Памятка для клиента физического лица, использующего систему «Интернет-Клиент»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая памятка устанавливает условия и порядок осуществления электронного взаимодействия, порядок подключения и работы Клиента в системе «Интернет-Клиент», а также определяет требования по обеспечению информационной безопасности при работе в системе «Интернет-Клиент».

1.2. Автоматизированная система электронного документооборота «Интернет-Клиент» (далее - система «Интернет-Клиент») предназначена для подготовки, учета и предварительной обработки электронных документов (далее – ЭД) Клиентов Банком. Она построена на основе технологии всемирной сети Интернет, обеспечивает конфиденциальность, надежность и достоверность информации, установление подлинности отправителя, проверку целостности и авторства документа. Также реализована возможность доказательного разрешения споров на основе программных и технических средств, организационных мер и договорно-правовых норм.

1.3. Электронные платежные документы, применяемые в системе «Интернет-Клиент», юридически эквивалентны бумажным платежным документам, используемым в соответствии с нормативными актами Банка России, и являются основанием для осуществления операции по счету Клиента.

1.4. Стороны признают, что система телекоммуникации, обработки и хранения информации является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а система защиты информации, обеспечивающая разграничение доступа, шифрование, контроль целостности и аналог собственноручной подписи, является достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и для разрешения спорных ситуаций.

1.5. Электронный документ порождает обязательства Сторон, если он инициирующей Стороной должным образом оформлен, заверен аналогом собственноручной подписи (далее - АСП), и передан на обработку, а принимающей Стороной принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление «В обработке» в строке статуса, отправленного документа. Под электронным документом подразумеваются расчетные, платежные и пр. документы.

1.6. Сведения, содержащиеся в документах, переданных Сторонами друг другу по системе «Интернет-Клиент», персональные электронные адреса, идентификационные параметры, регистрационные номера, пароли и АСП обеих Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы разрешительной экспертной комиссии по разбору Споров, являются конфиденциальными сведениями. Конфиденциальные сведения не подлежат разглашению третьим лицам ни при каких обстоятельствах, кроме установленного законом порядка.

II. УСЛОВИЯ И ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ БАНКОМ И КЛИЕНТОМ

2.1. Программное обеспечение Банка настроено на взаимодействие с системой «Интернет-Клиент» и предполагает использование этой системы Клиентом.

2.2. Электронные документы представляют собой электронные формы документов, заполняемые Клиентом в системе «Интернет-Клиент», согласно наименованиям полей и правилам, принятым в Банке. Часть полей заполняется автоматически в соответствии со встроенными справочниками реквизитов. Заполнение документов возможно только после установления защищенного (с использованием алгоритмов шифрования и обеспечения целостности) соединения между Клиентом и Банком.

2.3. Заполняемые в системе «Интернет-Клиент» документы проходят предварительную автоматическую проверку (на дату документа, на присутствие обязательной информации в полях документа, на соответствие вводимых данных - реквизитам, записанным во встроенном справочнике и иное) в соответствии с принятой технологией.

2.4. После заполнения электронной формы документа Клиентом и его проверки осуществляется подписание документа и отправка его в Банк. Подробности о порядке работы описаны в Руководстве пользователя (передается на диске Клиенту вместе с другой документацией).

2.5. На этапе обработки документов в Банке осуществляется автоматический контроль (на соответствие АСП, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка, РКЦ и иное) в соответствии с принятой технологией. В случае выявления несоответствий в ходе проверки документа, операции по документу не проводятся, а Клиенту предоставляется информация с указанием причин отказа в приеме на обработку ЭД.

2.6. Активной стороной при установлении связи является Клиент.

2.7. Основанием для отказа Банка от исполнения электронного платежного документа служат:

- отрицательный результат проверки АСП;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие ЭД требованиям Банка России и ООО «Банк БЦК-Москва».

2.8. Прием ЭД Клиента производится Банком ежедневно круглосуточно (в режиме «24х7»), кроме времени на профилактические работы. Банк производит списание денежных средств со Счетов Клиента в день получения ЭД, поступивших в Банк в течение операционного времени. Документы, поступившие после операционного времени обрабатываются в соответствии с действующими Тарифами Банка.

2.9. Банк уведомляет Клиента посредством SMS-сообщения и (или) Email - сообщения об операциях по Счету, совершенных с использованием системы «Интернет-Клиент», посредством изменения статуса ЭД, в том числе в случае отказа в исполнении документа с указанием причины. Уведомление, направленное по системе «Интернет-Клиент», считается полученным Клиентом с момента отправления его Банком.

III. РАБОТА КЛИЕНТА В СИСТЕМЕ «ИНТЕРНЕТ-КЛИЕНТ»

3.1. Общие положения

3.1.1. Защита информации в системе «Интернет-Клиент» является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения и специализированных программных и технических

средств и организационных мер, организации хранения программного обеспечения, используемого в системе «Интернет-Клиент».

3.1.2. Комплексная защита информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание АСП;
- АСП под ЭД;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения ЭД получателем;
- подтверждение авторства и целостность ЭД;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- разбор конфликтных ситуаций.

3.2. Порядок регистрации Клиента в системе «Интернет-Клиент»

3.2.1. По заявлению Клиента обслуживание его банковских счетов, открытых в ООО «Банк БЦК-Москва», может осуществляться с помощью системы «Интернет-Клиент». В этом случае сотрудники операционного отдела Банка информируют Клиента по вопросам: общего назначения системы «Интернет-Клиент», условиях ее установки, размера, сроков и порядка оплаты данной услуги. По техническим вопросам: порядок регистрации в системе «Интернет-Клиент», формирование АСП Клиента, безопасность системы «Интернет-Клиент» Клиента консультирует техническая поддержка Банка. По вопросам документального оформления работы в системе «Интернет-Клиент» Клиента консультируют сотрудники операционного отдела Банка.

3.2.2. Для подключения к системе «Интернет-Клиент» по обслуживанию банковского счета Клиенту необходимо представить в Банк следующие документы:

- Договор об обслуживании физического лица по системе «Интернет-Клиент» (2 экземпляра).

3.2.3. Процедура регистрации производится в Банке.

3.2.4. В процессе регистрации Клиент самостоятельно выбирает АСП (сеансовые ключи и (или) одноразовые пароли, отправляемые в виде SMS - оповещения на мобильный телефон Клиента) для работы в системе «Интернет-Клиент».

3.2.5. Логин и пароль учетной записи Клиента является конфиденциальной информацией.

3.2.6. Клиент вправе изменить пароль по своему усмотрению в любое время.

3.2.7. Клиент несет ответственность за обеспечение сохранности АСП от несанкционированного доступа.

3.3. Порядок хранения АСП

3.3.1. Надежность защиты от несанкционированного доступа и подлинности передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации АСП.

3.3.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение АСП и паролей. В случае потери, кражи, несанкционированного копирования или любого подозрения о компрометации АСП Клиент обязан прекратить работу в системе «Интернет-Клиент» и уведомить Банк либо по телефону, размещенному на официальном сайте Банка, либо направить письмо по электронному адресу **support@bcc-msk.ru**, а так же руководствоваться п.п. 6.1.5. - 6.1.6. Договора об обслуживании физического лица по системе «Интернет-Клиент».

3.3.4. Не допускается передавать АСП третьим лицам.

3.4. Порядок смены АСП

3.4.1. Смена АСП производится в случае:

- компрометации АСП;
- заявления одной из Сторон.

3.5. Порядок блокировки учетной записи

3.5.1. Банк блокирует (приостанавливает действие) учетной записи с момента получения письменного заявления Клиента о блокировке учетной записи (содержащего причину блокировки). В экстренных случаях блокировка может быть произведена при уведомлении иным способом (по телефону, по электронной почте, факсу и т.п.) с последующим предоставлением подписанного заявления Клиента.

3.5.2. Снятие блокировки производится на основании заявления Клиента с подтверждением об устранении причин, приведших к блокированию учетной записи. В случае блокировки учетной записи по инициативе Банка, снятие блокировки производится по согласованию с Клиентом.

3.5.3. Банк вправе блокировать учетную запись Клиента в одностороннем порядке в случае отказа Клиента от оформления документа на бумажном носителе (подлиннике).

3.5.4. Банк обязан блокировать работу счета/счетов Клиента в системе «Интернет-Клиент» в следующих случаях:

- возникновения подозрений в компрометации АСП;
- по письменному заявлению Клиента.

3.6. Порядок действий в случае компрометации секретных ключей АСП

3.6.1. Компрометация ключа – утрата доверия к тому, что используемый АСП недоступен посторонним лицам. К событиям, связанным с компрометацией АСП, относятся следующие:

- утрата АСП;
- временный доступ посторонних лиц к АСП, иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к АСП третьих лиц.

3.6.2. В случае компрометации или подозрения на компрометацию АСП, Клиент обязан предпринять все меры для прекращения любых операций с использованием этого АСП и незамедлительно известить уполномоченных сотрудников Банка о факте компрометации в соответствии с порядком установленным п. 3.5. настоящей Памятки.

В случае выявления хищения денежных средств, руководствоваться Порядком действий в случае выявления хищения денежных средств в системе «Интернет-Клиент» (физические лица), расположенном на официальном сайте Банка http://www.bcc-msk.ru.

IV. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРИ РАБОТЕ В СИСТЕМЕ «ИНТЕРНЕТ-КЛИЕНТ»

4.1. В целях предотвращения компрометации АСП **Клиент обязан выполнять следующие требования**:

4.1.2. Ограничить доступ к компьютерам, используемым для работы в системе «Интернет-Клиент».

4.1.3. Обеспечить безопасность и целостность среды исполнения на своем компьютере (отсутствие вирусов и программ-закладок).

4.1.4. Обеспечивать целостность и сохранность программных средств, электронных документов, защиту АСП, паролей доступа и другой информации, передаваемой и получаемой по системе «Интернет-Клиент».

4.1.5. На компьютерах, используемых для работы в системе «Интернет-Клиент», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п.

4.1.6. Перейти к использованию лицензионного программного обеспечения (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного программного обеспечения.

4.1.7. Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз.

4.1.8. Применять на рабочем месте специализированные программные средства безопасности: антивирусные средства антишпионское программное обеспечение и т.п.

4.1.9. Обеспечивать контроль за выполняемыми действиями при обслуживании компьютера Клиента

4.1.10. Никогда не передавать АСП третьим лицам для работы в системе «Интернет-Клиент», настроек взаимодействия с Банком и т.п.

4.1.11. При возникновении любых подозрений на компрометацию АСП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк и заблокировать учетную запись.

4.1.12. В случае проявления необычного поведения в системе «Интернет-Клиент» или каких-то изменений в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет – заблокировать учетную запись.

4.2. В случае невыполнения Клиентом требований, указанных, в п. 4.1. настоящей Памятки, Банк не несет ответственности за неправомерное списание денежных средств со счета Клиента.