

# Правила предоставления услуг систем «Телебанкинг», «SMS-банкинг» и «Интернет-банкинг» ОАО «Далькомбанк»

«\_\_» \_\_\_\_\_ 20\_\_ г.

## 1. Общее положение

1. ОАО «Далькомбанк», в дальнейшем БАНК, настоящими Правилами определяет отношения, а также устанавливает права, обязанности и ответственность, возникающие в процессе предоставления услуг систем дистанционного банковского обслуживания «Телебанкинг», «SMS-банкинг» и «Интернет-банкинг» (далее - систем ДБО) между БАНКОМ и КЛИЕНТОМ (далее - Стороны).

2. Настоящие Правила и иную информацию, включая Порядок подключения к системам ДБО, инструкции, Банк публично размещает:

- на корпоративном Интернет-сайте Банка [www.dalcombank.ru](http://www.dalcombank.ru);
- на информационных стендах в головном офисе / филиале / дополнительном / операционном офисе БАНКА в местах, доступных для КЛИЕНТОВ.

В дополнение к указанным выше способам публичного размещения информации БАНК вправе доводить эту информацию до потенциальных КЛИЕНТОВ и КЛИЕНТОВ БАНКА иными способами, в том числе путем рассылки информационных сообщений по электронной почте.

Моментом ознакомления КЛИЕНТА с публично размещенной информацией считается момент, с которого эта информация была размещена на сайте БАНКА и на информационных стендах в головном офисе / филиале / дополнительном / операционном офисе БАНКА в местах, доступных для КЛИЕНТОВ.

3. Условия настоящих Правил могут быть приняты КЛИЕНТОМ не иначе, как путем присоединения к предложенным БАНКОМ условиям в целом.

4. При работе в системах ДБО Стороны руководствуются инструкциями БАНКА по использованию соответствующей системы в соответствии с ее состоянием и развитием.

5. Передача всей информации в системе «Интернет-банкинг» осуществляться только с применением системы шифрования и электронной цифровой подписи в соответствии с действующим Федеральным законом РФ №1 от 10.01.2002 года «Об электронной цифровой подписи». Электронный документ, сформированный и подписанный с использованием электронной цифровой подписи, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с действующим законодательством РФ.

## 2. Права и обязанности БАНКА

### 2.1. БАНК обязуется:

1. предоставлять КЛИЕНТУ комплекс услуг систем ДБО, в зависимости от соответствия КЛИЕНТОМ условиям предоставления каждой конкретной услуги. Предоставление услуг начинается не позднее 2 (двух) рабочих дней после поступления бланка заказа и иных требуемых документов от КЛИЕНТА и ознакомления КЛИЕНТА с настоящими Правилами, но не ранее дня оплаты КЛИЕНТОМ подключения к системе ДБО;

2. консультировать КЛИЕНТА по вопросам, связанным с работой систем ДБО;

3. обеспечивать целостность, сохранность и конфиденциальность документов при их обработке в системах ДБО при соблюдении КЛИЕНТОМ настоящих Правил и инструкций БАНКА по использованию систем и систем защиты информации;

4. принимать все разумные меры для обеспечения конфиденциальности информации по счетам, операциям, другим данным КЛИЕНТА;

### 2.2. БАНК имеет право:

1. приостанавливать операции по счетам КЛИЕНТА, при получении документов на ограничение прав по распоряжению счетом в виде наложения ареста на денежные средства или приостановления операций в соответствии и порядке, установленном действующим законодательством РФ

2. возвращать КЛИЕНТУ платежные поручения, не проведенные РКЦ или иными расчетно-кассовыми центрами по причине неверного заполнения реквизитов КЛИЕНТОМ и/или по иным причинам, препятствующим осуществлению платежа по независящим от БАНКА причинам;

3. при невыполнении КЛИЕНТОМ своих обязанностей и/или использовании им имеющихся услуг, информации и других материалов систем ДБО в коммерческих или иных целях, не согласованных с БАНКОМ, полностью или частично прекратить предоставление услуг в системах ДБО КЛИЕНТУ в одностороннем порядке. Повторное включение в этих случаях возможно по индивидуальной письменной договоренности БАНКА и КЛИЕНТА;

4. в одностороннем порядке отменять, вводить новые и изменять условия предоставления услуг в системах ДБО, а именно настоящие Правила, Тарифы на услуги ОАО «Далькомбанк» для физических лиц (далее – Тарифы Банка), включая стоимость абонентного и расчетного обслуживания систем ДБО. БАНК обязан уведомлять КЛИЕНТА обо всех изменениях настоящих Правил и Тарифов Банка, определяющих их взаимоотношения, путем вывешивания информации в местах расчетного обслуживания клиентов подразделений БАНКА и опубликования в Интернет на веб-сайте БАНКА.

5. после предварительного предупреждения КЛИЕНТА, отказывать в приеме от него распоряжения на проведение операции по банковскому счету (вкладу), в случае выявления сомнительных операций в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

6. предоставлять денежные средства КЛИЕНТУ посредством системы «Интернет-банкинг» на условиях срочности, платности, возвратности и целевого характера, в соответствии с заявлением о предоставлении «Интернет-кредита».

### **3. Права и обязанности КЛИЕНТА**

#### **3.1. КЛИЕНТ обязуется:**

1. эксплуатировать системы ДБО и системы защиты информации в соответствии с настоящими Правилами и инструкциями БАНКА, при условии своевременного ознакомления БАНКОМ с ними КЛИЕНТА согласно п.1.1. настоящих Правил;

2. производить оплату услуг, оказываемых по настоящим Правилам БАНКА, в соответствии с Тарифами Банка;

3. своевременно и самостоятельно обновлять необходимые справочные данные системы ДБО;

4. самостоятельно обеспечивать работоспособность клиентской части используемых программных и технических систем, каналов связи, подключений к глобальной сети Интернет и т.п.;

5. сохранять конфиденциальность по всей методической, расчетной и финансовой информации, полученной в ходе эксплуатации систем ДБО;

6. своевременно оповещать БАНК об изменении своих реквизитов (изменение ФИО, смена паспортных данных, номера телефонов, адреса электронной почты, обслуживаемые счета и пр.). Для изменения/дополнения реквизитов необходимо оформить новый бланк заказа на услуги или новое заявление на подключение счета (-ов) к системе «Интернет-банкинг» для КЛИЕНТОВ физических лиц;

7. признать, что электронный документ, сформированный и подписанный с использованием электронной цифровой подписи, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с действующим законодательством РФ;

8. обеспечивать собственную информационную безопасность посредством:

- использования лицензионного программного обеспечения,
- принятия адекватных мер по сохранению в неприкосновенности и тайне от третьих лиц ключей шифрования и ЭЦП, паролей,
- организовать регулярное и своевременное обновление антивирусных программ и антивирусных баз. Использовать антивирусное ПО в «резидентном» режиме. Использовать средства обнаружения сетевых вторжений из состава антивирусного ПО или программных межсетевых экранов (firewall),
- организовать регулярное и своевременное обновление операционных систем, в особенности регулярную установку обновлений системы безопасности, критических обновлений,

БАНК \_\_\_\_\_

КЛИЕНТ \_\_\_\_\_

- максимально, на сколько возможно, ограничить использование компьютера с установленным АРМ клиента для посещения ресурсов сети Интернет, «сёрфинга» в Интернет. Ограничить нецелевое использование данных компьютеров (игры, загрузка приложений из сети Интернет и т.д.) Ограничить использование съемных носителей (флеш-карт, флэш-дисков и т.д.), так как они часто используются для распространения вредоносного программного обеспечения,
- не хранить ключи доступа к системам дистанционного банковского обслуживания на жестких магнитных дисках компьютеров или сетевых хранилищах,
- устанавливать ключевые носители только на период отправки платежа, по прекращении сеанса отправки, вынимать ключевые носители и помещать их в надежное хранилище (например, сейф). Отключать соединение с сетью Интернет, когда нет необходимости использовать его для отправки платежных документов,
- предоставлять пользователям для работы на компьютере минимально необходимые права для выполнения их должностных обязанностей. Стараться не использовать права «Администратора» если это возможно,
- оперативно контролировать результаты всех платежных операций,
- по возможности подключить услугу SMS-информирования о движениях по счету, с целью максимально быстрого реагирования в случае неправомерного списания денежных средств со счета,
- не загружать и не устанавливать неизвестное программного обеспечение, а так же не запускать программы полученные по электронной почте от неизвестных адресатов. В случае необходимости запуска программного обеспечения полученного из сети или через электронную почту предварительно проверять данные программы средствами антивирусной защиты,
- в случае получения электронных сообщений или телефонных звонков, якобы от сотрудников ОАО «Далькомбанк» с просьбой отправить им секретные ключи доступа к системам дистанционного банковского обслуживания, не делать этого ни при каких обстоятельствах. А так же обратиться по указанным в договоре телефонам в службу поддержки клиентов, с целью информирования Банка о подобных случаях,
- в случае существования технической возможности использования защищенных от копирования ключевых носителей использовать именно для хранения ключей именно их,
- использовать стойкие пароли для доступа к рабочей станции и системе дистанционного банковского обслуживания. Желательная длина пароля не менее 8 символов, наличие срочных и прописных символов, а так же цифр. Не использовать пароли которые однозначно связаны с пользователем системы (номер телефона, дата рождения, имя и т.д.),
- не использовать на компьютере с установленным АРМ клиента средств удаленного администрирования (RAdmin, TeamView, Ammyu и т.д.) или средств позволяющих работать в терминальном режиме, незаметно для основного пользователя.

### **3.2. КЛИЕНТ имеет право:**

1. на получение полного спектра банковских услуг, согласно оформленных бланков заказа на подключение к системам ДБО;
2. на техническую поддержку по вопросам, связанным с использованием систем ДБО, на консультации по «горячей» телефонной линии (тел. (4212) 38-07-07 – в г. Хабаровск или 8–800–555–27-27);
3. на передачу методической информации по системам ДБО третьей стороне в том случае, если третья сторона является сервисной службой и/или дистрибьютором программного обеспечения внутренней бухгалтерской системы КЛИЕНТА и методическая информация требуется третьей стороне для обеспечения выполнения программного интерфейса внутренней бухгалтерской системы с системами ДБО;
4. отказаться от всех или части услуг, предоставляемых в системах ДБО в одностороннем порядке, подав в БАНК заявку, установленной формы. БАНК прекращает предоставление услуг по заявлению КЛИЕНТА, начиная со следующего дня после принятия заявления;
5. на получение денежных средств через систему «Интернет-банкинг» на условиях срочности, платности, возвратности и целевого характера, при соответствии КЛИЕНТА условиям предоставления «Интернет-кредита».

## **4. Расчеты**

1. Плата за получение услуг систем ДБО определяется Тарифами Банка.

2. Оплата подключения к системам ДБО производится КЛИЕНТОМ в наличной форме либо безналично (путем перевода денежных средств на счет БАНКА).

3. Оплата услуг систем ДБО производится безналично путем безакцептного списания денежных средств со счета КЛИЕНТА в размере и порядке, предусмотренных в Тарифах Банка.

4. В случае отсутствия/недостатка средств на счете КЛИЕНТА для оплаты услуг, предоставляемых через системы ДБО, оказание КЛИЕНТУ услуг прекращается, до погашения задолженности. После погашения задолженности в полном объеме доступ к заблокированным счетам КЛИЕНТА автоматически возобновляется.

## 5. Применение шифрования и электронной цифровой подписи

Используемые термины и определения:

**Авторство документа** - принадлежность документа одной из Сторон. Авторство электронного документа определяется принадлежностью электронной цифровой подписи конкретному участнику электронного документооборота.

**Документ в электронной форме (далее - электронный документ / ЭД)** – совокупность данных, зафиксированных на материальном носителе (магнитном или ином) в компьютерной системе с реквизитами, позволяющими идентифицировать эту информацию и авторство документа. ЭД создается участником электронного документооборота на основе бумажного документа либо на основании другого электронного документа и полностью повторяет его по содержанию. ЭД обрабатываются и хранятся в компьютерных системах и могут передаваться по электронным каналам связи.

**Закрытый ключ** - уникальная последовательность символов, известная только владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

**Ключ (Криптографический ключ)** - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

**Компрометация ключа** - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. Компрометация ключа может произойти в следующих случаях:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- доступ к носителям ключевой информации посторонних лиц;
- появление в системе конфиденциальной связи сообщений от не установленных абонентов;
- нарушение печати на хранилище, в котором хранились ключевые носители;
- невозможность расшифровать зашифрованное сообщение или подтвердить достоверность ЭЦП.

**Открытый ключ** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

**Плановая смена ключей** - смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

**Проверка электронной цифровой подписи документа** - электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи;

**Сервер открытых ключей** – организованный Банком сервис по предоставлению участникам системы доступа к зарегистрированным открытым ключам абонентов. Банк при этом является одним из абонентов системы и его открытый ключ так же помещается в справочник на сервере.

БАНК \_\_\_\_\_

КЛИЕНТ \_\_\_\_\_

**Сертификат ключа подписи** - документ на бумажном носителе, включающий в себя открытый ключ электронной цифровой подписи и его атрибуты, заверенный собственноручной подписью владельца ключа электронной цифровой подписи. Передается банку для подтверждения подлинности ЭЦП и идентификации владельца ключа ЭЦП. Срок действия сертификата ключа подписи не ограничен, за исключением случаев компрометации Закрытого ключа.

**Средство криптографической защиты информации (СКЗИ)** - средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

**Электронная цифровая подпись (электронная подпись, ЭЦП)** – данные, добавляемые к блоку данных, полученные в результате его криптографического преобразования, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а так же обеспечить защиту от подлога со стороны приемника данных;

5.1. При обмене документами между собой КЛИЕНТ и БАНК признают действие электронной цифровой подписи как имеющей юридическую силу, равной силе собственноручной подписи. Передача данных между КЛИЕНТОМ и БАНКОМ ведутся на основе электронных документов, достоверность и конфиденциальность которых обеспечивается применением системы криптографической защиты информации, использующей систему открытых и закрытых ключей шифрования/ЭЦП. Открытые ключи хранятся в справочнике на сервере открытых ключей банка, закрытые ключи хранятся в тайне. В качестве средства криптографической защиты информации используется программный пакет PGP разработки компании PGP Corporation.

5.2. КЛИЕНТ самостоятельно производит выработку личных ключей (открытого и закрытого), в соответствии с инструкцией, размещенной на корпоративном Интернет-сайте Банка [www.dalcombank.ru](http://www.dalcombank.ru), которые будут использоваться им в дальнейшем для формирования ЭЦП для ЭД и его шифрования. После этого открытые ключи регистрируются на сервере открытых ключей БАНКА, для чего составляется сертификат ключа подписи, распечатывается и заверяется собственноручной подписью КЛИЕНТА и лично передается КЛИЕНТОМ в БАНК.

5.3. Ответственные сотрудники БАНКА за регистрацию открытых ключей КЛИЕНТА, в соответствии с установленными правилами регистрации открытых ключей БАНКА, производит проверку идентификационных данных КЛИЕНТА (или его доверенного лица), после чего подписывает своей личной ЭЦП его открытый ключ и заносит его в справочник открытых ключей. В дальнейшем, при плановой смене ключей, передавать в БАНК открытый ключ можно как электронный документ, подписанный действующим личным ключом.

5.4. КЛИЕНТ с помощью открытых ключей на носителе шифрует информацию и проверяет истинность электронной цифровой подписи БАНКА, а с помощью закрытых дешифрует пришедшую в его адрес информацию и подписывает отправляемые документы.

5.5. КЛИЕНТ или его доверенное лицо должны хранить и использовать свои закрытые ключи таким образом, чтобы исключить возможность доступа к ним других лиц, в том числе сотрудников БАНКА. Передача закрытых ключей другим лицам не допускается.

В случае компрометации закрытых ключей клиента КЛИЕНТ обязан немедленно прекратить обмен данными с БАНКОМ и оповестить БАНК о возникших обстоятельствах.

5.6. В случае действительной или предполагаемой компрометации ключей выполняются следующие действия:

5.6.1. КЛИЕНТ обращается в банк, пишет заявление о временном прекращении обмена документами в электронной форме.

5.6.2. Ответственный сотрудник на основании письменного заявления КЛИЕНТА составляет АКТ (2 экземпляра) о временном прекращении обмена документами в электронной форме.

5.6.3. БАНК принимает меры по предупреждению приема документов от КЛИЕНТА и совместно с КЛИЕНТОМ осуществляет сверку документов, полученных за период с предполагаемого времени компрометации ключей.

5.6.4. КЛИЕНТ самостоятельно производит генерацию новых ключей шифрования/ЭЦП.

## **6. Ответственность БАНКА и КЛИЕНТА**

### **6.1. Ответственность БАНКА**

6.1.1. БАНК несет ответственность за ущерб, причиненный КЛИЕНТУ, в случае подделки, сбоя, выхода из строя средств криптографической защиты информации, происшедших по вине БАНКА, повлекших за собой материальный ущерб КЛИЕНТУ. Отсутствие вины БАНКА в

причинении ущерба КЛИЕНТУ, подтвержденное выводами комиссии, в случае сбоя, выхода из строя средств криптографической защиты информации, освобождает БАНК от возмещения ущерба КЛИЕНТУ.

6.1.2. БАНК не несет ответственности за нанесение ущерба КЛИЕНТУ вследствие несоблюдения КЛИЕНТОМ требований информационной безопасности (подпункт 8) п. 3.1. настоящих Правил) либо вследствие противоправных действий третьих лиц в отношении самого КЛИЕНТА либо средств автоматизации, используемой КЛИЕНТОМ при использовании систем ДБО.

6.1.3. БАНК не несет ответственности за существование расчетов, за несоблюдение КЛИЕНТОМ и его контрагентами формы и правильности заполнения реквизитов платежных документов. Все спорные вопросы, возникающие по взаимным платежам, участники расчетов регулируют между собой и/или в соответствии с действующим законодательством РФ.

6.1.4. БАНК не несет ответственности за отказы в работе систем ДБО по вине провайдеров связи, из-за форс-мажорных обстоятельств, по причине отказа или сбоя в работе средств автоматизации и программного обеспечения КЛИЕНТА.

6.1.5. БАНК не несет ответственности за несоблюдение требований информационной безопасности провайдерами связи, привлекаемыми КЛИЕНТОМ при использовании систем ДБО.

## **6.2. Ответственность КЛИЕНТА**

В случае нарушения КЛИЕНТОМ настоящих Правил ответственность за причиненный КЛИЕНТУ и/или БАНКУ ущерб полностью возлагается на КЛИЕНТА.

БАНК не несет ответственности за произошедшее без вины БАНКА получение третьими лицами доступа к информации КЛИЕНТА, передаваемой по открытым каналам связи (телефон, SMS, электронная почта без применения СКЗИ и т.п.).

БАНК не несет ответственности за сбои в работе каналов передачи данных и сервисов, предоставляемых третьими лицами (интернет-провайдеры, операторы проводной связи, операторы сотовой связи и т.п.).

## **6.3. Освобождение от ответственности**

В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

Сторона, понесшая в результате форс-мажорных обстоятельств убытки из-за неисполнения или приостановления другой стороной исполнения своих обязанностей, может потребовать от стороны, ставшей объектом действий непреодолимой силы, документальных подтверждений о произошедших событиях.

## **6.4. Разрешение конфликтов**

В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с использованием электронной цифровой подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях: не подтверждение подлинности электронных документов средствами проверки ЭЦП принимающей стороны; оспаривание передающей стороной факта формирования электронного документа; оспаривание передающей стороной принадлежности ключа ЭЦП, которым подписан электронный документ, его владельцу; заявление об искажении электронного документа.

Споры и разногласия, возникающие при предоставлении услуг по настоящим Правилам, решаются, прежде всего, путем переговоров и в соответствии с действующим законодательством России. При использовании системы криптографической защиты «PGP», споры, связанные со случаями подделки информации, передаваемой по электронным каналам с использованием средств криптографической защиты информации (СКЗИ), сбоя, выхода СКЗИ из строя, решаются в следующем порядке:

БАНК \_\_\_\_\_

КЛИЕНТ \_\_\_\_\_

1. В случае возникновения конфликтной ситуации Сторона, предполагающая ее возникновение (Уведомитель), должна в срок не позднее 3-х суток направить в адрес другой Стороны (Участника) уведомление об этом. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. Независимо от формы, в которой составлено уведомление (письменная или электронный документ), оно должно содержать реквизиты электронного документа, а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

Участник обязан в течение следующего рабочего дня проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, после чего направить Уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Уведомитель удовлетворен информацией, полученной от Участника, которому было направлено уведомление.

2. В случае, если Уведомитель не удовлетворен полученной информацией, то для рассмотрения конфликтной ситуации формируется рабочая комиссия. Рабочая комиссия формируется из равного количества уполномоченных представителей от каждой из конфликтующих Сторон. Право представлять в комиссии соответствующую Сторону подтверждаться доверенностью, выданной каждому представителю на срок работы комиссии. По инициативе любой из Сторон к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты без права голоса, обладающими необходимыми знаниями в области защиты информации и работы компьютерных систем. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

3. Сформированная комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной ЭЦП, идентичности отправленного и полученного электронного документа.

4. По итогам работы технической комиссии составляется Акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии Акт должен также содержать следующие данные:

- состав комиссии;
- дату и место составления Акта;
- даты и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

К Акту может прилагаться особое мнение члена (или членов) комиссии, не согласных с выводами технической комиссии, указанными в Акте. Особое мнение составляется в произвольной форме и составляет приложение к Акту.

5. Результаты работы комиссии используются при определении степени виновности Сторон в конфликтной ситуации для последующего возмещения ущерба. Все вопросы, неурегулированные в процессе работы комиссии, решаются в соответствии с действующим законодательством.

БАНК \_\_\_\_\_

КЛИЕНТ \_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_