

## **ПРАВИЛА** **дистанционного банковского обслуживания физического лица в ОАО «СМП Банк»**

### **1. ПРИМЕНЯЕМЫЕ ТЕРМИНЫ**

**Аналог собственноручной подписи** – персональный идентификатор Клиента, являющийся контрольным параметром правильности составления всех обязательных реквизитов электронного документа и неизменности их содержания.

**Банк** – Открытое акционерное общество Банк «Северный морской путь» (ОАО «СМП Банк»).

**Заявление о дистанционном банковском обслуживании** – заявление по форме, установленной Банком (Приложение № 2 к настоящим Правилам), о дистанционном банковском обслуживании счетов Клиента с использованием систем «СМП ON-Банк» и/или «СМП-Онлайн», подписанное Клиентом в Банке с целью заключения Договора о дистанционном банковском обслуживании физического лица.

**Договор** – настоящие Правила, Тарифы, Заявление о дистанционном банковском обслуживании надлежащим образом оформленные, составляющие в совокупности Договор о дистанционном банковском обслуживании физического лица.

**Карта сеансовых ключей** – документ, содержащий сеансовые ключи, выдаваемый Банком при заключении настоящего Договора и в дальнейшем по заявлению Клиента

**Клиент** - физическое лицо (резидент или нерезидент в соответствии с законодательством Российской Федерации), заключившее (заключающее) настоящий Договор.

**Логин** – уникальная последовательность алфавитно-цифровых символов, присваиваемых идентифицированному Клиенту Банком и позволяющая однозначно идентифицировать Клиента в Системе.

**Опубликование информации** - размещение Банком информации в местах и способами, установленными настоящими Правилами, обеспечивающими возможность ознакомления с этой информацией Клиентов. Опубликование информации не означает ее обязательного распространения через средства массовой информации.

**Пароль** – последовательность алфавитно-цифровых символов в количестве от 6 до 10 знаков (без пробелов), связанная с присвоенным Клиенту логином и являющаяся кодом аутентификации Клиента в Системе.

**Правила** – настоящие Правила дистанционного банковского обслуживания физического лица в ОАО «СМП Банка», присоединяясь к которым путем подписания и подачи Заявления о дистанционном банковском обслуживании, Клиент заключает Договор о дистанционном банковском обслуживании физического лица.

**Сеансовый ключ** – одноразовый числовой код, вводимый Клиентом в Систему в подтверждение правильного оформления электронного документа перед отправкой его в Банк. Сеансовый ключ аннулируется после его использования. Для целей настоящих Правил сеансовый ключ является аналогом собственноручной подписи Клиента.

**Система** – Система дистанционного банковского обслуживания «СМП ON-Банк» или «СМП-Онлайн»

**Тарифы** - документ Банка, являющийся неотъемлемой частью Договора о дистанционном банковском обслуживании физического лица и устанавливающий размер вознаграждения, взимаемого Банком с Клиента за подключение/использование систем «СМП ON-Банк» и «СМП-Онлайн».

**Электронный платежный документ (ЭПД)**- электронный документ, представляющий собой расчетный документ Клиента на совершение операций по его банковскому счету, составленный в электронном виде, содержащий все предусмотренные законодательством РФ реквизиты, подписанный сеансовым ключом и полученный с применением системы шифрования трафика, имеющий равную юридическую силу с расчетными документами, составленными на бумажных носителях, подписанными собственноручной подписью Клиента и являющийся основанием для совершения операций по счетам Клиента, открытым в Банке.

**Электронный служебно-информационный документ (ЭСИД)** – электронный документ, обеспечивающий обмен информацией между Клиентом и Банком (выписки из счета, информационные сообщения и т.п.).

**eToken** - устройство, предназначенное для генерации сеансовых ключей.

### **2. ОБЩИЕ ПОЛОЖЕНИЯ**

2.1. Настоящие Правила являются типовым документом Банка, распространение текста которого Банком по открытым каналам связи должно рассматриваться физическими лицами как публичное предложение (оферта) Банка заключить настоящий Договор путем присоединения на определенных Банком условиях.

2.2. Заключение Договора осуществляется в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, в форме присоединения Клиента в целом к условиям настоящих Правил путем представления в Банк подписанного Заявления о дистанционном банковском обслуживании.

2.3. Банк с целью ознакомления Клиентов с настоящими Правилами и Тарифами размещает их путем Опубликования информации одним или несколькими из указанных способов по усмотрению Банка:

- размещение информации в операционных залах Банка;
- размещение информации на корпоративном Интернет-сайте Банка [www.smpbank.ru](http://www.smpbank.ru);
- оповещение Клиентов через системы удаленного доступа Банка;
- рассылка Клиентам информационных сообщений по электронной почте;
- иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

Момент ознакомления Клиента с опубликованной информацией считается момент, с которого информация опубликована и доступна для ознакомления.

2.4. Заключая настоящий Договор, Банк и Клиент, далее совместно именуемые «Стороны», принимают на себя обязательство исполнять в полном объеме требования настоящих Правил.

### **3. ПРЕДМЕТ ДОГОВОРА**

3.1. Банк оказывает Клиенту услуги по дистанционному банковскому обслуживанию всех открытых ему в Банке текущих счетов, счетов по вкладам и счетов банковских карт (далее именуемых «Счета»), с использованием системы дистанционного банковского обслуживания «СМП-Онлайн» либо с использованием системы дистанционного банковского обслуживания «СМП ON-Банк», которая включает в себя систему «СМП-Онлайн», обеспечивающую проведение электронных расчетов с использованием Счетов и оформление ЭПД, а также обмен ЭСИД между Банком и Клиентом по сети Интернет согласно Тарифам Банка. Для Клиентов, являющихся нерезидентами РФ, Система позволяет проводить электронные расчеты только между Счетами Клиента, открытыми в Банке. В системе «СМП ON-Банк» Клиенту также доступны дополнительные услуги (ведение электронного бюджета, учет доходов и расходов и другое),

Выбор Системы дистанционного банковского обслуживания осуществляется при подписании соответствующего Заявления о дистанционном банковском обслуживании. В отдельных подразделениях Банка может быть доступна для подключения только одна из Систем.

3.2. Предоставление доступа к Системе осуществляется через сеть Интернет на сайте Банка [www.smpbank.ru](http://www.smpbank.ru), [www.bk.smpbank.ru](http://www.bk.smpbank.ru) (система «СМП-Онлайн»), [www.budget.smpbank.ru](http://www.budget.smpbank.ru) (система «СМП ON-Банк»).

3.3. Распоряжение денежными средствами, находящимися на Счете, осуществляется с использованием аналога собственноручной подписи в форме сеансовых ключей, которые могут быть получены Клиентом в Банке в виде карты сеансовых ключей, либо путем получения сообщений на номер мобильного телефона, указанный в Заявлении о дистанционном банковском обслуживании, (SMS-информирование), либо путем использования eToken.

Способ получения сеансовых ключей указывается Клиентом в Заявлении о дистанционном банковском обслуживании.

3.4. В рамках дистанционного банковского обслуживания в соответствии с настоящим Договором Сторонами используется кодовое слово для блокировки работы Клиента в Системе в случае обнаружения нарушений безопасности Системы. Кодовое слово указывается Клиентом в Заявлении о дистанционном банковском обслуживании.

3.5. Стороны признают, что применение Клиентом логинов и паролей (далее именуемых «средства доступа») в Системе, а также использование сеансовых ключей в качестве аналога собственноручной подписи Клиента, является достаточным условием для идентификации Клиента и подтверждения его прав по проведению операций по Счетам, а также по использованию иных услуг, предоставляемых Системой.

3.6. Стороны признают используемую ими Систему достаточной для обеспечения надежной и эффективной работы при приеме, передаче и обработке ЭПД и ЭСИД (далее совместно именуемых «электронными документами»), а систему защиты информации достаточной для защиты от несанкционированного доступа, подтверждения подлинности информации, содержащейся в электронных документах.

3.7. Достоверность ЭПД, заверенного сеансовым ключом и направленного в Банк, считается подтвержденной, если автоматическая процедура проверки сеансового ключа, применяемая в Системе, дает положительный результат.

3.8. Стороны признают, что ЭПД Клиента, созданные и переданные с использованием Системы, заверенные им сеансовыми ключами, имеют равную юридическую силу и влекут возникновение таких же правовых обязанностей, что и документы, оформленные на бумажном носителе в соответствии с требованиями законодательства РФ и подписанные собственноручной подписью Клиента или его уполномоченного представителя.

3.9. Стороны признают, что все расчеты, полученные в системе «СМП ON-Банк» (вне системы «СМП Онлайн») носят исключительно информационный характер и не могут являться достаточным основанием для принятия Клиентом каких-либо решений, в том числе финансового характера,

3.10. Заключением Договора Клиент выражает свое согласие на осуществление Банком обработки (сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования и уничтожения), в том числе принятия решений на основе исключительно автоматизированной обработки, его персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных".

3.11. ЭПД, поступившие в Банк в операционное время, установленное Банком для расчетно-кассового обслуживания клиентов по соответствующим видам операций, считаются поступившими текущим рабочим днем. ЭПД, поступившие в Банк после операционного времени, установленного Банком для расчетно-кассового обслуживания клиентов, считаются поступившими следующим рабочим днем.

3.12. При проведении электронных расчетов с использованием Системы Стороны руководствуются требованиями, установленными законодательством РФ, нормативными документами Банка России (в частности Положением Центрального Банка РФ № 222-П от 01.04.2003 «О порядке осуществления безналичных расчетов физическими лицами в Российской Федерации»), настоящими Правилами, а также договорами, заключенными между Банком и Клиентом, в соответствии с которыми Клиенту открыты Счета, и настоящим Договором.

#### **4. УСЛОВИЯ ДОСТУПА КЛИЕНТА К СИСТЕМЕ**

4.1. После заключения настоящего Договора Клиент получает в Банке запечатанный конверт, содержащий средства доступа к Системе, а также карту сеансовых ключей (в случае её выбора) либо средства для создания сеансовых ключей.

4.2. Подключение Клиента к системе «СМП-Онлайн» осуществляется не позднее дня, следующего за днем заключения настоящего Договора. Подключение Клиента к системе «СМП ON-Банк» осуществляется Клиентом самостоятельно.

4.3. При первом входе в Систему Клиенту необходимо сформировать пароль, который в дальнейшем будет использоваться Клиентом при входе в Систему (последовательность алфавитно-цифровых символов в количестве от 6 до 10 знаков без пробелов).

#### **5. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ**

5.1. Прием электронных документов от Клиента в Банке производится в автоматическом режиме круглосуточно, с учетом п. 3.11. настоящих Правил.

5.2. Основаниями для отказа от исполнения Банком ЭПД Клиента служат:

- неверные или неполные реквизиты ЭПД;
- отсутствие или наличие некорректного сеансового ключа Клиента в электронном документе;
- недостаток денежных средств на Счете для проведения операции Клиента в Банке (с учетом комиссионного вознаграждения Банка);

- нарушение условий договора(ов), в соответствии с которым(ыми) Клиенту открыт(ы) Счет(а);
- недостаток информации и необходимых документов по проводимой Клиентом операции (копий договоров и т.п.) в случаях, предусмотренных действующим законодательством РФ и нормативными документами Банка России в целях выполнения требований валютного контроля и внутреннего контроля по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- арест денежных средств на Счете в случаях, предусмотренных действующим законодательством РФ (в пределах суммы, на которую наложен арест) или иное ограничение по распоряжению денежными средствами на Счете в случаях, предусмотренных законодательством РФ.

- квалификация Банком операции в качестве сомнительной или подозрительной, определяемой таковой законодательством РФ и внутренними нормативными документами Банка. О данном факте Банк уведомляет Клиента информационным сообщением, отправленным по Системе, и отключает Клиента от Системы. При этом Банк принимает от Клиента расчетные документы на бумажном носителе и исполняет их при отсутствии других причин, указанных в настоящем пункте.

5.3. Выписки по Счетам Клиента за текущий операционный день формируются и становятся доступны Клиенту для просмотра и печати на следующий операционный день. В случае обнаружения спорной операции по Счету, Клиент обязан в течение 10 (Десяти) календарных дней с даты формирования выписки письменно уведомить Банк о суммах, ошибочно списанных/ зачисленных на Счет.

5.4. Прием Клиентом сформированных Банком и предназначенных Клиенту ЭСИД, а также передача Банку созданных Клиентом ЭПД и ЭСИД производится исключительно по инициативе Клиента путем организации им сеанса электронной связи с Банком с использованием Системы.

5.5. В соответствии с Тарифами Банк в безакцептном порядке взимает комиссионное вознаграждение с Клиента за услуги по дистанционному банковскому обслуживанию Счета(ов) Клиента.

5.6. В случае невыполнения Клиентом своих обязательств по настоящему Договору, а также в случае возникновения задолженности по оплате услуг, в соответствии с п. 5.5. настоящих Правил Банк в одностороннем порядке приостанавливает действие

настоящего Договора до устранения выявленных нарушений или задолженности, о чем Клиенту направляется сообщение в форме ЭСИД с указанием срока их устранения.

Возобновление договорных отношений производится после устранения Клиентом указанных нарушений/задолженности. В случае невыполнения Клиентом требования Банка об устранении нарушений или допущения нарушений, устранение которых не представляется возможным, обслуживание Клиента по Системе прекращается, а настоящий Договор расторгается в порядке, определенном п. 10.2. настоящих Правил.

## 6. ПРАВА И ОБЯЗАННОСТИ БАНКА

### 6.1. Банк обязан:

6.1.1. Выдавать Клиенту средства доступа к Системе, сеансовые ключи либо средства для их создания после заключения настоящего Договора, либо по заявлению Клиента для их замены.

6.1.2. Осуществлять расчетное и информационное обслуживание Клиента в соответствии с законодательством Российской Федерации и условиями, предусмотренными настоящим Договором.

6.1.3. Своевременно обрабатывать полученные от Клиента в процессе сеансов электронной связи с использованием Системы ЭПД и ЭСИД.

6.1.4. Оказывать Клиенту консультационные услуги по вопросам функционирования Системы по рабочим дням с 9.30 до 21 часа по московскому времени по телефону 8 -495- 980-24-80.

6.1.5. Не разглашать и не передавать третьим лицам информацию, связанную с использованием Клиентом Системы, а также информацию, введенную клиентом в Систему, за исключением случаев, предусмотренных действующим законодательством РФ.

6.1.6. Принимать меры для предотвращения несанкционированного доступа третьих лиц к информации о Счетах Клиента и проведенных по ним операциях, отраженным в Системе.

6.1.7. Предоставлять по требованию Клиента документы на бумажном носителе, подтверждающие совершение операций по Счетам Клиента в соответствии с его ЭПД.

6.1.8. Уведомить Клиента об отказе в исполнении ЭПД не позднее 1 (Одного) рабочего дня, следующего за днем поступления ЭПД в Банк.

6.1.9. Блокировать работу Клиента в Системе в случае обнаружения Клиентом нарушения безопасности Системы на основании устного заявления Клиента, полученного по телефону, с указанием ФИО Клиента, даты и места рождения и кодового слова. Блокировка работы Клиента в Системе осуществляется до момента поступления в Банк письменного заявления Клиента о возобновлении работы в Системе по форме, установленной в Банке.

6.1.10. Вести архив электронных документов.

### 6.2. Банк имеет право:

6.2.1. Запрашивать у Клиента копии ЭПД, составленные на бумажном носителе и заверенные собственноручной подписью Клиента, создавшего ЭПД.

6.2.2. Ограничить максимальную сумму ЭПД.

6.2.3. Приостановить дистанционное банковское обслуживание Клиента с использованием Системы в случае наличия у Банка оснований предполагать несанкционированное использование Системы от имени Клиента, в т.ч. в связи с компрометацией используемых Клиентом средств доступа к Системе и аналогов собственноручной подписи Клиента.

6.2.3. Требовать от Клиента замены средств доступа к Системе или аналога собственноручной подписи в случае компрометации или подозрения на компрометацию средств доступа к Системе и/или аналога собственноручной подписи Клиента.

## 7. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

### 7.1. Клиент обязан:

7.1.1. Использовать при работе с Системой только исправное и проверенное на отсутствие компьютерных вирусов оборудование.

7.1.2. Не разглашать и не передавать третьим лицам информацию, связанную с использованием Системы, в т.ч. средства доступа к Системе и аналог собственноручной подписи,

7.1.3. Соблюдать Правила информационной безопасности при использовании систем дистанционного банковского обслуживания через сеть Интернет (Приложение № 1 к настоящим Правилам)..

7.1.4. Контролировать корректность реквизитов получателя и собственных платежных реквизитов при составлении ЭПД.

7.1.5. Уплачивать Банку комиссионное вознаграждение за предоставление услуг по обслуживанию Клиента с использованием Системы в соответствии с Тарифами. Клиент предоставляет Банку право списывать в безакцептном порядке с его Счета(ов) сумму комиссионного вознаграждения Банка в соответствии с Тарифами.

7.1.6. При возникновении подозрений в нарушении безопасности Системы, выявлении признаков или фактов, а также возможности таких нарушений, немедленно приостановить использование Системы до момента устранения обстоятельств, их повлекших, а также проинформировать об этом Банк по телефону 8 -800-555-2-555 с указанием своего ФИО, даты и места рождения и кодового слова.

7.1.7. В целях обеспечения оперативности ознакомления с информацией, переданной Клиенту Банком в виде электронных документов, регулярно осуществлять вход в Систему.

Информация, переданная Банком Клиенту с использованием Системы, считается доведенной до сведения Клиента по истечении 1 (Одного) календарного дня, начиная со дня ее передачи Клиенту, независимо от фактического восприятия информации Клиентом (независимо от того, была информация прочитана или нет).

7.1.8. Представлять заявление в письменном виде по форме, утвержденной Банком, в случае необходимости выдачи новой карты сеансовых ключей, прекращения (в т.ч. временного) работы в Системе, возобновления работы в Системе.

7.1.9. Осуществлять смену средств доступа к Системе и аналога собственноручной подписи по требованию Банка, а также в случае выявления их компрометации.

7.1.10. Предоставлять информацию и необходимые документы по проводимой Клиентом операции (копии договоров и т.п.) в случаях, предусмотренных действующим законодательством РФ и нормативными документами Банка России.

### 7.2. Клиент имеет право:

7.2.1. Получать выписки по Счету(ам) и иную информацию, имеющую отношение к обслуживанию Клиента в Банке в рамках настоящего Договора, в виде ЭСИД.

7.2.2. Передавать в Банк и получать от Банка расчетные и иные документы, имеющие отношение к обслуживанию Клиента в Банке в рамках настоящего Договора, не только в электронном виде, но и на бумажном носителе в установленном порядке.

7.2.3. В случае прекращения или временного отключения Клиента от обслуживания с использованием Системы предоставлять в Банк оригиналы документов на бумажном носителе в срок, установленный Банком для приема данных платежных поручений.

7.2.4. В процессе проведения сеанса электронной связи с использованием Системы Клиент имеет возможность:

- получить информацию о совершенных операциях по его Счетам в Банке (выписки по его Счетам в Банке),
- получить информацию о текущих остатках средств на его Счетах в Банке,
- передать в Банк созданные им ЭПД и ЭСИД,
- получить информацию о статусе электронных документов, переданных им в Банк,

- принять от Банка созданные Банком и предназначенные Клиенту ЭСИД.

7.2.5. По своему желанию заявить об отключении от Системы (в т.ч. временном), смене средств доступа к Системе, способа получения сеансовых ключей путем представления в Банк соответствующего заявления в письменном виде по форме, установленной в Банке.

## **8. ОТВЕТСТВЕННОСТЬ СТОРОН**

8.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору, виновная Сторона несет ответственность в соответствии с действующим законодательством РФ.

8.2. Клиент соглашается на обмен документами в электронном виде с использованием Системы и принимает на себя все риски, связанные с возможным нарушением конфиденциальности (несанкционированного доступа к передаваемой информации третьих лиц) и иные риски, связанные с использованием сети Интернет.

8.3. Банк не несет ответственности за возникновение конфликтных ситуаций вне сферы его контроля, в том числе в случаях:

- разглашения Клиентом третьим лицам средств доступа к Системе, аналога собственноручной подписи, используемых в Системе;
- неверно указанных Клиентом средств доступа к Системе или сеансового ключа;
- неверного или неполного указания Клиентом реквизитов ЭПД;
- непредставления Клиенту услуги, вызванного некачественной работой сторонних лиц;
- технической неисправности компьютера Клиента, с которого осуществляется доступ в Систему.

8.4. Банк не несет ответственности за результаты расчетов и информацию о бюджете Клиента, полученную Клиентом в системе «СМП ОН-Банк» (вне системы «СМП Онлайн»), а также за риски, понесенные Клиентом результате использования указанной информации.

8.5. Сторона, не исполнившая или ненадлежащим образом исполнившая обязательство по настоящему Договору, не несет за это ответственности перед другой Стороной, если докажет, что надлежащее исполнение оказалось невозможным вследствие наличия обстоятельств непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств, не зависящих от воли Сторон, в т.ч. военных действий, стихийных бедствий, срыва в работе компьютерных систем, средств связи, отключения электроэнергии и т.п.; принятия решений органами государственной власти и управления, Банком России, повлекших за собой невозможность исполнения настоящего Договора.

## **9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ**

9.1. Все споры, возникающие из настоящего Договора или в связи с ним, в том числе касающиеся его изменения, исполнения, прекращения или недействительности, передаются на разрешение постоянно действующего Третейского суда при Банке в соответствии с регламентом этого суда в количественном и персональном составе судей, назначенном для рассмотрения конкретного спора по усмотрению Председателя указанного Третейского суда.

При этом Стороны договорились, что решение Третейского суда по конкретному спору является окончательным и не может быть оспорено. Правила постоянно действующего Третейского суда рассматриваются в качестве неотъемлемой части третейского соглашения.

9.2. Стороны признают, что электронные документы Клиента, созданные в Системе, являются доказательным материалом для решения спорных вопросов, возникших между Сторонами. При этом ЭПД рассматриваются в том виде, в котором они поступили в Банк по каналам связи.

## **10. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА**

10.1. Настоящий Договор вступает в силу с даты представления Клиентом в Банк надлежаще оформленного Заявления о дистанционном банковском обслуживании и действует одновременно с заключенным(ими) между Клиентом и Банком договором(ами), в соответствии с которым(ими) открыт(ы) Счет(а), и/или иным договором, соглашением и т.п. между Сторонами по предоставлению/оказанию Банком Клиенту банковских услуг, в рамках которого(ых) возможно осуществление дистанционного банковского обслуживания и информационного обмена электронными документами между Сторонами посредством Системы.

Расторжение всех договоров, соглашений и т.п. между Сторонами по предоставлению/оказанию Банком Клиенту банковских услуг, в рамках которых возможно осуществление дистанционного банковского обслуживания и информационного обмена электронными документами между Сторонами посредством Системы, автоматически влечет за собой прекращение действия настоящего Договора.

10.2. Каждая из Сторон вправе расторгнуть настоящий Договор в одностороннем порядке, письменно уведомив об этом другую Сторону за 10 (Десять) рабочих дней до даты расторжения.

10.3. При расторжении настоящего Договора информация о Клиенте, все его документы и данные о совершенных им финансовых операциях перемещаются Банком в архив Системы, и хранятся в нем в течение 5 (Пяти) лет. После истечения данного срока вся указанная выше информация удаляется Банком из Системы безвозвратно.

## **11. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ПРАВИЛА И ИЗМЕНЕНИЕ ТАРИФОВ**

11.1. Банк вправе в одностороннем порядке вносить изменения в настоящие Правила, в том числе путем утверждения новой редакции Правил.

11.2. Для вступления в силу изменений, внесенных в настоящие Правила Банком, Банк обязан опубликовать информацию об изменениях в порядке, предусмотренном п. 2.3 настоящих Правил. Банк не несет ответственности, если информация об изменении настоящих Правил, опубликованная в порядке, установленные настоящими Правилами, не была получена, и/или изучена, и/или правильно понята Клиентом

11.3. Изменения настоящих Правил, в том числе внесенные Банком в связи с изменением законодательства Российской Федерации, вступают в силу с соответствующей даты, указанной в опубликованной информации.

11.5. Любые изменения настоящих Правил с даты их вступления в силу равно распространяются на всех лиц, присоединившихся к Правилам, в том числе присоединившихся к Правилам ранее дня вступления изменений в силу.

11.6. Банк вправе в одностороннем порядке устанавливать или изменять Тарифы. Изменения Тарифов вступают в силу с соответствующей даты, указанной в опубликованной информации.

## **12. ПРОЧИЕ УСЛОВИЯ**

12.1. Все, что не предусмотрено настоящими Правилами, регулируется в соответствии с действующим законодательством Российской Федерации.

12.2. Если какое-либо из положений настоящих Правил по какой-либо причине станет недействительным, это не затрагивает действительность других положений настоящих Правил.

12.3. Ни одна из Сторон не может передавать свои права и обязательства по Договору какой-либо третьей стороне без письменного согласия на то другой Стороны.

**ПРАВИЛА**  
**информационной безопасности при использовании систем дистанционного**  
**банковского обслуживания через сеть Интернет**

**1. Общие положения**

**1.1. Термины и определения.**

**Банк** – ОАО «СМП Банк» (Головной офис, филиалы и внутренние структурные подразделения (дополнительные, операционные и кредитно-кассовые офисы Банка/филиала).

**Защитная мера** - сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения информационной безопасности в Системе.

**Злоумышленник** - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

**Злоумышленные действия** – любые действия, совершаемые Злоумышленником в Системе.

**Информационная безопасность** - безопасность, связанная с угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

**Инцидент информационной безопасности (Инцидент)** - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, т.е. реализацию нарушения свойств информационной безопасности информационных активов Банка. Нарушение может вызываться источниками угроз информационной безопасности: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

**Карта** – банковская карта, предназначенная для совершения операций за счет средств, находящихся на счете Клиента.

**Клиент** – физическое лицо/индивидуальной инфраструктуры/физическое лицо, осуществляющее в установленном законодательстве РФ порядке частной практикой, являющее(ий)ся пользователем Системы, а также юридическое лицо, уполномоченные представители которого являются пользователями Системы.

**Обработка риска нарушения информационной безопасности** - процесс выбора и реализации защитных мер, снижающих риск нарушения информационной безопасности, или мер по переносу, принятию или уходу от риска.

**Риск** - мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

**Риск нарушения информационной безопасности** - риск, связанный с угрозой информационной безопасности.

**Система** – система дистанционного банковского обслуживания

**Угроза** - опасность, предполагающая возможность потерь (ущерба).

**ЭЦП** – электронная цифровая подпись.

1.2. Настоящие Правила составлены в соответствии с требованиями действующего законодательства Российской Федерации, стандартом Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» и другими нормативными документами Банка России, Международными стандартами ISO 27001:2005 и ISO 17799.

1.3. Настоящие Правила определяют рекомендуемые Банком действия Клиентов по Обработке рисков нарушения информационной безопасности при использовании Системы.

1.4. При работе с Системой через сеть Интернет необходимо учитывать следующее:

1.4.1. 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) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими.

1.4.2. Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет.

1.4.3. Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные к/из сети Интернет.

1.4.4. Гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

**2. Ответственность сторон**

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему, Клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

2.2. Клиент уведомлен о том, что за пользование нелегализованным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

2.3. Срок для предъявления претензий по услугам, оказанным с использованием Системы, составляет 10 (Десять) рабочих дней с момента осуществления операции. По каждой опротестовываемой операции оформляется отдельная претензия.

2.4. Окончательное решение об использовании Защитных мер, предлагаемых Банком в разделе 3 настоящих Правил, принимает сам Клиент.

2.5. Банк вправе устанавливать ограничения по составу услуг и объему операций, доступных при использовании той или иной Защитной меры.

2.6. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы. Содержимое журнала Системы используется при разрешении спорных ситуаций.

**3. Рекомендуемые Клиенту Защитные меры**

3.1. Не сообщайте посторонним лицам персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашим счетам.

3.2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

3.3. Не используйте функцию запоминания логина и пароля в браузерах.

3.4. Не используйте одинаковые логин и пароль для доступа к различным системам.

3.5. Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковском счете.

3.6. Всегда явным образом завершайте сеанс работы с Системой, используя пункт меню «Выход».

3.7. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки). После возвращения к своему персональному компьютеру обязательно смените логин и пароль.

3.8. Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка), перезвоните в Службу клиентской поддержки Банка по телефону (495) 981-8181 и сообщите о письме или перешлите его на адрес [ibank@smpbank.ru](mailto:ibank@smpbank.ru). **Банк никогда не просит передать данные по электронной почте.** Обновление ключевых персональных данных осуществляется только сотрудником Банка.

Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

3.9. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способное украсть Ваши идентификационные данные для входа в Систему.

3.10. При регистрации на сторонних интернет-сайтах всегда изменяйте пароли, которые приходят Вам по электронной почте. Помните, что Банк никогда не направляет пароли по электронной почте.

3.11. Регулярно, не реже одного раза в месяц, производите смену пароля.

3.12. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < > . Настоятельно рекомендуется использовать специализированные программы-генераторы паролей (<http://www.infotecs.ru/Soft/pass.htm>).

3.13. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

3.14. При использовании ЭЦП не позволяйте третьим лицам производить за Вас генерацию ключей.

3.15. При использовании ЭЦП присоединяйте ключевой носитель ЭЦП к компьютеру непосредственно перед началом работы с Системой. По окончании работы извлекайте ключевой носитель из компьютера.

3.16. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что за пользование нелегальным программным обеспечением предусмотрена уголовная ответственность в соответствии со статьей 146 УК РФ, **использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа к Ваш компьютер.**

3.17. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль в Системе.

3.18. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников.

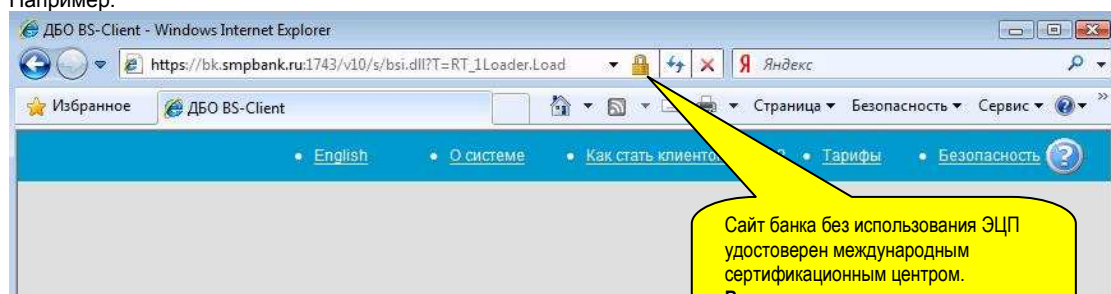
3.19. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

3.20. Не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены Злоумышленниками и использованы для получения доступа к Вашим счетам.

3.21. Если Вам пришло письмо или SMS-сообщение о выигрыше в акции, лотерее, розыгрыше удостоверьтесь в его подлинности, прежде чем отсылать деньги на чей-то счет с использованием Системы. Все акции, проводимые Банком не требуют от Клиента перевода денежных средств для получения приза.

3.22. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в Систему.

Например:



 **testtonk,**  
Добро пожаловать в систему ДБО BS-Client v.3!

Последний визит: 07.02.2011, 13:35:48.6500  
[EXTIP: 195.146.76.194][IP: 192.168.101.235][MAC: 00-1A-4D-39-C6-F9]

В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов ОАО "СМП Банк", сообщите об этом по электронной почте [ibank@smpbank.ru](mailto:ibank@smpbank.ru).

3.23. Используйте предлагаемые Банком услуги по дополнительному информированию о входе в Систему и совершаемых операциях. Регулярно проверяйте входящую электронную почту, а также контролируйте выписки по счетам. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

3.24. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно смените логин и пароль и сообщите об Инциденте информационной безопасности в Службу технической поддержки Банка. Следуйте указаниям специалистов Банка.

3.25. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо подать заявление на временное отключение от Системы и произвести смену ключей ЭЦП (в случае использования).