

**ПРАВИЛА**  
**дистанционного банковского обслуживания**  
**физических лиц в «Тимер Банк» (ПАО)**

Казань  
2019

# ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ФИЗИЧЕСКИХ ЛИЦ В «ТИМЕР БАНК» (ПАО)

## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Авторизация** – предоставление Клиенту прав на выполнение определённых действий в Интернет-банке и/или Мобильном банке, проверка (подтверждение) данных прав при попытке выполнения этих действий.

**Аутентификация** – процедура проверки легальности Клиента при сверке соответствия введённого им Логина и Пароля учётной записи и Паролю в базе данных.

**Банк** – «Тимер Банк» (публичное акционерное общество) («Тимер Банк» (ПАО)). Юридический адрес: 420066, г. Казань, пр. Ибрагимова, д. 58. Фактический адрес: 420066, г. Казань, пр. Ибрагимова, д. 58, тел. (843) 525-74-74, факс (843) 525-74-28. Официальный сайт Банка в сети Интернет: [www.timerbank.ru](http://www.timerbank.ru).

**Дистанционное банковское обслуживание (ДБО)** – предоставление Банком Клиенту предусмотренных настоящими Правилами банковских и информационных услуг с использованием Интернет-банка и/или Мобильного банка.

**Заявление (распоряжение)** – электронное сообщение или несколько связанных электронных сообщений, содержащих распоряжения Клиента Банку о совершении Финансовой операции и иных действий. Заявление (распоряжение) при получении от Клиента проходит процедуру подтверждения - дополнительной Идентификации Клиента и/или контроля подлинности, неизменности и целостности Заявления (распоряжения).

**Идентификатор** – условное наименование, число или иная информация, позволяющая идентифицировать Клиента.

**Идентификация** – процедура установления личности Клиента с помощью Идентификатора.

**Карта** – платежная карта, выпущенная Банком на имя Клиента.

**Клиент** – физическое лицо, присоединившееся к Правилам.

**Логин** – имя учетной записи Клиента, которое используется для Аутентификации и Идентификации Клиента при входе в Интернет-банк и/или Мобильный банк.

**Мобильный банк** – комплекс программно-технических средств и организационных мероприятий Банка, позволяющий предоставлять Клиентам удаленные банковские услуги с помощью Мобильного приложения, установленного на мобильный телефон, имеющий доступ в сеть Интернет.

**Мобильное приложение** – клиентское приложение Мобильного банка, устанавливаемое на устройство Клиента.

**Одноразовый пароль** – электронное средство, которое представлено в виде нумерованного цифрового кода и используется для подтверждения Заявлений (распоряжений) и иных документов Клиента, передаваемых в ДБО. Одноразовый пароль высылается на номер мобильного телефона Клиента в виде SMS-сообщения или PUSH-уведомления. Одноразовый пароль является аналогом собственноручной подписи Клиента. В каждый момент запроса Банком Одноразового пароля только один Одноразовый пароль является актуальным для подтверждения операции в ДБО. Информация в электронной форме, при подписании которой использовался Одноразовый пароль, признается Электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

**Пароль** – последовательность символов, используемая для Аутентификации и Идентификации Клиента при выполнении процедуры подключения к ДБО. Информация в электронной форме, при подписании которой использовался Пароль, признается Электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

**Правила** – настоящие Правила дистанционного банковского обслуживания физических лиц в «Тимер Банк» (ПАО).

**Протокол соединения** – Электронный документ, подтверждающий факт передачи Клиентом Заявления (распоряжения), в том числе протокол сеанса связи в виде совокупности записей в базе данных Банка.

**Репозиторий** – App Store и Google Play, через которые осуществляется установка Мобильного приложения.

**Интернет-банк** – комплекс программно-технических средств и организационных мероприятий Банка, позволяющий предоставлять Клиентам удаленные банковские услуги посредством Интернета и обеспечивающий формирование, передачу, регистрацию, исполнение Заявлений (распоряжений) Клиентов и проведение на их основе Финансовых операций.

**Средства авторизации** - электронные средства, используемые для Идентификации Клиента при осуществлении доступа к Интернет-банку и/или Мобильному банку (Логин, Пароль).

**Стороны** – Банк и Клиент.

**Счет** – банковский счет, открытый Клиенту в Банке.

**Тарифы** – утвержденные тарифы на услуги Банка для физических лиц.

**Финансовая операция** – любая финансовая операция или сделка, осуществляемая Банком по Заявлению (распоряжению) Клиента, в соответствии с настоящими Правилами и иными заключенными между Сторонами соглашениями (договорами).

**Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.

**Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения лица, подписывающего информацию.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила принимаются физическими лицами путем присоединения в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации. Условия настоящих Правил могут быть приняты Клиентом не иначе как путем присоединения к предложенным Банком условиям в целом.

2.2. Настоящие Правила регулируют отношения Сторон, возникающие в процессе оказания Банком услуг по Дистанционному банковскому обслуживанию Клиентов с использованием Интернет-банка и/или Мобильного банка, в том числе порядок обмена Электронными документами, права, обязанности и ответственность Сторон.

2.3. Подключение Клиента к Дистанционному банковскому обслуживанию осуществляется путем регистрации в сети Интернет по адресу: <https://online.timerbank.ru/> одним из 2 (двух) способов:

- по серии, номеру документа, удостоверяющего личность Клиента и номеру действующей Карты;

- по серии, номеру документа, удостоверяющего личность Клиента и номеру Счета, открытому Клиенту в Банке.

2.4. Клиент соглашается, что использование Средств авторизации, в том числе сгенерированных Банком Одноразовых паролей, является надлежащей и достаточной Идентификацией Клиента, подтверждением права совершать операции через Интернет и эквивалентом собственноручной подписи Клиента.

2.5. Банк для ознакомления Клиента с Правилами, Тарифами, а также изменениями и дополнениями в Правилах, Тарифы публично размещает Правила и Тарифы в сети Интернет на сайте Банка. Моментом ознакомления Клиента с публично размещенной информацией считается момент, с которого данная информация была размещена на сайте Банка. Банк не

несет ответственности, если публично размещенная информация не была получена и/или изучена и/или неправильно понята Клиентом.

2.6. Вся информация, связанная с использованием Клиентом Средств авторизации и Одноразовых паролей, является строго конфиденциальной и не может быть передана третьим лицам.

Клиент подтверждает, что ему известно о том, что несанкционированная передача конфиденциальной информации по Интернет-банку и/или Мобильному банку влечет риск несанкционированного доступа к такой информации третьих лиц.

2.7. Доступ Клиента к Интернет-банку осуществляется посредством браузера при наличии на устройстве доступа к сети Интернет.

Поддерживаемые браузеры:

- Microsoft Internet Explorer 11;
- Microsoft Edge;
- Mozilla Firefox (63.x и выше);
- Google Chrome (70.x и выше);
- Opera (55.x и выше);
- Safari (10.x, 11.x, 12.x).

2.8. Доступ Клиента к Мобильному банку осуществляется после установки Мобильного приложения через Репозиторий при наличии на устройстве доступа к сети Интернет.

Требования для установки Мобильного приложения:

- операционная система Android (7.x и выше);
- операционная система iOS (10.x и выше).

### **3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

#### **3.1. Клиент имеет право:**

3.1.1. Приостановить в соответствии с п. 3.3.2. настоящих Правил или прекратить в соответствии с п. 11.3. настоящих Правил доступ к ДБО в течение срока действия Правил.

#### **3.2. Банк имеет право:**

3.2.1. Отказать в исполнении Заявления (распоряжения) Клиента в следующих случаях:

- выявления сомнительных операций Клиента без объяснения причин;
- получения сведений, указывающих на изменение получателя информации, направленной Банком и используемой при Аутентификации Клиента;
- выявления признаков нарушения безопасности, в том числе, если Банк имеет основания считать, что выполнение Заявления (распоряжения) может повлечь убытки для Банка либо для Клиента;

- противоречия Заявления (распоряжения) действующему законодательству Российской Федерации и/или настоящим Правилам.

Отказ Банка в совершении Финансовой операции не является основанием для возникновения гражданско-правовой ответственности Банка перед Клиентом за нарушение условий Правил.

3.2.2. Отказать в приеме заявления Клиента об отмене ранее переданного Заявления (распоряжения), если удовлетворение заявления невозможно в силу исполнения Заявления (распоряжения) Банком к моменту получения данного заявления.

3.2.3. Приостановить ДБО Клиента при наличии у Банка оснований полагать, что возможно несанкционированное использование Интернет-банка и/или Мобильного банка от имени Клиента, а также в случае нарушения Клиентом обязательств, предусмотренных настоящими Правилами и нормами действующего законодательства.

3.2.4. Отказать в возобновлении ДБО в случае нарушения Клиентом обязательств, предусмотренных настоящими Правилами.

3.2.5. Потребовать от Клиента подписания в любой момент документов на бумажном носителе, соответствующих по смыслу и содержанию переданным Клиентом и зарегистрированным Банком Заявлениям (распоряжениям) независимо от того, были ли

исполнены эти Заявления (распоряжения) Банком, а также не регистрировать новые и не исполнять зарегистрированные Заявления (распоряжения) до подписания Клиентом указанных выше документов.

3.2.6. Вводить в одностороннем порядке следующие ограничения на исполнение Заявлений (распоряжений) Клиентов:

- установка лимитов на операции ДБО;
- запрет на проведение по определенным каналам связи;
- прочие ограничения, осуществляемые Банком в целях безопасности.

3.2.7. Вносить изменения в Интернет-банк и/или Мобильный банк, производить модификацию и выпуск новых версий.

### **3.3. Клиент обязуется:**

3.3.1. Не раскрывать третьим лицам и сотрудникам Банка информацию об используемых им Средствах авторизации и Одноразовых паролях, а также принять все необходимые меры для того, чтобы в течение всего срока действия Правил Средства авторизации и Одноразовые пароли не стали известны третьим лицам.

3.3.2. Обратиться в Банк с требованием о приостановлении ДБО, если у Клиента возникли основания полагать, что Средства авторизации и/или Одноразовые пароли стали известны третьему лицу или были утеряны (утрачены), путем подачи в Банк письменного Заявления о приостановлении (блокировке) / возобновлении (разблокировке) дистанционного банковского обслуживания физических лиц (далее – Заявление о приостановлении/возобновлении ДБО) (Приложение № 1 к настоящим Правилам). До момента подачи письменного Заявления о приостановлении/возобновлении ДБО Клиент несет ответственность за незаконное использование третьими лицами его Средств авторизации и/или Одноразовых паролей.

3.3.3. Обеспечить безопасное использование предоставляемой услуги ДБО в соответствии с Рекомендациями Банка по обеспечению Клиентом «Тимер Банк» (ПАО) безопасного использования Интернет-банка/Мобильного банка (Приложение № 2 к настоящим Правилам) (далее – Рекомендации Банка).

3.3.4. Контролировать правильность оформления, в том числе реквизиты Заявления (распоряжения), перед отправкой в Банк.

3.3.5. Предоставлять в Банк обновленную информацию об изменении персональных данных, способных повлиять на выполнение Сторонами обязательств согласно Правилам, в том числе гражданства, реквизитов документа, удостоверяющего личность, места жительства (регистрации), телефонных номеров в течение 7 (семи) календарных дней с даты указанных изменений. При непредставлении обновленных данных Банк считает имеющиеся у него ранее предоставленные данные действительными до момента их обновления, и обязанности Банка считаются исполненными при использовании имеющихся данных.

3.3.6. Следить за изменениями и дополнениями, вносимыми в Правила и Тарифы, которые размещены в сети Интернет на сайте Банка.

3.3.7. Оплачивать услуги ДБО в соответствии с Тарифами.

3.3.8. Отслеживать факт исполнения/отказа в исполнении Банком Заявлений (распоряжений) на перечисление денежных средств.

3.3.9. Информировать Банк при невозможности исполнить свои обязательства в соответствии с настоящими Правилами.

### **3.4. Банк обязуется:**

3.4.1. Фиксировать поступившие от Клиента Заявления (распоряжения) и хранить не менее 3 (трех) лет с момента получения.

3.4.2. Обеспечивать Клиенту возможность получения актуальной и достоверной информации о поступивших от Клиента Заявлениях (распоряжениях).

3.4.3. Обеспечивать информационную поддержку Клиентов по услуге ДБО.

3.4.4. Обеспечивать выявление в Репозитории систем Мобильного банка, размещенных со ссылкой на Банк без получения согласия Банка.

3.4.5. Обеспечивать оперативное уведомление Клиентов и лиц, обладающих правами на управление Репозиторием, о выявленных случаях размещения систем, указанных в п. 3.4.4. настоящих Правил.

#### **4. ПОДКЛЮЧЕНИЕ И ДОСТУП КЛИЕНТА К ДБО**

4.1. Подключение Клиента к услуге ДБО производится на сайте Банка при наличии действующей Карты или открытого Счета. Логин задается автоматически, Клиент может оставить его, либо назначить свой. Пароль вводится Клиентом. Для завершения процедуры подключения Клиента к системе ДБО на номер мобильного телефона Клиента, зарегистрированный в базе данных Банка, высылается Одноразовый пароль. Ввод Одноразового пароля является подтверждением выполнения процедуры подключения Клиента к услуге ДБО и присоединения к настоящим Правилам.

4.2. Для подключения Мобильного банка Клиент переходит по ссылке, указанной на странице входа в Интернет-банк для установки Мобильного приложения.

4.3. Клиент не может иметь более одного действующего Логина и/или Пароля одновременно.

4.4. Вход в Интернет-банк осуществляется путем ввода Клиентом Логина и Пароля, при этом проводится Аутентификация, Идентификация Клиента и выполнение процедуры Авторизации.

Вход в Мобильный банк осуществляется путем ввода ПИН-кода или Логина и Пароля в Мобильном приложении.

4.5. В случае некорректного введения Клиентом Средств авторизации в количестве 5 (пяти) раз доступ Клиента к ДБО блокируется автоматически на определенный период времени, установленный Банком. По истечении данного периода времени доступ Клиента к ДБО автоматически возобновляется.

4.6. Если Клиент не предпринял меры безопасности согласно Рекомендациям Банка, Банк не несет ответственности за убытки, причиненные Клиенту несанкционированным использованием третьим лицом Средств авторизации и Одноразовых паролей Клиента.

4.7. Стороны признают, что:

4.7.1. Все Заявления (распоряжения) Клиента, полученные Банком по Интернет-банку и/или Мобильному банку и прошедшие проверку персональных Идентификаторов (Логин, Пароль, Одноразовый пароль), признаются подтвержденными Клиентом.

Заявления (распоряжения), переданные Клиентом в Банк и подтвержденные Одноразовыми паролями:

- удовлетворяют требованию совершения сделки в простой письменной форме и создают для Сторон юридические последствия, аналогичные последствиям совершения письменных сделок путем составления единого документа, выражающего их содержание и подписанного собственноручно лицами, совершающими сделку (-и);

- имеют равную юридическую и доказательственную силу с аналогичными по содержанию и смыслу документами на бумажном носителе, составленными в соответствии с требованиями, предъявляемыми к документам такого рода, подписанными собственноручной подписью Клиента, и являются основанием для проведения Банком операций и совершения иных действий от имени Клиента;

- не могут быть признаны недействительными только на том основании, что они оформлены в электронном виде и переданы в Банк с использованием Интернет-банка и/или Мобильного банка.

4.7.2. Протокол соединения является достаточным доказательством и может использоваться Банком в качестве подтверждения (доказательства) факта передачи Клиентом Заявления (распоряжения) о проведении операции в соответствии с параметрами, содержащимися в Протоколе соединения или в Заявлении (распоряжении) Клиента.

4.8. Доступ к услугам ДБО предоставляется Клиенту круглосуточно за исключением времени, необходимого для проведения технической профилактики.

## **5. ОДНОРАЗОВЫЕ ПАРОЛИ**

5.1. Одноразовые пароли считаются действующим средством подтверждения, находящимся в распоряжении Клиента с момента подключения и предоставления доступа к ДБО.

5.2. Одноразовые пароли используются для подтверждения Заявления (распоряжения) и совершаемых действий Клиента в ДБО.

5.3. Одноразовый пароль действителен на протяжении ограниченного периода времени, установленного Банком.

5.4. Положительный результат проверки Одноразового пароля означает, что Заявление (распоряжение) Клиента принято в обработку.

## **6. ПОРЯДОК СОВЕРШЕНИЯ ОПЕРАЦИЙ В ДБО**

6.1. Передача Клиентом Заявления (распоряжения) в Банк означает, что Клиент поручает Банку провести Финансовую операцию (сделку), соответствующую указанному Заявлению (распоряжению).

6.2. Моментом поступления в Банк Заявления (распоряжения) считается время и дата регистрации Заявления (распоряжения), определенное по часам оборудования, используемого Банком для регистрации Заявлений (распоряжений).

6.3. Заявление (распоряжение), переданное в ДБО, проходит Авторизацию и подтверждение с помощью Одноразового пароля. До подтверждения Клиентом Заявления (распоряжения) на номер мобильного телефона, зарегистрированный в базе данных Банка, направляется сообщение с информацией о параметрах Заявления (распоряжения), включая сумму и получателя денежных средств, и Одноразовый пароль для подтверждения Заявления (распоряжения). При отсутствии подтверждения Заявление (распоряжение) не регистрируется и считается, что Заявление (распоряжение) Клиентом не передавалось.

6.4. Если по каким-либо причинам (разрыв связи и т.п.) Клиент не получил сообщение о регистрации либо об отказе в регистрации Заявления (распоряжения), ответственность за установление окончательного результата передачи Заявления (распоряжения) средствами Интернет-банка и/или Мобильного банка лежит на Клиенте.

6.5. Заявление (распоряжение) Клиента исполняется в сроки, установленные действующим законодательством для исполнения распоряжений такого рода, и в порядке, установленном настоящими Правилами.

6.6. При проведении Финансовых операций на основании Заявлений (распоряжений) Клиента используются открытые Счета, в отношении которых отсутствует запрет для использования в Интернет-банке и/или Мобильном банке или иные ограничения, установленные в соответствии с требованиями действующего законодательства.

6.7. Все действия Клиента в ДБО записываются в электронный журнал операций для следующих целей:

- урегулирования спорных ситуаций с Клиентом;
- сбора статистической информации;
- пресечения несанкционированного доступа к ДБО.

При этом записи в электронном журнале являются необходимыми и достаточными доказательствами при разрешении споров между Сторонами.

## **7. ПРИОСТАНОВКА И ВОЗОБНОВЛЕНИЕ ДБО**

7.1. Приостановление ДБО возможно:

7.1.1. по инициативе Клиента, если у Клиента возникли основания полагать, что Средства авторизации и Одноразовые пароли стали известны третьему лицу, путем предоставления Клиентом в Банк письменного Заявления о приостановлении/возобновлении ДБО в соответствии с п. 3.3.2. настоящих Правил;

7.1.2. по инициативе Банка при наличии у Банка оснований полагать, что возможно несанкционированное использование Интернет-банка и/или Мобильного банка от имени

Клиента, а также в случае нарушения Клиентом обязательств, предусмотренных настоящими Правилами.

7.2. В случае приостановления ДБО по инициативе Банка Банк уведомляет Клиента о причине приостановления по каналам контактной связи, указанным в базе данных Банка, в течение 5 (пяти) рабочих дней со дня приостановления ДБО.

7.3. В случае приостановления ДБО Банк не возвращает полученную с Клиента плату за услуги, предоставление которых приостановлено.

7.4. Банк возобновляет ДБО, приостановленное по инициативе Клиента, не позднее 3 (трех) рабочих дней после получения от Клиента письменного Заявления о приостановлении/возобновлении ДБО.

7.5. Банк возобновляет ДБО, приостановленное по инициативе Банка, не позднее 3 (трех) рабочих дней после получения Заявления о приостановлении/возобновлении ДБО, устранения задолженности по оплате услуг Банка, а также устранения Клиентом нарушений Правил, явившихся основанием для приостановления ДБО.

## **8. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ**

8.1. Клиент оплачивает услуги Банка, предоставляемые в рамках Правил, в соответствии с Тарифами, действующими на момент совершения операции.

8.2. В случае образования задолженности Клиента перед Банком за оказанные услуги ДБО Клиент предоставляет Банку право списывать в бесспорном порядке (на условиях заранее предоставленного согласия (акцепта) Клиента) задолженность за оказанные услуги ДБО с любых Счетов Клиента, открытых в Банке.

8.3. В случае недостаточности средств на Счетах Клиента для списания платы за услуги ДБО в размере, предусмотренном Тарифами, Банк вправе не исполнять Заявление (распоряжение) Клиента.

8.4. При списании Банком денежных средств со Счета, открытого в валюте, отличной от валюты перевода, Банк осуществляет конвертацию валют согласно Тарифам.

## **9. УРЕГУЛИРОВАНИЕ РАЗНОГЛАСИЙ**

9.1. При несогласии Клиента с действиями Банка по исполнению его Заявлений (распоряжений) Клиент лично предоставляет в Банк письменную претензию по форме Банка.

9.2. Банк обязуется рассмотреть претензию и предоставить Клиенту возможность получения информации о результатах рассмотрения в срок не более 30 (тридцати) календарных дней со дня получения претензии, а по операциям трансграничного перевода денежных средств – в срок не более 60 (шестидесяти) календарных дней со дня получения претензии.

9.3. При невозможности достижения между Сторонами взаимоприемлемого решения любой спор, разногласие или претензия, вытекающие из или в связи с Правилами либо их нарушением, прекращением или недействительностью, подлежат рассмотрению в судебном порядке в соответствии с действующим законодательством Российской Федерации.

## **10. ОТВЕТСТВЕННОСТЬ БАНКА И КЛИЕНТА**

10.1. Банк несет ответственность перед Клиентом за убытки, которые возникли у Клиента в результате ошибок при использовании Интернет-банка и/или Мобильного банка и вызваны исключительно несоблюдением Банком требований настоящих Правил и действующего законодательства.

10.2. Банк не несет ответственности:

10.2.1. за неисполнение Заявления (распоряжения) Клиента, если исполнение привело бы к нарушению требований настоящих Правил, в том числе, если Заявление (распоряжение) не было подтверждено Клиентом; проверка подтверждения дала отрицательный результат; средств на Счете недостаточно для исполнения Заявления (распоряжения).

10.2.2. за исполнение Заявлений (распоряжений), ошибочно переданных Клиентом повторно.



10.2.3. за невыполнение, несвоевременное или неправильное выполнение Заявлений (распоряжений), если оно вызвано предоставлением Клиентом недостоверной информации; потерей актуальности информации, ранее предоставленной Клиентом и используемой при регистрации и исполнении Банком Заявления (распоряжения); вводом Клиентом неверных данных.

10.2.4. за ущерб, возникший вследствие несанкционированного использования третьими лицами Средств авторизации и Одноразовых паролей Клиента, если такое использование стало возможным не по вине Банка.

10.2.5. за невыполнение или несвоевременное выполнение Заявлений (распоряжений), если выполнение данных Заявлений (распоряжений) зависит от определенных действий третьей стороны, которая не может или отказывается совершить необходимые действия, совершает их с нарушениями установленного порядка или недоступна для Банка.

10.2.6. за полное или частичное неисполнение, неправильное или несвоевременное исполнение своих обязательств, вытекающих из настоящих Правил, если такое неисполнение вызвано: решениями органов законодательной и/или исполнительной власти Российской Федерации, Банка России; задержками переводов по вине Банка России; обстоятельствами непреодолимой силы; военными действиями, стихийными или иными бедствиями, происходящими в районах, официально признанных находящимися под влиянием вышеуказанных обстоятельств.

10.2.7. в случае, если информация, связанная с использованием Клиентом Интернет-банка и/или Мобильного банка, станет известной третьим лицам в результате доступа к информации при передаче по каналам связи, которые находятся вне пределов Банка.

10.3. Клиент несет ответственность за убытки, возникшие у Банка в результате исполнения Заявлений (распоряжений), переданных в Банк от имени Клиента неуполномоченным лицом, при условии, что это стало возможно не по вине Банка.

10.4. Клиент несет риск убытков, возникших у него в результате исполнения Заявлений (распоряжений), переданных в Банк с использованием принадлежащих Клиенту Средств авторизации и Одноразовых паролей.

## **11. СРОК ДЕЙСТВИЯ ПРАВИЛ**

11.1. Настоящие Правила становятся обязательными для Сторон со дня предоставления доступа к ДБО и действуют бессрочно.

11.2. Прекращение доступа к ДБО возможно в одностороннем порядке по инициативе любой из Сторон.

11.3. При прекращении доступа к ДБО по инициативе Клиента Клиент обязан предоставить в Банк письменное Заявление о прекращении доступа к дистанционному банковскому обслуживанию физических лиц (далее – Заявление о прекращении ДБО) (Приложение № 3 к настоящим Правилам). Доступ к ДБО считается прекращенным со дня, указанного в Заявлении о прекращении ДБО, но не ранее дня подачи Заявления о прекращении ДБО.

11.4. При прекращении доступа к ДБО по инициативе Банка Банк обязан направить Клиенту уведомление о прекращении доступа к ДБО в письменном виде по адресу, указанному в базе данных Банка. Доступ к ДБО считается прекращенным в день, указанный Банком в уведомлении о прекращении доступа к ДБО, но не позднее 10 (десяти) рабочих дней со дня направления данного уведомления Клиенту.

11.5. Прекращение Доступа к ДБО по инициативе Клиента возможно при отсутствии у Клиента задолженности по оплате услуг ДБО.

11.6. Прекращение Доступа к ДБО не влечет прекращения обязательств по взаиморасчетам Сторон и возмещению убытков, возникших до момента прекращения доступа к ДБО.

## 12. ПРОЧИЕ УСЛОВИЯ

12.1. Настоящая редакция Правил вступает в силу с момента их утверждения единоличным исполнительным органом Банка.

12.2. Стороны признают, что настоящие Правила являются соглашением, в рамках которого происходит регулирование отношений в области использования Электронных подписей в соответствии с Федеральным законом от 06.04.2011 года № 63-ФЗ «Об электронной подписи».

Информация в электронной форме, подписанная простой Электронной подписью, признается Электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

12.3. Банк вправе в одностороннем порядке вносить изменения и дополнения в Правила и Тарифы, уведомляя Клиента путем размещения Правил и Тарифов с учетом изменений и дополнений в сети Интернет на сайте Банка.

12.4. Любые изменения и дополнения в Правила с момента вступления их в силу равно распространяются на всех лиц, присоединившихся к ним ранее даты вступления изменений и дополнений в силу. В случае несогласия с изменениями и дополнениями в Правила Клиент имеет право до вступления в силу изменений и дополнений прекратить доступ к ДБО в порядке, установленном пунктом 11.3. настоящих Правил.

**ЗАЯВЛЕНИЕ**  
**о приостановлении (блокировке) / возобновлении (разблокировке)**  
**дистанционного банковского обслуживания физических лиц**

Я, \_\_\_\_\_,  
(фамилия, имя, отчество Клиента)  
паспорт: \_\_\_\_\_ выдан \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ года,  
серия, номер  
зарегистрированный по адресу: \_\_\_\_\_,  
номер мобильного телефона +7 \_\_\_\_\_, в связи с \_\_\_\_\_  
указать причину  
прошу **приостановить (блокировать) / возобновить (разблокировать)** (*нужное подчеркнуть*)  
**Интернет-банк/Мобильный банк** (*нужное подчеркнуть*).

Клиент: \_\_\_\_\_ ( \_\_\_\_\_ ) «\_\_» \_\_\_\_\_ 20\_\_ г.  
подпись ФИО

**Заполняется Банком**

Заявление принято в \_\_\_\_\_ в \_\_\_\_\_ часов \_\_\_\_\_ минут «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подразделение Банка)

Сотрудник Банка: \_\_\_\_\_ ( \_\_\_\_\_ ) «\_\_» \_\_\_\_\_ 20\_\_ г.  
подпись ФИО

**РЕКОМЕНДАЦИИ**  
**Банка по обеспечению Клиентом «Тимер Банк» (ПАО)**  
**безопасного использования Интернет-банка/Мобильного банка**

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей Интернет-банка и/или Мобильного банка файлов с секретными ключами ЭЦП и пароли. Трояны распространяются через e-mail, по каналам сервисов мгновенной передачи информации, через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают ключи ЭЦП, пароли доступа, что позволяет совершать операции от имени Клиента.

**При работе в Интернет с использованием Интернет-банка и/или Мобильного банка рекомендуется соблюдать следующие правила безопасности, применяющиеся для защиты данных:**

- Устанавливать Мобильное приложение только из App Store и Google Play.
- При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- Пользоваться персональными компьютерами, мобильными устройствами с установленным лицензионным программным обеспечением.
- Своевременно обновлять установленное программное обеспечение и операционную систему (установка критичных обновлений).
- Включить системный аудит событий операционной системы, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
- Установить и своевременно обновлять на компьютере, мобильном устройстве антивирусное программное обеспечение.
- Антивирусное программное обеспечение должно запускаться автоматически с загрузкой операционной системы. Рекомендуется ежедневная проверка компьютера, мобильного устройства на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, мобильного устройства вплоть до полного излечения от вирусов.
- При выходе в Интернет использовать межсетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.
- Не давать разрешения неизвестным программам выходить в Интернет.
- При работе в Интернет не соглашаться на установку каких-либо дополнительных программ.
- Воздерживаться от использования программ онлайн-общения на компьютере, мобильном устройстве, используемых для работы в Интернет-банке и/или Мобильном банке.
- Необходимо предусмотреть невозможность установки посторонними лицами на компьютер или мобильное устройство специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.
- Рекомендуется ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

- Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.
- Важно знать, что ни одна антивирусная программа не обеспечивает 100% защиты.
- После окончания работы в Интернет-банке и/или Мобильном банке необходимо выйти из Интернет-банка/Мобильного приложения.
- При подозрениях на наличие вирусов на персональном компьютере, мобильном устройстве (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности) полностью воздержаться от использования Интернет-банка и/или Мобильного банка до исправления ситуации.
- Следите за своими операциями. Информация по Счетам, полученная через Интернет-банк и/или Мобильный банк, позволит Вам своевременно обнаружить и оперативно известить Банк об имеющихся несоответствиях.

### **Требования к персональному компьютеру, мобильному устройству, используемому при работе в Интернет-банке/Мобильном банке**

Обращаем Ваше внимание, что персональные компьютеры, мобильные устройства, на которых ведется работа в Интернет-банке и/или Мобильном банке, должны отвечать следующим требованиям:

- Пароли учетных записей, обладающих правами администратора, должны быть сложными и содержать не менее 6 (шести) символов.
- Пароль доступа необходимо менять не реже одного раза в 3 (три) месяца или при подозрении в его компрометации. В частности, компрометацией является вирусная активность на персональном компьютере в период использования Интернет-банка.
- Учетная запись «Гость» должна быть выключена.
- Не должно быть учетных записей с пустыми паролями.

**Ключевая информация – это аналог Вашей личной подписи. При ее использовании соблюдайте следующие правила:**

- Никогда и никому, включая сотрудников Банка, не сообщайте Средства авторизации и Одноразовые пароли. Сотрудники Банка никогда не запросят у Вас подобную информацию.
- Прежде чем вводить Логин и Пароль убедитесь, что Вы находитесь на сайте Интернет-банка: в адресной строке должен быть адрес: <https://online.timerbank.ru/>. Будьте внимательны: сайты, выглядящие почти точной копией банковских, созданы специально для получения Ваших персональных данных.
- При работе в Интернет-банке и/или Мобильном банке используйте Логин, Пароль и Одноразовые пароли. Ваши персональные данные и номер Карты могут использоваться только при подключении к ДБО.
- Не записывайте свои Логин и Пароль там, где они могут стать доступными другим лицам.
- Если Вам пришло SMS-сообщение с Одноразовым паролем для платежа, который Вы не совершали, известите Банк. Ни в коем случае не вводите и никому не сообщайте пришедший Одноразовый пароль.
- Старайтесь не работать с Интернет-банком с общедоступных компьютеров, например, в Интернет-кафе. Если Вам пришлось воспользоваться Интернет-банком с компьютера общего пользования, поменяйте Пароль с личного компьютера при первой же возможности.

- Ограничьте доступ к номеру Вашего мобильного телефона, в том числе в социальных сетях и других открытых источниках.
- Если Вам пришло уведомление о блокировке SIM-карты, немедленно сообщите в Банк для блокировки доступа в Интернет-банк и Мобильный банк.
- В случае утери мобильного телефона немедленно заблокируйте SIM-карту.
- Не отправляйте конфиденциальную информацию о Средствах авторизации и/или о движении Ваших денежных средств по электронной почте.

Если Вы обнаружили в сети Интернет ложный Web-сайт «Тимер Банк» (ПАО), отличный от <https://online.timerbank.ru/>, [www.timerbank.ru](http://www.timerbank.ru), или с Вами пытаются связаться по электронной почте или иным способом лица с требованиями о предоставлении Средств авторизации, просьба немедленно сообщить об этом в Банк по телефону 8 (800) 100-66-77.

Хотим отметить, что вышеуказанные Рекомендации относятся к любой системе дистанционного банковского обслуживания любого банка. В целом, разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Однако, соблюдение перечисленных простых «гигиенических» мер позволяет существенно снизить риски, связанные с использованием систем дистанционного банковского обслуживания, и, в конечном итоге, предотвратить хищение Ваших денежных средств.

В связи с этим просим отнестись с особым вниманием к расчетам в сети Интернет и не отвечать на сомнительные запросы. Стоит помнить, что Банк никогда не будет запрашивать по электронной почте персональную информацию Клиента, так как это противоречит соображениям безопасности.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошеннических действий. Телефон клиентской поддержки Банка 8 (800) 100-66-77.

**ЗАЯВЛЕНИЕ**

**о прекращении доступа к дистанционному банковскому обслуживанию физических лиц**

Я, \_\_\_\_\_,  
(фамилия, имя, отчество Клиента)  
паспорт: \_\_\_\_\_ выдан \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ года,  
серия, номер  
зарегистрированный по адресу: \_\_\_\_\_,  
номер мобильного телефона +7\_\_\_\_\_, настоящим прошу «Тимер Банк»  
(ПАО) прекратить доступ к дистанционному банковскому обслуживанию физических лиц с  
«\_\_» \_\_\_\_\_ 20\_\_ г. по моей инициативе.

Клиент: \_\_\_\_\_ («\_\_» \_\_\_\_\_ 20\_\_ г.)  
подпись ФИО

---

**Заполняется Банком**

Заявление принято в \_\_\_\_\_ в \_\_\_\_\_ часов \_\_\_\_\_ минут «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подразделение Банка)

Сотрудник Банка: \_\_\_\_\_ («\_\_» \_\_\_\_\_ 20\_\_ г.)  
подпись ФИО