторжения.

Досрочное расторжение Договора возможно при условии выполнения Сторонами обязательств, предусмотренных настоящим Договором, приложениями к Договору.

9.5. В случае необходимости внесения изменений либо дополнений в Систему, по взаимному согласию Сторон настоящий Договор может быть изменен или дополнен приложениями к нему при обязательном соблюдении их письменной формы и подписании уполномоченными представителями Сторон.

9.6 В случаях, не предусмотренных настоящим Договором, Стороны руководствуются действующим законодательством, банковскими правилами и соответствующим договором банковского счета.

**10. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН:**

**БАНК:**

Акционерное общество Банк «Тамбовкредитпромбанк»

юридический адрес: 392000, г. Тамбов, ул. Советская, 118

адрес для переписки: 392000, г. Тамбов, ул. Советская, 118

ИНН 6829000028, ОКПО - 09263511, к/с № 30101810600000000755 в ГРКЦ ГУ ЦБ Банка России г. Тамбова,

БИК 046850755

Тел. (4752) 559-777 Факс. (4752) 559-777

**КЛИЕНТ:**

Подписано от **БАНКА:** Подписано от **КЛИЕНТА:**

Подпись: ..................................................... Подпись: .................................................

Ф.И.О: Ф.И.О:

Должность: Должность:

 М.П. М.П.

Приложение № 1 к Договору об обслуживании банковского счета с использованием документов в электронной форме

Порядок разрешения спорных ситуаций, связанных с принятием (неприятием) и/или

исполнением (неисполнением) документа в электронной форме

1. Любые споры в отношении авторства и/или подлинности документа, переданного с использованием Системы, подписанного Секретным ключом и предназначенного для проверки Сертификатом, зарегистрированным в Системе, разрешаются между участниками путем проведения переговоров.

2. При невозможности разрешения спора в отношении авторства и/или подлинности документа, подписанного Секретным ключом, путем переговоров, участники вправе обращаться к разработчику (оператору) Системы, имеющему эталон программного обеспечения Системы (далее Оператор), с письменным заявлением о создании экспертной комиссии для разрешения спора.

Оператор принимает участие в урегулировании разногласий между участниками при условии заблаговременного предоставления Оператору всех документов, касающихся возникших разногласий, документов, подтверждающих полномочия сторон, государственную регистрацию сторон, а также иных документов, дополнительно затребованных Оператором.

Экспертная комиссия создается из уполномоченных представителей Сторон с равным количеством членов комиссии с каждой Стороны и представителей Оператора. Не предоставление одним из участников со своей стороны членов комиссии не является основанием для отложения или не рассмотрения заявления. В таком случае заключение об авторстве и/или подлинности электронного документа делается только представителями Оператора.

3. Экспертная комиссия создается и приступает к работе в двухнедельный срок с момента поступления письменного заявления от заинтересованного участника. Экспертная комиссия осуществляет свою работу на территории Оператора и должна вынести свое заключение, оформленное соответствующим актом, в месячный срок с момента начала работы. Акт комиссии признается имеющим силу в случае согласия с содержащимся в нем решении большинства членов комиссии. В случае несогласия с решением комиссии, член комиссии вправе указать в решении своё мотивированное особое мнение.

4. Для разрешения спора о подлинности документа, подписанного Секретным ключом, заинтересованный участник предоставляет Оператору для передачи экспертной комиссии:

1. спорный документ в электронном виде;
2. спорный документ на бумажном носителе;
3. акт о передаче Клиенту Сертификата, подписанный участниками, с указанием идентификатора Сертификата (DN) участника.

5. Для проверки подлинности документа, подписанного Секретным ключом, и достоверной идентификации Сертификата используется Эталонный Модуль Проверки подписи документа, хранящийся у Оператора. Результатом работы такого Эталонного Модуля Проверки является:

* установление факта создания спорного документа с использованием Системы;
* установление факта подписи спорного документа в соответствии с технологией Системы;
* установление факта целостности спорного документа
* раскрытие информации об идентификаторе Сертификата (DN), соответствующего Секретному ключу, использованному для подписи спорного документа.

6. Экспертная комиссия сравнивает данные идентификатора Сертификата (DN), содержащиеся в акте о передаче Сертификата и полученные в результате работы Эталонного Модуля Проверки подписи документа.

7. Подтверждением подлинности электронного документа является единовременное наличие следующих условий:

* подтверждена подлинность Секретного ключа, использованного для подписи спорного документа;
* подтверждена целостность спорного документа;
* идентификатор Сертификата (DN), содержащийся в акте о передаче Сертификата, и идентификатор Сертификата (DN), полученный в результате работы Эталонного Модуля Проверки подписи документа, совпадают;
* получен положительный результат проверки спорного документа на соответствие технологии Системы.

 В указанном случае экспертной комиссией составляется акт о признании подлинности документа, подписанного Секретным ключом.

 8. При отсутствии одного или нескольких из вышеперечисленных условий (п.7), экспертной комиссией составляется акт о не признании подлинности документа, подписанного Секретным ключом. Акты, составленные экспертной комиссией, являются доказательством при дальнейшем разбирательстве спора.

9. Подтверждение экспертной комиссией подлинности документа, подписанного Секретным ключом, принятого по Системе, означает, что этот документ имеет юридическую силу.

 10. Не подтверждение экспертной комиссией подлинности документа, подписанного Секретным ключом, принятого по Системе, означает, что этот документ не имеет юридической силы.

11. Если по результатам работы экспертной комиссии Стороны не достигли договоренности, либо одна из Сторон не согласна с выводами экспертной комиссии, дальнейшее разбирательство спора продолжается в установленном действующим законодательством порядке в Арбитражном суде.

Банк Клиент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 2 к Договору об обслуживании банковского счета с использованием документов в электронной форме

**А К Т**

**о признании электронной подписи к Договору об обслуживании банковского счета с использованием документов в электронной форме**

|  |  |
| --- | --- |
|  | «\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г. |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** именуемый в дальнейшем Клиент**,** в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и АО Банк «ТКПБ», именуемый в дальнейшем Банк, в лице \_\_\_\_\_\_\_\_\_\_\_, составили настоящий Акт о нижеследующем:

 1. В соответствии с условиями Договора об обслуживании банковского счета с использованием документов в электронной форме Банком произведена Аккредитация\_\_\_\_\_\_\_\_\_\_\_ в Системе в качестве Клиента.

 2. В соответствии с условиями Договора об обслуживании банковского счета с использованием документов в электронной форме и запросом Клиента Банком был создан Секретный ключ и Электронный сертификат (Сертификат) со следующими параметрами**:**

**Наименование Сертификата:**

**Версия:**

**Номер Сертификата:**

**Алгоритм подписи:**

**Кем заверен:**

**Годен с:**

**Годен до:**

**Алгоритм публичного ключа:**

**Открытый ключ:**

**Алгоритм отпечатка:**

**Отпечаток:**

Носитель ключа: смарт-карта.

 3. Электронный сертификат (сертификат) и Секретный ключ был получен Клиентом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и зарегистрирован в Системе.

 4. Срок действия Электронного сертификата (Сертификата) составляет 1 (Один) календарный год с момента его изготовления.

5. Ответственное лицо, уполномоченное Клиентом получить Электронный сертификат (сертификат) и Секретный ключ: (не заполняется при удаленном обновлении)

ФИО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Паспорт \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Получение подтверждаю (подпись) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 6**.** С момента подписания настоящего Акта:

- Клиент признает, что получение Клиентом документа, подписанного электронной подписью участника, юридически эквивалентно получению Клиентом документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Участника и оттиском печати Участника. Клиент признает, что документ, подписанный электронной подписью клиента, юридически эквивалентен документу на бумажном носителе, заверенном собственноручными подписями уполномоченных лиц Клиента и оттиском печати Клиента. Обязательства Клиента, предусмотренные настоящим пунктом, действительны при условии, что секретный ключ и сертификат участника созданы с использованием Системы**.**

 - Банк признает, что получение Банком документа, подписанного электронной подписью клиента, юридически эквивалентно получению Банком документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Клиента и оттиском печати Клиента. Банк признает, что документ, подписанный электронной подписью банка, юридически эквивалентен документу на бумажном носителе, заверенном собственноручными подписями уполномоченных лиц Банка и оттиском печати Банка. Обязательства Банка, предусмотренные настоящим пунктом, действительны при условии, что секретный ключ и сертификат клиента созданы с использованием системы.

**АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН**

**БАНК:**

Акционерное общество Банк «Тамбовкредитпромбанк»

юридический адрес: 392000, г. Тамбов, ул. Советская, 118

адрес для переписки: 392000, г. Тамбов, ул. Советская, 118

ИНН – 6829000028, ОКПО - 09263511, к/с № 30101810600000000755 в ГРКЦ ГУ ЦБ Банка России

г. Тамбова,

БИК 046850755 Тел. (4752) 559-777 Факс. (4752) 559-777

**КЛИЕНТ:**

ПОДПИСИ СТОРОН:

|  |  |  |
| --- | --- | --- |
| БАНК |  | КЛИЕНТ |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |  | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
|  |  |  |
| М.П. |  | М.П. |

Приложение № 3 к Договору об обслуживании банковского счета с использованием документов в электронной форме

должность руководителя подразделения банка

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО руководителя подразделения банка

 от \_\_\_\_\_\_\_\_\_\_\_

краткое наименование клиента

**ИНН**

**КПП**

**Договор банковского счета**

№ \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

**ЗАЯВКА**

на изготовление сертификата

« \_\_\_\_ » \_\_\_\_\_\_\_\_\_ 20\_\_ г.

Просим Вас изготовить ключ для работы в системе Интернет-Банк ,

(полное наименование клиента)

используя в качестве ключевого носителя смарт-карту.

I. Перечень счетов, открытых в АО Банк «ТКПБ», на которые распространяется действие договора об участии в Системе электронных платежей «Интернет-банк»:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

II. Ключ электронной подписи и сертификаты ключей проверки электронной подписи изготавливаются на имя (руководитель организации, имеющий право подписывать платежные документы)

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

III. Ответственным за работу с системой «Интернет-Банк» и уполномоченным Клиентом использовать ЭП для подписания электронных документов от Клиента назначается сотрудник(и):

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

IV. Ответственным лицом, уполномоченным Клиентом получить Электронный сертификат (сертификат) и Секретный ключ назначается сотрудник:

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

V. Данные для контакта:

- по техническим вопросам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ тел. \_\_\_\_\_\_\_\_\_

(Ф.И.О.)

-по коммерческим вопросам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ тел. \_\_\_\_\_\_\_\_\_

(Ф.И.О.)

VI. Юридический адрес клиента:

E-mail :

VII. Номера мобильных телефонов для отсылки одноразовых паролей:

основной:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

дополнительный (при необходимости):

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

VIII. Дополнительные меры информационной безопасности (*заполняется при необходимости*):

Список IP – адресов

Лимит на сумму перевода

Суточный лимит

SMS – уведомления (приходят на основной и дополнительный номера)

E-MAIL – уведомления

адрес почты

VIII. Укажите слово – пароль (*на русском языке)* – для блокировки сертификата при обращении по телефону в БАНК:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

IX. В соответствии с требованиями федерального закона №152-ФЗ «О персональных данных» Клиент подтверждает, что обладает согласием лиц, указанных в данной заявке, на передачу их персональных данных в АО Банк «ТКПБ», с последующей обработкой этих сведений банком, в том числе с использованием средств автоматизации, в целях исполнения Договора об обслуживании банковского счета с использованием документов в электронной форме и законодательства РФ.

X. Наименование сертификата (*заполняется для действующего сертификата*)

CN= OU= O= L= C=

ХI. Уполномоченный сотрудник ПОД/ФД (подтверждение целесообразности предоставления услуги интернет-банкинга)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Клиент:**

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность:\_\_\_\_\_\_\_

Ф.И.О: \_\_\_\_\_\_\_\_\_\_\_

М.П.

Приложение № 4 к Договору об обслуживании банковского счета с использованием документов в электронной форме

должность руководителя подразделения банка

ФИО руководителя подразделения банка

от

краткое наименование клиента

**ИНН**

**КПП**

**Договор банковского счета**

№ \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

**ЗАЯВКА**

на изготовление сертификата

« \_\_\_\_ » \_\_\_\_\_\_\_\_\_ 20\_\_ г.

Просим Вас изготовить дополнительный ключ для работы в системе «Интернет-Банк» без права подписи ,

(полное наименование клиента)

используя в качестве ключевого носителя смарт-карту.

I. Перечень счетов, открытых в АО Банк «ТКПБ», на которые распространяется действие договора об участии в Системе электронных платежей «Интернет-банк»:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

II. Ключ электронной подписи и сертификаты ключей проверки электронной подписи изготавливаются на имя (руководитель организации, имеющий право подписывать платежные документы)

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

III. Ответственным за работу с системой «Интернет-Банк» и уполномоченным Клиентом использовать ЭП для подписания электронных документов от Клиента назначается сотрудник(и):

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

IV. Ответственным лицом, уполномоченным Клиентом получить Электронный сертификат (сертификат) и Секретный ключ назначается сотрудник:

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество (полностью) | Должность | Паспортные данные, адрес регистрации |
|  |  |  |

V. Данные для контакта:

- по техническим вопросам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ тел. \_\_\_\_\_\_\_\_\_

(Ф.И.О.)

-по коммерческим вопросам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ тел. \_\_\_\_\_\_\_\_\_

(Ф.И.О.)

VI. Юридический адрес клиента:

E-mail :

VII. Номера мобильных телефонов для отсылки одноразовых паролей:

основной:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

дополнительный (при необходимости):

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

VIII. Дополнительные меры информационной безопасности (*заполняется при необходимости*):

Список IP – адресов

Лимит на сумму перевода

Суточный лимит

SMS – уведомления (приходят на основной и дополнительный номера)

E-MAIL – уведомления

адрес почты

VIII. Укажите слово – пароль (*на русском языке)* – для блокировки сертификата при обращении по телефону в БАНК:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

IX. В соответствии с требованиями федерального закона №152-ФЗ «О персональных данных» Клиент подтверждает, что обладает согласием лиц, указанных в данной заявке, на передачу их персональных данных в АО Банк «ТКПБ», с последующей обработкой этих сведений банком, в том числе с использованием средств автоматизации, в целях исполнения Договора об обслуживании банковского счета с использованием документов в электронной форме и законодательства РФ.

X. Наименование сертификата (*заполняется для действующего сертификата*)

CN= OU= O= L= C=

**Клиент:**

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность:\_\_\_\_\_\_\_

Ф.И.О: \_\_\_\_\_\_\_\_\_\_\_

М.П.

Приложение № 5 к Договору об обслуживании банковского счета с использованием документов в электронной форме

должность руководителя подразделения банка

ФИО руководителя подразделения банка

от

краткое наименование клиента

**ИНН**

**КПП**

**Договор банковского счета**

№ \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

**заявление**

о приостановлении работы в системе «Интернет-банк»

« \_\_\_\_ » \_\_\_\_\_\_\_\_\_ 20\_\_ г.

Прошу Вас приостановить работу в системе «Интернет-банк» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(полное наименование клиента)

с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ по причине \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (дата начала приостановления работы) (причина приостановления работы)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Должность:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Ф.И.О: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 М.П.

Приложение № 6 к Договору об обслуживании банковского счета с использованием документов в электронной форме

**Требования по обеспечению информационной безопасности
автоматизированного рабочего места Клиента**

Настоящие требования определяют перечень мер, обязательных для применения Клиентом и предназначенных для обеспечения защиты конфиденциальной информации на стороне Клиента при использовании системы «Интернет-банк».

Выполнение настоящих требований по информационной безопасности позволит обеспечить защиту юридически значимого электронного документооборота Клиента с Банком и минимизировать риски возможных финансовых потерь.

Форма и порядок реализации приведенных требований информационной безопасности устанавливается Клиентом самостоятельно.

Клиент обязан учитывать то, что:

* информационно-телекоммуникационная сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) информационно-телекоммуникационной сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
* существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством информационно-телекоммуникационной сети Интернет;
* существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из информационно-телекоммуникационной сети Интернет;
* гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
* меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
* расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы.
* Банк никогда не осуществляет рассылку писем, содержащих ссылки для перехода на страницы в сети Интернет, или для загрузки какого-либо программного обеспечения или данных. Необходимое для работы системы «Интернет-банк» программное обеспечение размещено на веб-сайте Faktura.ru в разделе «Настройка и поддержка».
* Банк никогда не запрашивает у клиентов конфиденциальную информацию по собственной инициативе!

Информационная безопасность автоматизированного рабочего места Клиента в системе «Интернет-банк» (далее по тексту АРМ) обеспечивается применением совокупности организационных и технических мер и средств защиты информации.

**Организационные меры**

Клиент разрабатывает и документально фиксирует правила подготовки, ввода в эксплуатацию и использования АРМ.

Клиент определяет и документально фиксирует (например, приказом) перечень лиц из числа своих работников, имеющих доступ к рабочему месту, с закреплением за каждым из них допустимых полномочий. В этот перечень включаются:

* лицо, непосредственно осуществляющее работу на АРМ в системе «Интернет-банк»;
* лицо, осуществляющее системное администрирование АРМ;
* лицо, ответственное за обеспечение информационной безопасности АРМ и администрирующее установленные на АРМ средства защиты информации;
* лица, замещающие вышеперечисленных на время их отсутствия.

Остальным работникам Клиента должен быть установлен запрет на доступ к АРМ.

Лица, допущенные к конфигурированию и эксплуатации АРМ, обязаны ознакомиться под подпись с установленными для Клиента правилами, инструкциями, размещенными на сайте Faktura.ru, а также настоящими требованиями.

Размещение оборудования АРМ осуществляется способом, исключающим возможность его несанкционированного использования, и производится в служебном помещении, для которого обеспечен режим ограниченного доступа (защищаемые помещения).

Защищаемое помещение необходимо оборудовать прочной входной дверью с замками, гарантирующими надежное закрытие в нерабочее время. По окончании рабочего дня защищаемое помещение и установленные в нем хранилища закрывают.

Для предотвращения наружного наблюдения за деятельностью сотрудников окна помещения необходимо защитить.

Окна помещения, расположенного на первом или последнем этаже здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в защищаемое помещение.

Клиент устанавливает режим охраны, предусматривающий периодический контроль за состоянием технических средств охраны.

Ключи от защищаемого помещения подлежат учету и выдаются только лицам, имеющим право допуска в защищаемые помещения, согласно перечню.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в защищаемое помещение посторонних лиц, Клиент обязан оценить возможность несанкционированного доступа к системе или компрометации ключа электронной подписи и при необходимости максимально быстро уведомить об инциденте Банк с последующим направлением письменного заявления.

Клиент устанавливает порядок хранения и использования носителей ключевой информации, исключающий возможность несанкционированного доступа третьих лиц.

Клиент определяет и документально фиксирует (например, приказом) перечень лиц из числа своих работников, имеющих право использования ключа электронной подписи.

Во время работы с носителями ключевой информации необходимо исключить доступ к АРМ посторонних лиц.

Хранение носителей ключевой информации осуществляется в сейфах или запираемых металлических шкафах (хранилищах), исключающих возможность несанкционированного доступа, неправомерного использования или утраты (хищения).

По окончании рабочего дня, а также между сеансами работы с системой носители ключевой информации убираются в хранилище.

В отношении носителей ключевой информации необходимо установить запрет на:

* передачу другим работникам и посторонним лицам;
* использование не по назначению;
* подключение к другим компьютерам или иному оборудованию;
* оставление без присмотра на рабочем месте.

При смене лица, наделенного правом использования ключей электронной подписи, Клиент обязан признать его компрометацию и уведомить об этом Банк, с дальнейшим изготовлением новых ключей на вновь назначенных лиц.

**Технические меры и средства**

Для осуществления работы в системе «Интернет-банк» необходимо использовать отдельное, специально выделенное для этих целей АРМ, на котором в обязательном порядке обеспечиваются меры защиты от несанкционированного доступа и защиты от вредоносного программного обеспечения.

Защита АРМ от несанкционированного доступа осуществляется с целью исключения возможностей:

* внесения несанкционированных изменений в технический или программный состав АРМ;
* несанкционированного вмешательства в электронный документооборот Клиента с Банком.

Клиент предпринимает меры, препятствующие несанкционированному доступу и вскрытию технических средств АРМ.

 Необходимо установить запрет на несанкционированное подключение к АРМ внешних устройств, в том числе съёмных носителей информации, а также автозапуск программ со всех устройств хранения, в том числе съемных.

На АРМ устанавливают только одну операционную систему, а также исключают возможность загрузки с внешних носителей (CD/DVD, USB flash).

Клиентом осуществляются мероприятия по ограничению программной среды АРМ, обеспечивающие:

* установку и (или) запуск только разрешенного к использованию программного обеспечения;
* невозможность установки стороннего программного обеспечения;
* отсутствие средств разработки и отладки программного обеспечения.

Клиентом регламентируются процедуры мониторинга и установки обновлений системного и прикладного программного обеспечения.

Необходимо предусмотреть процедуры контроля целостности программного обеспечения, обнаружения фактов её несанкционированного нарушения и последующего восстановления при необходимости.

Клиентом исключается возможность использования на АРМ нелицензионных копий и свободно распространяемого программного обеспечения.

Клиентом определяется порядок идентификации и аутентификации пользователей на АРМ, а также разграничения доступа и предоставления полномочий. Устанавливаемый порядок исключает возможность наделения какого-либо пользователя максимальными полномочиями (администрирования АРМ, администрирования средств защиты, осуществления работы в системе «Интернет-банк»). Доступ к изменению настроек BIOS также сопровождается процедурой аутентификации (защита паролем). Учетную запись «Гость» необходимо выключить.

Длина используемых паролей составляет не менее восьми символов, включая заглавные, строчные буквы и специальные символы. Сложность пароля выбирают достаточной дляисключения возможности подбора. Срок действия паролей необходимо ограничить.

Клиентом предусматриваются меры по защите АРМ при взаимодействии с информационно-телекоммуникационными сетями. Для этого рекомендуется установить и настроить соответствующим образом персональный межсетевой экран.

Меры устанавливают запрет сетевого доступа к ресурсам АРМ с других рабочих станций локальной сети или с использованием внешних сетей общего пользования, в том числе в режимах удаленного рабочего стола и удаленного администрирования.

Необходимо установить строгое ограничение на использование ресурсов сети Интернет пользователями АРМ, что означает определение законченного списка доступных для соединения адресов (например, разрешить только соединение с серверами системы «Интернет-банк»).

При использовании на АРМ систем обмена сообщениями или электронной почты пользователи информируются о мерах предосторожности при работе с электронными письмами или сообщениями, получаемыми от неизвестных источников.

В случае если при включении или в процессе работы с системой «Интернет-банк» будут обнаружены какие-то не имевшие ранее места события: самопроизвольные движения указателя мыши, нештатные информационные окна, несанкционированные платежи или сообщения об ошибках, о неверном ключе или пароле, и т.п. – Клиент обязан незамедлительно прекратить работу в системе, зафиксировать суть события и сопутствующую информацию и уведомить о событии сотрудников Банка.

Меры по защите АРМ от вредоносного кода (ВК) обеспечивают обнаружение компьютерных программ, предназначенных для внедрения в информационные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, участвующее в дистанционном банковском обслуживании, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также реагирование на обнаружение этих программ и информации.

На АРМ организуют непрерывное функционирование средств защиты от ВК в автоматическом режиме с регулярным контролем целостности и работоспособности защитного ПО.

Обновление баз сигнатур средств защиты от ВК необходимо производить в автоматическом режиме по мере их размещения (выпуска) разработчиком.

Рекомендуется осуществлять полную еженедельную проверку АРМ на наличие ВК.

Средства защиты от ВК осуществляют фильтрацию всех сообщений электронной почты, интернет-мессенджерах и т.д.

На АРМ обеспечивается обязательная проверка подключаемых съемных носителей информации на наличие ВК.

Средство защиты от ВК настраивают таким образом, чтобы при обнаружении признаков присутствия ВК на АРМ автоматически реализовывался комплекс мер по блокированию нежелательной активности и устранению последствий, а также происходило уведомление пользователя об инциденте. А в случае обнаружения атаки ВК в сетевом трафике с внешнего по отношению к АРМ источника, средство защиты от ВК автоматически блокирует обмен данными с этим источником.

При возникновении инцидентов, связанных с воздействием вредоносного кода на АРМ, Клиент обязан незамедлительно прекратить работу в системе «Интернет-банк», выяснить и устранить возможные последствия, зафиксировать всю доступную информацию об инциденте и уведомить сотрудников Банка.

Клиент предусматривает использование средств анализа наличия на АРМ уязвимостей системного и прикладного программного, особенно в части защиты от ВК.

Средства защиты от ВК предусматривают средства обобщения и анализа информации, фиксируемой в журналах протоколирования работы защитного ПО.

При выборе средств защиты от ВК рекомендуется отдавать предпочтение известным, хорошо зарекомендовавшим себя в течение продолжительного времени компаниям-разработчикам, предлагающим продукты, использующие зарегистрированные товарные знаки. Целесообразно предусматривать приобретение средств защиты от ВК у авторизованных партнеров компаний - разработчиков.

Приложение № 7 к Договору об обслуживании банковского счета с использованием документов в электронной форме

**Сведения о выполнении Клиентом требований к обеспечению**

**информационной безопасности автоматизированного рабочего места Клиента**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование мероприятия** | **Степень выполнения** | **Примечание** |
| 1 | Разработаны ли установленные требованиями внутренние нормативные документы (правила, руководства, положения)? |  |  |
| 2 | Определен ли перечень лиц из числа работников, имеющих доступ к АРМ. Установлен ли запрет на доступ к АРМ остальным работникам? |  |  |
| 3 | Определен ли перечень лиц из числа работников, имеющих право использования ключа электронной подписи? |  |  |
| 4 | Выделено ли отдельное АРМ для работы в системе «Интернет-банк»? |  |  |
| 5 | Соблюдаются ли требования к помещениям, в котором размещается оборудование АРМ? |  |  |
| 6 | Соблюдаются ли требования по хранению и использованию носителей ключевой информации? |  |  |
| 7 | Предприняты ли меры противодействия несанкционирован-ному вмешательству в технический состав АРМ? |  |  |
| 8 | Реализованы ли мероприятия по ограничению программной среды АРМ?  |  |  |
| 9 | Выполнены ли требования к программному обеспечению АРМ? |  |  |
| 10 | Определён ли порядок идентификации и аутентификации пользователей на АРМ, а также разграничения доступа и предоставления полномочий? |  |  |
| 11 | Предприняты ли меры по защите АРМ при взаимодействии с информационно-телекоммуникационными сетями? |  |  |
| 12 | Развернуты ли на АРМ средства защиты от вредоносного кода? |  |  |
| 13 | Организовано ли непрерывное функционирование средств защиты от ВК в автоматическом режиме, а также автоматическое обновление баз сигнатур по мере их размещения (выпуска) разработчиком? |  |  |
| 14 | Осуществляется ли периодическая проверка АРМ на наличие ВК, а также проверка подключаемых съемных носителей информации? Осуществляется ли фильтрация электронных сообщений? |  |  |
| 15 | Используются ли средства анализа наличия на АРМ уязвимостей системного и прикладного программного, особенно в части защиты от ВК? |  |  |
|  |  |  |  |
|  | Суммарное значение: |  |  |
|  | Корректирующий коэффициент: |  |  |
|  | **Итоговый показатель:** |  |  |

**Клиент:**

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность:\_\_\_\_\_\_\_

Ф.И.О: \_\_\_\_\_\_\_\_\_\_\_

М.П.

**Краткая инструкция по заполнению**

Для оценки выполнения Клиентом требований к обеспечению информационной безопасности при использовании системы «Интернет-банк» используется следующий подход:

* оценка 0 выставляется, в случае если требование не выполняется;
* оценка 1 выставляется, в случае если требование выполняется частично;
* оценка 2 выставляется, в случае если требование выполняется полностью.

Итоговый показатель вычисляется как среднее арифметическое оценок выполнения указанных требований умноженное на корректирующий коэффициент.

Корректирующий коэффициент определяется по следующим правилам:

* в случае отсутствия требований, которые полностью не выполняются, корректирующий коэффициент принимается равным 1;
* для случая, когда количество требований, которые полностью не выполняются, больше 0, но меньше 5, корректирующий коэффициент принимается равным 0.85;
* для случая, когда количество требований, которые полностью не выполняются, больше или равно 5, корректирующий коэффициент принимается равным 0.7.

На основе вычисленного значения итогового показателя формируется обобщенное суждение о выполнении Клиентом требований к обеспечению информационной безопасности в соответствии со следующим общим подходом:

* в случае если значение итогового показателя больше или равно 0.85, предпринятые меры обеспечивает выполнение установленных требований на необходимом уровне (значение качественной оценки «хорошая»);
* в случае если значение итогового показателя больше или равно 0.70 и меньше 0.85, предпринятые меры в целом обеспечивают выполнение установленных требований (значение качественной оценки «удовлетворительная»);
* в случае если значение итогового показателя больше или равно 0.5 и меньше 0.7, предпринятые меры частично обеспечивают выполнение установленных требований (значение качественной оценки «сомнительная»);
* в случае если значение итогового показателя меньше 0.5, предпринятые меры не обеспечивают выполнение установленных требований (значение качественной оценки «неудовлетворительная»).