

СОГЛАШЕНИЕ № _____
об обслуживании банковских счетов с использованием системы ДБО
«ИНТЕРНЕТ-КЛИЕНТ»

г. Санкт - Петербург

«___» _____ 20___ г.

Открытое акционерное общество «Санкт – Петербургский Индустриальный Акционерный Банк», именуемое в дальнейшем Банк, в лице _____, действующей(его) на основании _____, и _____, именуемый (ое) в дальнейшем Клиент, в лице _____, действующего на основании _____, вместе именуемые Стороны, заключили настоящее Соглашение (далее Соглашение) о нижеследующем.

1. Термины и определения

В настоящем Соглашении используются следующие термины и определения:

• **Система электронного документооборота «ИНТЕРНЕТ - КЛИЕНТ» (Система)** – автоматизированная компьютерная система, позволяющая Клиенту осуществлять информационное взаимодействие с Банком в режиме удаленного доступа с использованием глобальной информационно-телекоммуникационной сети Интернет (далее Интернет);

• **Электронный документ (ЭД)** – совокупность данных, зафиксированная на магнитных, оптических или иных устройствах хранения данных, передаваемая по телекоммуникационным каналам с реквизитами, позволяющими идентифицировать эти данные и их автора. Электронный документ может быть создан на основе документа на бумажном носителе, на основе другого электронного документа или порождаться в процессе информационного взаимодействия Клиента и Банка;

• **Электронный платежный документ (ЭПД)** – электронный документ, представляющий собой поручение Клиента на совершение операции по счету Клиента, открытому в Банке, составленное в электронном виде и содержащее все предусмотренные банковскими правилами реквизиты, подписанное первой и второй электронными цифровыми подписями (или одной подписью, в случае отсутствия в организации должностного лица, которому может быть предоставлено право второй подписи) владельцев электронных цифровых подписей Клиента, имеющий равную юридическую силу с платежным документом, составленным на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц (лица) Клиента и заверенными оттиском печати в соответствии с предоставленной Банку карточкой с образцами подписей и оттиска печати, и являющийся основанием для совершения операции по счету Клиента, открытому в Банке;

• **Электронная цифровая подпись (ЭЦП)** – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

• **Владелец ЭЦП** – уполномоченное должностное лицо Клиента, указанное в Карточке с образцами подписей и оттиска печати, электронная цифровая подпись которого зарегистрирована в Банке;

• **Система криптографической защиты информации (СКЗИ)** – система защиты электронного документа от несанкционированного изменения и доступа к его содержимому посторонних лиц при помощи алгоритмов криптографического преобразования. В рамках Системы под криптографической защитой понимается шифрование, электронная цифровая подпись и вычисление хэш-функций программного обеспечения;

• **Персональный идентификатор «Рутокен»** – персональное устройство доступа к информационным ресурсам, полнофункциональный аналог смарт-карты, выполненный в виде usb – брелока. Идентификатор предназначен для безопасного хранения и использования цифровых сертификатов, ключей шифрования и ЭЦП.

• **Персональный идентификационный номер (пин-код)** – аналог пароля, который нужно набрать, чтобы получить доступ к чтению закрытого ключа ЭЦП, хранящегося в криптоконтейнере персонального идентификатора «Рутокен».

БАНК _____

КЛИЕНТ _____

• **Хэш-функция** – сопоставление произвольного набора двоичных данных образу фиксированной небольшой длины, позволяющее использовать эту функцию в системе криптографической защиты для формирования электронной цифровой подписи и контроля целостности программного обеспечения;

• **Ключевая информация** – набор двоичных данных, используемый в системе криптографической защиты, состоящий из секретного и публичного ключей;

• **Закрытый ключ** – секретная часть ключевой информации, представляющая собой уникальную последовательность двоичных данных и предназначенная для создания в электронном документе электронной цифровой подписи владельца ЭЦП;

• **Открытый ключ** – несекретная часть ключевой информации, связанная с секретным ключом с помощью особого математического соотношения и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

• **Ключевые носители** – съемные носители, содержащие ключевую информацию;

• **Компрометация ключевой информации** – утрата доверия к тому, что используемый Закрытый ключ недоступен посторонним лицам.

К событиям, связанным с компрометацией ключевой информации, относятся:

- утрата ключевых носителей, в том числе с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- утрата ключей от сейфа в момент нахождения в нем ключевых носителей;
- временный доступ посторонних лиц к ключевой информации;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к Системе посторонних лиц.

2. Предмет Соглашения

2.1. Настоящее Соглашение определяет порядок организационно-технического обеспечения обмена документами в электронной форме между Банком и Клиентом и осуществления расчетов по поручению Клиента посредством Системы, а также способ подтверждения авторства и процедуру установления подлинности таких документов.

2.2. Клиент поручает Банку исполнять операции по своим счетам, открытым в Банке, на основании ЭД, полученных Банком по Системе и заверенных зарегистрированными в Банке ЭЦП лиц, имеющих право подписи.

2.3. Банк принимает на себя обязательства по расчетному обслуживанию Клиента с использованием Системы, а именно:

- принимает и исполняет поручения Клиента, оформленные в виде ЭПД, на выполнение операций по счетам Клиента, указанных в Заявлении на подключение к системе дистанционного банковского обслуживания, заполненного по утвержденной форме Банка;

- передает Клиенту выписки по его счетам в виде ЭД;

- передает Клиенту текстовые ЭД;

- передает Клиенту информационную и справочную информацию.

2.4. Клиент и Банк признают, что оформленные надлежащим образом ЭПД, которые были получены Банком, успешно расшифрованы, и проверка ЭЦП которых дала положительный результат, имеют юридическую силу платежных документов, составленных на бумажном носителе и заверенных собственноручными подписями уполномоченных лиц с приложением печати Клиента, и являются основанием для осуществления операций по счетам Клиента.

2.5. Стороны признают, что используемое в Системе программное СКЗИ, обеспечивающее шифрование и формирование ЭЦП, достаточно для подтверждения подлинности и целостности ЭД, а также для обеспечения защиты ЭД от несанкционированного доступа.

3. Порядок подключения к Системе

3.1. Подключение Клиента к Системе производится Банком на основании Заявления на подключение к системе дистанционного банковского обслуживания.

3.2. Необходимым условием подключения Клиента к Системе является наличие автоматизированного рабочего места (АРМ), оборудованного из собственных технических средств Клиента, минимальная конфигурация которого включает:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 гигагерц (ГГц) или выше;
- 32 МБ оперативной памяти;
- 40 МБ свободного дискового пространства;
- русифицированный принтер;
- операционную систему Microsoft® Windows® XP (с установленным пакетом обновлений Service Pack 3)/ Microsoft® Windows® 7/Vista;
- установленный Интернет-обозреватель Microsoft® Internet Explorer версии 6 и выше;

- как минимум один свободный универсальный последовательный порт USB;
- доступ в глобальную сеть Интернет по протоколам HTTP и HTTPS и портам доступа 80/tcp, 443/tcp;
- легально – приобретенное, постоянно обновляемое антивирусное программное обеспечение, а так же выполнение требований, находящихся в Приложении 1 к настоящему Договору.

3.3. Установка и настройка Системы осуществляется Клиентом самостоятельно с использованием документации и рекомендаций Банка из эталонной дистрибутивной копии программного обеспечения, предоставленной Банком. В случае невозможности установки Клиентом Системы самостоятельно, установку осуществляет сотрудник Банка. Услуга по установке Системы сотрудником Банка оплачивается Клиентом согласно действующих Тарифов Банка.

В число работ, выполняемых сотрудником Банка при подключении Клиента к Системе, входят:

- проверка возможности установки клиентской части Системы на выделенное АРМ,
- установка и настройка клиентской части Системы;
- обучение уполномоченных лиц Клиента работе с Системой.

Указанный выше перечень выполняемых сотрудником Банка работ является исчерпывающим. Специалисты Банка не осуществляют настройку сопутствующего программного обеспечения (прокси сервера, антивирусы, 1С и т.д.) и операционной системы.

3.4. Факт подключения Клиента к Системе оформляется Актом приема-передачи во временное использование программного обеспечения, подписываемого уполномоченными представителями Банка и Клиента.

3.5. Ключи ЭЦП выдаются руководителю Клиента либо уполномоченному лицу Клиента. Для получения ключей ЭЦП получателю необходимо иметь при себе паспорт и печать Клиента. В случае смены и регенерации персонального идентификатора «Рутокен» получателю необходимо иметь при себе паспорт, печать Клиента и персонального идентификатора «Рутокен». В случае отсутствия персонального идентификатора «Рутокен», Клиенту выдаётся новый персональный идентификатор «Рутокен», оплата за который осуществляется согласно действующим тарифам Банка.

4. Порядок регистрации электронной цифровой подписи

4.1. Регистрация Открытого ключа ЭЦП Клиента в Системе оформляется Сертификатом Открытого ключа по утвержденной Банком форме. Сертификат подписывается уполномоченными лицами Банка и Клиента. Сертификаты хранятся по одному экземпляру у Банка и Клиента.

4.2. Закрытые Ключи ЭЦП Клиента, хранящиеся на персональном идентификаторе «Рутокен» считаются действительными со дня издания Сертификата в течение 1 года. По истечении срока действия ключей ЭЦП требуется плановая смена ключей ЭЦП, хранящихся на персональном идентификаторе «Рутокен». Сообщение о необходимости плановой смены ключей ЭЦП формируется в Системе автоматически за 30 дней до окончания срока действия ключей ЭЦП.

4.3. Для подписи документов ЭЦП соответствующее уполномоченное лицо Клиента использует свой личный Закрытый ключ, хранящийся на персональном идентификаторе «Рутокен», доступ к которому осуществляется при вводе пин-кода Клиента. Клиент несет полную ответственность за подлинность и конфиденциальность Закрытого ключа, принадлежащего его должностным лицам. В частности, все документы, подписанные при проверке действительным Открытым ключом лица является корректной, считаются подписанными этим лицом, даже если подпись была поставлена другим лицом, получившим каким-либо образом доступ к Закрытому ключу этого лица.

4.4. Ключи ЭЦП перестают считаться действительными с момента получения Банком Заявления об отмене действия/изменении ключевой информации, составленного по утвержденной Банком форме. Заявление направляется Клиентом в следующих случаях:

- в случае изменения списка лиц, имеющих право подписи согласно карточке с образцами подписей и оттиска печати;
- в случае смены ключей подписи уполномоченных лиц, уже имеющих право подписи;
- в случае утраты Секретного ключа одного из лиц или его компрометации;
- в иных случаях по согласованию Сторон.

После получения Заявления Банком производится смена ключевой информации и оформляется новый Сертификат и Акт приема - передачи во временное использование программного обеспечения.

4.5. Для исключения возможности подбора кода доступа устанавливается трехкратное ограничение на количество ошибок при введении пин-кода для персонального идентификатора «Рутокен». Разблокировка персонального идентификатора «Рутокен» осуществляется в Головном отделении Банка в присутствии Владельца ЭЦП.

4.6. В случае утраты пин-кода к персональному идентификатору «Рутокен» требуется его внеплановая регенерация аналогично п. 4.1 и 4.2 настоящего Соглашения.

5. Порядок и условия совершения операций по счетам и режим счетов

5.1 Проведение всех расчетных операций и получение всей информации по Системе осуществляется Клиентом в режиме онлайн посредством глобальной сети Интернет. При этом протоколом передачи информации в Системе является HTTPS (HTTP/1.1 через SSL или TLS), являющийся международным стандартом (RFC 2818).

5.2. Все справочники, шаблоны ЭД, сами ЭД после их сохранения, а также выписки и вся иная информация в Системе находятся в Банке и доступны для работы Клиенту только во время проведения авторизованных сеансов связи с Банком через Интернет.

5.3. Прием ЭД от Клиента осуществляется Банком круглосуточно в автоматическом режиме.

Банк производит списание денежных средств со счета Клиента по поступившим в Банк ЭПД не позднее дня, следующего за днем поступления указанного ЭПД. Списание со счетов Клиентов платежных документов, принятых от Клиентов в послеоперационное время, осуществляется на следующий рабочий день.

5.4. Клиент в соответствии с полученным в электронном виде «Руководством Пользователя» формирует и передает в Банк ЭД необходимого вида, а также дает Банку инструкцию на его исполнение. При получении ЭД Банк осуществляет его проверку и сохраняет, а при получении инструкции на исполнение ЭД также осуществляет его проверку и принимает ЭД к исполнению.

5.5. Статусы ЭД, однозначно отражающие их состояние, автоматически отслеживаются во время сеансов связи, проводимых Клиентом.

5.6. Основанием для отказа от исполнения Банком ЭПД Клиента служат:

- отсутствие в ЭПД зарегистрированной ЭЦП Клиента или отрицательный результат проверки ЭЦП;
- неверные или неполные реквизиты ЭПД;
- недостаток информации и необходимых документов по проводимой Клиентом операции в случаях, предусмотренных действующим законодательством, требованиями валютного контроля и нормативными документами Банка России;
- нарушение действующего законодательства, нормативных актов Банка России, условий настоящего Соглашения или несоответствие операции режиму счета.

• подозрение на несанкционированный доступ к Системе на стороне Клиента

5.7. При обнаружении ошибок в ЭПД или при возникновении сбоев во время передачи ЭД по телекоммуникационным каналам Банк направляет Клиенту ЭД с указанием типа ошибки или характера сбоя, возникшего в телекоммуникационных каналах. При невозможности использовать Систему для передачи указанного ЭД, сообщение передается по телефону.

5.8. Для отзыва переданного в Банк ЭД Клиент выполняет следующие действия:

- в соответствии с «Руководством Пользователя» формирует запрос на отзыв и дает Банку инструкцию на его исполнение;
- Банк принимает запрос на отзыв ЭД только в том случае, если ЭД еще не исполнен или у Банка имеется технологическая возможность отменить его исполнение.

5.9. На следующий операционный день Клиент выполняет следующие действия:

- после 10:00 получает выписки по своим счетам в электронном виде при помощи Системы;
- в случае необходимости, самостоятельно создает запросы выписки в течение дня;
- выверяет их с отправленными ЭПД документами, и при обнаружении расхождений связывается с Банком по телефону и выясняет причины расхождений.

5.10. Стороны устанавливают, что вся информация по Системе считается доведенной до сведения Клиента по истечении 3 (трех) банковских дней с даты ее размещения на Интернет-сервере Системы (включая день размещения).

6. Права и обязанности сторон при исполнении Соглашения

6.1. Банк обязуется:

- произвести подключение Клиента к Системе в соответствии с разделом 3 настоящего Соглашения;
- обеспечивать круглосуточный прием ЭД от Клиента;
- исполнять поручения Клиента в соответствии с полученными от него ЭПД, прошедшими проверку подлинности ЭЦП, полноты переданной информации, соответствия структуры и состава реквизитов нормативно-справочной информации;
- предоставлять Клиенту возможность получения выписок о состоянии его счетов в электронном виде;
- обеспечивать защиту банковской части Системы от несанкционированного доступа и конфиденциальность информации, связанной с использованием Системы, в соответствии с действующим законодательством;
- сообщать Клиенту об обнаружении попыток несанкционированного доступа к Системе, если это затрагивало операции Клиента, и о случаях компрометации Ключевой информации Банка;

БАНК _____

КЛИЕНТ _____

- прекратить прием ЭД от Клиента в случае компрометации Ключевой информации Клиента. Возобновить прием ЭД от Клиента после регистрации вновь сгенерированной Ключевой информации и подписания Сертификата Открытого ключа;

- предоставлять Клиенту новые версии программного обеспечения Системы, а также оказывать помощь в случае сбоев в работе программного обеспечения Системы;

- организовать надлежащий режим хранения и резервного копирования информации, исключающий ее потерю, поддерживать архивы файлов протоколов, электронных документов и системных журналов в течение 5 (пяти) лет, а в случае возникновения споров – до их разрешения.

6.2. Банк вправе:

- отложить подписание Клиента к Системе в случае несоответствия оборудования АРМ Клиента требованиям п. 3.2 настоящего Соглашения до устранения несоответствия;

- проверять правильность эксплуатации СКЗИ на рабочем месте Клиента;

- в счет погашения денежных обязательств Клиента перед Банком по настоящему Соглашению (включая обязательства по оплате услуг Банка, возмещению расходов Банка и уплате неустойки) в безакцептном порядке списывать со счета Клиента соответствующие суммы. В случае если денежные обязательства Клиента перед Банком выражены в иностранной валюте, списание со счета суммы, эквивалентной сумме задолженности Клиента, в счет погашения денежных обязательств последнего производится Банком по курсу Банка России на день списания. Если курсы соответствующих валют не устанавливаются, списание производится по курсу, установленному Банком;

- приостановить обслуживание Клиента с использованием Системы по истечении 14 календарных дней со дня возникновения задолженности по оплате услуг Банка в соответствии с настоящим Соглашением;

- в случае выявления сомнительной операции после предварительного предупреждения Клиента отказать Клиенту в приеме от него распоряжений на проведение операций, подписанных ЭЦП и потребовать надлежащим образом оформленные расчетные документы на бумажном носителе;

- отказать Клиенту в приеме от него распоряжений на проведение операций, подписанных ЭЦП, в случаях, предусмотренным законодательством.

6.3. Клиент обязуется:

- не изменять технические и программные параметры настроек функционирования Системы без согласования с Банком;

- при работе с Системой следовать «Руководству Пользователя», предоставленному Клиенту Банком в электронном виде;

- соблюдать инструктивные документы по использованию Системы, предоставляемые Банком Клиенту;

- незамедлительно приостановить расчеты с использованием Системы и проинформировать Банк о невозможности использования Системы в случае возникновения технических неисправностей Системы или ее элементов, а также при компрометации или подозрении на компрометацию Ключевой информации;

- не передавать третьим лицам предоставляемое Банком программное обеспечение Системы и документацию;

- при изменении регистрационных данных и (или) должностных лиц Клиента, имеющих право подписи расчетно-денежных документов, и (или) изменении их полномочий, незамедлительно, в день осуществления соответствующих изменений, представить в Банк Заявление об отмене действия/изменении ключевой информации по утвержденной Банком и размещенной на информационном сайте Банка по адресу www.siab.ru форме;

- информировать Банк об изменении почтового адреса, адресов местонахождения АРМ, на которых установлена Система, контактных телефонных номеров;

- организовать делопроизводство и внутренний режим функционирования АРМ Системы таким образом, чтобы исключить возможность его использования лицами, не имеющими допуска к работе с Системой;

- организовать надлежащий режим хранения и резервного копирования информации, исключающий ее потерю, поддерживать архивы переданных и принятых файлов, ЭД и системных журналов в течение 5 (пяти) лет, а в случае возникновения споров – до их разрешения.

- соблюдать требования по работе с СКЗИ (Приложение 1 к настоящему Соглашению);

- оплачивать услуги Банка в соответствии с настоящим Соглашением и Тарифами Банка.

7. Оплата услуг и возмещение расходов Банка

7.1. Клиент обязуется оплачивать услуги Банка по настоящему Соглашению в размерах и на условиях, определенных действующими Тарифами Банка, которые доводятся до сведения Клиента путем размещения в помещениях для обслуживания Клиентов в доступном для ознакомления месте и на информационном сайте банка по адресу www.siab.ru.

БАНК _____

КЛИЕНТ _____

7.2. Комиссия за подключение к Системе списывается Банком со счета Клиента в безакцептном порядке после подписания Соглашения. Комиссия при изменении Клиентом ключевой информации списывается Банком в безакцептном порядке со счета Клиента на основании подданного в Банк Заявления об отмене действия/изменении ключевой информации.

7.3. Банк вправе в одностороннем порядке изменять и дополнять Тарифы, в том числе вводить плату за новые банковские услуги. Информация об изменениях Тарифов доводится до сведения Клиента не позднее, чем за 10 (десять) банковских дней до даты их введения, путем размещения в помещениях для обслуживания Клиентов в доступном для ознакомления месте и на информационном сайте банка по адресу www.siab.ru. Информация об изменениях Тарифов может направляться Банком Клиенту в виде ЭД посредством Системы.

7.4. В случае расторжения настоящего Соглашения по инициативе Клиента Банк в безакцептном порядке списывает со счета Клиента установленную Тарифами сумму абонентской платы за использование Системы в последнем месяце обслуживания в полном объеме, независимо от того, сколько дней обслуживался Клиент с начала месяца.

8. Ответственность сторон и разрешение споров

8.1. Банк не несет ответственности:

- за последствия исполнения ЭПД, подписанных недействительной или скомпрометированной ЭЦП Клиента, поступивших в Банк до получения им информации о недействительности или компрометации ЭЦП Клиента;
- за возможные опечатки и искажения в платежных документах, отправленных Клиентом и заверенных его ЭЦП, возникшие по вине Клиента;
- за неблагоприятные последствия для Клиента, наступившие в результате несанкционированного доступа к Системе неуполномоченных или третьих лиц, возникшего не по вине Банка;
- за неблагоприятные последствия для Клиента, наступившие в результате утечки информации, являющейся банковской тайной, вызванные нарушением Клиентом условий настоящего Соглашения.

8.2. Клиент несет ответственность за правильность и достоверность передаваемой в Банк с помощью Системы информации.

8.3 Клиент несет ответственность за правильное использование СКЗИ.

8.4. Стороны не несут ответственности за неполадки в работе Системы, вызванные неисправностью телекоммуникационных каналов или действием обстоятельств непреодолимой силы, препятствующих выполнению Клиентом и Банком своих обязательств по настоящему Соглашению.

8.5. При возникновении разногласий и споров, связанных с настоящим Соглашением, Клиент и Банк обязуются решать их путем переговоров.

8.6. Для разрешения спорной ситуации, связанной с отказом Клиента от авторства или содержания электронного документа или связанной с отказом Банка от факта приема или исполнения ЭД, переданного Клиентом по Системе, а также с другими ситуациями, возникающими при использовании Системы, создается экспертная комиссия из уполномоченных представителей Клиента и Банка с равным количеством членов комиссии с каждой стороны. В случае необходимости к работе комиссии могут привлекаться представители разработчика Системы и независимые эксперты. Состав комиссии согласовывается Клиентом и Банком.

8.7. Экспертная комиссия создается и приступает к работе в течение 7 (семи) календарных дней со дня поступления письменного заявления Клиента в Банк.

8.8. Экспертная комиссия осуществляет свою работу на территории Банка и должна вынести свое заключение, оформленное соответствующим актом, в течение 30 (тридцати) календарных дней со дня начала работы.

8.9. Признание экспертной комиссией подлинности ЭПД означает, что оспариваемый ЭПД имеет юридическую силу и является основанием для осуществления Банком операций по счету Клиента.

8.10. Непризнание экспертной комиссией подлинности ЭПД означает, что оспариваемый ЭПД не имеет юридической силы и не является основанием для осуществления Банком операций по счету Клиента.

8.11. Если в результате работы экспертной комиссии Банк и Клиент не достигли договоренности, дальнейшее разрешение спора продолжается в установленном действующим законодательством порядке в Арбитражном суде Санкт-Петербурга и Ленинградской области. При этом составленный экспертной комиссией акт признания (непризнания) подлинности ЭПД может быть использован Банком и Клиентом в дальнейшем разбирательстве.

9. Срок действия и порядок расторжения Соглашения

9.1. Настоящее Соглашение вступает в силу с момента подписания и действует в течение срока действия договоров банковского счета, заключенных между Клиентом и Банком.

9.2. Клиент вправе в одностороннем порядке расторгнуть настоящее Соглашение, подав письменное заявление о расторжении.

БАНК _____

КЛИЕНТ _____

Требования по обеспечению функционирования и безопасности применяемых средств криптографической защиты информации

1. Средства криптографической защиты информации (СКЗИ) используются для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации.

2. Пользователи СКЗИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящего документа. При этом пользователи должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

3. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

- соблюдением сотрудниками режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

- точным выполнением сотрудниками требований к обеспечению безопасности конфиденциальной информации;

- надежным хранением сотрудниками СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;

- своевременным выявлением сотрудниками попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;

- немедленным принятием сотрудниками мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

4. Обязанности между сотрудниками должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой документации и документов, а также за порученные участки работы.

5. Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

6. Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, в том числе сведения о криптоключках;

- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

- исключить возможность несанкционированного доступа к компьютерам, на которых используются СКЗИ;

- использовать антивирусное программное обеспечение на компьютерах, где используются СКЗИ;

- сообщать в ОАО «СИАБ» о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать в ОАО «СИАБ» СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- немедленно уведомлять ОАО «СИАБ» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, выявленных вирусных заражениях компьютеров, на которых используются СКЗИ, а также о причинах и условиях возможной утечки таких сведений.

7. Пользователям СКЗИ запрещается:

- обсуждать конфиденциальную информацию, к которой они допущены, в том числе сведения о криптоключках в присутствии посторонних;

- выполнять операции с использованием СКЗИ в присутствии посторонних;

- оставлять без присмотра СКЗИ, включенные и не заблокированные компьютеры, на которых используются СКЗИ;

- сохранять средствами операционной системы или программного обеспечения СКЗИ ключевую информацию (ключи ЭЦП и шифрования) вне штатных средств хранения (выданных носителей ключевой информации - ruToken) и пароли доступа (pin-коды) к ключевой информации и СКЗИ;

- работать с СКЗИ на компьютерах без использования антивирусного программного обеспечения.

8. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего инструктажа. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники ОАО «СИАБ».

9. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

10. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия. О необходимости вывода криптоключей из действия необходимо сообщить в ОАО «СИАБ».

11. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в ОАО «СИАБ». В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

12. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов.

13. Помещения, где установлены СКЗИ или хранятся ключевые документы к ним, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

14. Пользователям СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

15. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и ответственному сотруднику ОАО «СИАБ».

16. ОАО «СИАБ» вправе контролировать выполнение пользователями СКЗИ данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение ими условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ и настоящих Требований.

17. Если в использовании СКЗИ обнаружены недостатки, то ОАО «СИАБ» и пользователи СКЗИ обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки. При необходимости может быть составлен план мероприятий, где предусматривается решение соответствующих вопросов.

Общие рекомендации по обеспечению информационной безопасности

- Своевременно сообщайте в отдел дистанционного банковского обслуживания о всех изменениях в ваших контактных лицах и их телефонах, для обеспечения оперативной связи с ними сотрудников банка.

- Своевременно устанавливайте обновления операционной системы.

- При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

- Установите на компьютере и регулярно обновляйте антивирусное программное обеспечение. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.

- Используйте межсетевые экраны (firewall), разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.

- При работе в Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.

- Не работайте под учетной записью с административными правами, особенно с использованием доступа в интернет.

- Ежемесячно производите смену паролей доступа к системам дистанционного банковского обслуживания.

- На компьютере, используемом для работы в системе «Банк-Клиент», не должно быть учетных записей (пользователей) с пустыми паролями.

- При использовании «Интернет-Клиента» внимательно следите за правильность подключения к сайту Банка.

Если происходит переадресация или сайт выглядит не как обычно, прекратите работу и свяжитесь с технической поддержкой ДБО.

БАНК _____

КЛИЕНТ _____

**Рекомендации по обеспечению информационной безопасности
при работе в системах «Банк-Клиент», «Интернет-Клиент»**

- Персональный идентификатор «Рутокен» с закрытым ключом ЭЦП нельзя передавать третьим лицам, оставлять без присмотра, хранить в общедоступном месте.

- В случае компрометации или подозрения на компрометацию следует немедленно произвести смену паролей доступа и замену ключа ЭЦП. В качестве события, рассматриваемого как компрометация ключа, может выступать как потеря ключевого носителя (даже с последующим обнаружением), так и увольнение или смена лиц, допущенных к этим ключам.

- В случае использования системы «Интернет-Клиент» с публичных компьютеров (библиотека, Интернет-кафе) риск хищения и последующего неправомерного использования секретного ключа ЭЦП и другой аутентификационной информации (имя / пароль) значительно возрастает.

Просим Вас незамедлительно обращаться в Банк при возникновении следующих ситуаций:

- В выписке обнаружены несанкционированные Вами расходные операции.
- Утерян или похищен ключевой носитель с закрытым ключом ЭЦП или компьютер, на котором был установлена система «Банк-Клиент».
- У Вас не работает система «Банк-Клиент»/ «Интернет-Клиент» по неизвестным причинам.
- У Вас выявлено вирусное заражение или нетипичная работа (сбой в работе) Вашего компьютера.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошенничества.

БАНК _____

КЛИЕНТ _____