

УТВЕРЖДАЮ

Председатель Правления
ОАО Комбанк «Химик»

_____ Вихарев Н.П.

22 июня 2010 года

РЕГЛАМЕНТ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СИСТЕМЕ «КЛИЕНТ-БАНК» ОАО КОМБАНК «ХИМИК»

РАЗРАБОТАЛ

Старший инженер-программист отдела автоматизации и связи

_____ Сорокина Н.А.

Согласовано

Заместитель Председателя Правления

_____ Мелехин В.В

Начальник отдела автоматизации и связи

_____ Волкова И.Ю

Дзержинск
2010 г.

1. Термины и определения

1.1. В настоящем Регламенте электронного документооборота в Системе «Клиент-Банк» ОАО Комбанк «Химик» (далее – Регламент) используются следующие **Термины и Определения:**

АБС - Автоматизированная банковская система обработки расчетных документов Клиента.

Банк – Открытое акционерное общество Коммерческий банк «Химик» (ОАО Комбанк «Химик»).

Безопасность информации - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п. Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Владелец сертификата ключа ЭЦП - физическое лицо, на имя которого Банком выдан сертификат ключа ЭЦП и которое владеет закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

Выписка по счету - документ, формируемый Банком в электронном виде, содержащий сведения об остатках по счету и операциях за истекший операционный день и направленный Клиенту с использованием системы «Клиент-Банк» в порядке, предусмотренном Регламентом.

Договор об электронном обмене документами - двухсторонний договор между Банком и Клиентом об обслуживании с использованием Системы «Банк-Клиент» заключаемый в соответствии с действующей в Банке типовой формой (далее по тексту - Договор). Заключение Договора производится после подачи Клиентом Заявки.

Договор банковского обслуживания - договор банковского счета, договор банковского вклада (депозита), договор об открытии банковского счета для расчетов с использованием Корпоративных карт и выпуске Корпоративных карт, договор по обслуживанию Предприятия в рамках «зарплатного проекта с использованием банковских карт», депозитарного, брокерского или иного обслуживания, заключаемый между Банком и Клиентом.

Доставка ЭД – процесс перемещения ЭД из программной среды отправителя в программную среду получателя.

Закрытый ключ ЭЦП - уникальная последовательность символов, известная только владельцу сертификата ключа ЭЦП и предназначенная для создания в ЭД ЭЦП с использованием средств ЭЦП.

Защита информации - комплекс организационно-технических мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации.

Система Клиент-Банк с доступом через интернет (Клиент-WEB) – версия Системы, реализующая функции электронного документооборота путем доступа Клиента на web-сайт Банка. Включает в себя программное обеспечение, предназначенное для взаимной аутентификации Банка и Клиента и криптографической защиты передаваемых документов.

«Классическая» версия Системы – версия Системы, включающая в себя клиентскую часть программного обеспечения (рабочее место Клиента), устанавливаемого на аппаратных средствах Клиента; средство криптографической защиты. Данная версия системы осуществляет работу по средством коммутируемого доступа.

Клиент - юридическое лицо (не являющееся кредитной организацией)/ индивидуальный предприниматель – резидент РФ/ юридическое лицо - нерезидент РФ, который ознакомлен и согласен с условиями настоящего Регламента и заключил с Банком договор об обслуживании с использованием системы «Клиент-Банк».

Ключевой носитель - физический носитель, предназначенный для размещения на нем ключевой информации.

Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают должную безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- утрата (в том числе хищение) ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение или перевод на другой участок работы сотрудников, имевших доступ к ключевой информации;
- передача ключевой информации по линии связи в открытом виде;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- несанкционированное копирование ключевых носителей.

Открытый ключ ЭЦП - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная Сторонам и предназначенная для подтверждения подлинности ЭЦП в ЭД с использованием СЭЦП.

Отправитель ЭД - физическое лицо, которое само непосредственно направляет или юридическое лицо, от имени которого направляется электронный документ, за исключением лиц, действующих в качестве информационных

посредников в отношении этого документа.

Положительный результат проверки ЭЦП - подтверждение соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа ЭЦП принадлежности ЭЦП в ЭД владельцу сертификата ключа ЭЦП и отсутствия искажений в подписанном данной ЭЦП ЭД, а также соответствия полномочий владельца сертификата ключа ЭЦП статусу ЭД.

Получатель ЭД - физическое или юридическое лицо, которому электронный документ отправлен за исключением лиц, действующих в качестве информационных посредников в отношении этого документа.

Сертификат ключа ЭЦП - документ на бумажном носителе или ЭД с ЭЦП Удостоверяющего центра Банка, который включают в себя открытый ключ ЭЦП и который выдается Банком Клиенту для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа ЭЦП.

Система «Клиент-Банк» (далее - Система) - корпоративная система электронного документооборота, включающая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи электронных документов и средств электронной цифровой подписи, позволяющая Сторонам обмениваться электронными документами.

Система электронного документооборота (СЭД) - организационно-техническая система, представляющая собой совокупность программного, информационного, аппаратного и организационного обеспечения Банка и Клиента, позволяющая реализовать электронный документооборот между Банком и Клиентом.

Средства криптографической защиты информации (СКЗИ) - совокупность программно-технических средств, обеспечивающих применение ЭЦП и шифрования при организации ЭДО. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Средства ЭЦП (СЭЦП) - программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание ЭЦП в ЭД с использованием закрытого ключа ЭЦП, подтверждение подлинности ЭЦП с использованием открытого ключа ЭЦП, создание закрытых и открытых ключей ЭЦП.

Формат ЭД - структура содержательной части электронного сообщения, на основе которого сформирован ЭД.

Шифрование - криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Электронный документ (ЭД) - расчетный или иной документ одной из Сторон на бумажном носителе, подписанный должностными лицами, обладающими соответствующими правами, и заверенный печатью (в предусмотренных случаях), составленный с учетом требований действующего законодательства Российской Федерации, нормативных документов Банка России, договоров, заключенных между Сторонами, преобразованный в электронно-цифровой вид с учетом требований настоящего Регламента к форме таких документов, заверенный ЭЦП (подписями), и переданный между Сторонами с использованием Системы.

Электронный документооборот (ЭДО) - обмен ЭД в соответствии с настоящим Регламентом.

Электронное сообщение (ЭС) - логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия, закодированная способом, позволяющим обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

Электронная цифровая подпись (ЭЦП) - реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа ЭЦП, а также установить отсутствие искажения информации в ЭД.

2. Общие положения

- 2.1. Настоящий Регламент устанавливает общие принципы осуществления ЭДО между Банком и Клиентом (при совместном упоминании – Стороны).
- 2.2. Настоящий Регламент является типовыми для всех Клиентов заключившим Договор об электронном обмене документами. Заключение Договора осуществляется после подачи Заявки на подключение к Системе «Клиент-Банк» по установленной форме (Приложение №2) (далее – Заявка).
- 2.3. Стороны признают используемые в Системе Средства ЭЦП достаточными для защиты от несанкционированного доступа к информации, передаваемой с использованием Системы.
- 2.4. Стороны признают используемые в Системе Средства ЭЦП достаточными для подтверждения подлинности ЭЦП, идентификации Владельцев сертификатов ключей ЭЦП и отсутствия искажений в ЭД.
- 2.5. Подключение Клиента к Системе осуществляется на условиях, предусмотренных настоящим Регламентом. Клиент указывает вариант подключения к Системе в Заявке. Требования к аппаратным средствам Клиента определяются в Приложении №4 к Регламенту.
- 2.6. Клиент считается принятым на обслуживание с использованием Системы только после подписания всего пакета документов директором или лицом имеющим право подписания документов по Клиент-Банку (в частности Сертификата открытого ключа).
- 2.7. Положения настоящего Регламента применяются, если иное не предусмотрено законодательными или иными правовыми актами РФ, включая нормативные акты Банка России. Для Клиентов, заключивших с Банком Договор, положения настоящего Регламента действуют в части не противоречащей условиям Договора.
- 2.8. ЭДО в СЭД регулируется действующим законодательством РФ, нормативными актами Банка России,

настоящим Регламентом.

- 2.9. Клиент допускается к осуществлению документооборота в СЭД после выполнения им совокупности следующих действий:
- Ознакомление и согласие с условиями настоящего Регламента путем передачи в Банк Заявки и подписи в Журнале получения ключевых дискет;
 - установки необходимых аппаратных средств, клиентского программного и информационного обеспечения в соответствии с Приложением №4 к настоящему Регламенту;
 - установки программного обеспечения Системы и получения ключевой дискеты с ключами Банка, необходимых паролей, идентификаторов и другой информации для доступа к СЭД;
 - генерации ключей ЭЦП Клиентом (в количестве, определенном Клиентом) и изготовление Сертификата ключа ЭЦП Клиента;
 - передачи Открытого ключа ЭЦП для регистрации в Банке в электронном виде и подписанным Владелцем Сертификатом ЭЦП на бумажном носителе;
 - Регистрации Банком открытых ключей Клиента и принятия оформленных в соответствии с требованиями Приложения №3 к Регламенту Сертификатов ключей ЭЦП на бумажном носителе;
 - Подписание Владелцем данных Сертификатов ключей ЭЦП на бумажном носителе и передача 1 экземпляра в Банк.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Права и обязанности Сторон.

- 3.1.1. Стороны при обмене ЭД с использованием Системы обязуются руководствоваться правилами и требованиями, установленными действующим законодательством Российской Федерации, нормативными актами Банка России, Договорами банковского обслуживания, настоящим Регламентом.
- 3.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных действующим законодательством Российской Федерации) способы защиты информации, реализованные в Системе, а также любые конфиденциальные данные, ставшие известными Сторонам в процессе исполнения Договора.
- 3.1.3. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях компрометации закрытых ключей ЭЦП, а также повреждениях программно-технических средств обработки, хранения, передачи ЭД и Средств ЭЦП.

3.2. Права и обязанности Клиента.

Клиент обязан:

- 3.2.1. Обеспечить наличие и функционирование в течение всего срока действия Договора программно-технических средств в комплектации, соответствующей требованиям, изложенным в Приложении №4 к Регламенту.
- 3.2.2. Строго соблюдать настоящий Регламент.
- 3.2.3. При изменении Владелец сертификатов ключей ЭЦП произвести смену ключей ЭЦП в соответствии с Регламентом.
- 3.2.4. Оформлять ЭД только от своего имени в соответствии с собственными реквизитами, установленными в Системе на основании документов, предоставленных Клиентом в Банк, и требованиями действующего законодательства Российской Федерации, нормативных актов Банка России, Договоров банковского обслуживания, настоящего Регламента.
- 3.2.5. Работать с Системой только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере.
- 3.2.6. Производить оплату услуг Банка, оказанных в соответствии с Договором в размере и сроки, предусмотренные тарифами Банка (далее – Тарифы), если иное не установлено соглашениями Сторон, либо Договорами банковского обслуживания.
- 3.2.7. Выполнить всю совокупность действий, необходимых для получения допуска к осуществлению ЭДО и предусмотренных в пункте 2.9 настоящего Регламента.
- 3.2.8. Незамедлительно уведомлять Банк о компрометации зарегистрированных ключей, прекращении полномочий уполномоченных лиц Клиента, а также соблюдать организационно-технические требования по обеспечению безопасности информации, установленные в настоящем Регламенте.
- 3.2.9. Использовать полученные у Банка программно-технические средства и ключи ЭЦП только для целей осуществления ЭДО с Банком, не передавать без письменного согласия Банка данные средства третьим лицам, вернуть их по первому требованию, включая резервные копии программных средств, не использовать указанные средства в каких либо других, в том числе открытых системах.
- 3.2.10. Не производить модификацию программных средств, не совершать относительно указанных программно-технических средств других действий, нарушающих действующее законодательство Российской Федерации.
- 3.2.11. Не совершать действий, способных привести к нарушению целостности СЭД, а также незамедлительно сообщать Банку о ставших известными Клиенту попытках третьих лиц совершить действия, способные привести к нарушению целостности СЭД.
- 3.2.12. Выполнять все обновления, проводимые Банком в Системе. В случае неисполнения Клиентом этих обязанностей Банк осуществляет действия, указанные в п. 3.3.27 настоящего Регламента.

- 3.2.13. Проводить смену ключей ЭЦП Клиента в случае, если Банк уведомит Клиента об необходимости этого (но не чаще 1 раза в год).
- 3.2.14. Информировать Банк об изменении своих реквизитов путем предоставления в Банк соответствующих документов в пятидневный срок. Не передавать в Банк ЭД до момента обновления собственных реквизитов в Системе.

Клиент имеет право

- 3.2.15. Направить в Банк Заявку на выезд специалиста Банка (Приложение № 5 к Регламенту) для установки, переустановки или восстановления работоспособности Системы, с последующей оплатой, согласно Тарифам.
- 3.2.16. Получать необходимую информацию по использованию Системы.
- 3.2.17. Самостоятельно осуществить настройку программы в соответствии с технологической инструкцией системы, импорта-экспорта ЭД в собственную бухгалтерскую программу согласно инструкции, передаваемой Клиенту.
- 3.2.18. Клиент имеет право блокировать открытый ключ ЭЦП Клиента, т.е. приостановить свою работу в системе «Клиент-Банк», направив письменное уведомление по форме Приложения №2 к Договору на обслуживание по системе Клиент-Банк. Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.
- 3.2.19. Требовать замену Ключа ЭЦП в случае потери доверия к нему;
- 3.2.20. Досрочно прекращать действие открытых ключей ЭЦП Клиента (вместе с соответствующим закрытым ключом ЭЦП Клиента), направив письменное уведомление по форме Приложения №2 к Договору на обслуживание по системе Клиент-Банк. Для продолжения дальнейшей работы в системе «Клиент-Банк» уполномоченный представитель Клиента должен сгенерировать новую пару ключей ЭЦП Клиента и выполнить действия описанные в Приложении 1 к данному Регламенту.
- 3.2.21. Требовать от Банка предоставления на бумажном носителе копий полученных Банком электронных документов с проставлением на них соответствующих отметок Банка (об исполнении и др.). Указанные документы предоставляются уполномоченному лицу Клиента при его явке в Банк.

3.3. Права и обязанности Банка

Банк обязан

- 3.3.1. В сроки согласованные с Клиентом после регистрации Заявки в Банке предоставить Клиенту программное обеспечение Системы, ключевой носитель с ключами Банка, а также инструкцию по работе и подключению к системе. В случае, если подключение к Системе осуществляется по просьбе Клиента специалистами Банка, выезд специалиста Банка осуществляется в сроки, согласованные с Клиентом.
- 3.3.2. Организовывать работу с криптографическими ключами Клиента в объеме и в соответствии с порядком, определяемым настоящим Регламентом
- 3.3.3. Предоставить Клиенту инструкции по работе с Системой в электронном виде.
- 3.3.4. Исполнять принятые от Клиента электронные документы, подписанные корректной ЭЦП Клиента, в соответствии с условиями Договора, Договора банковского счета и действующим законодательством.
- 3.3.5. При получении от Клиента факса или Заявки по форме Приложения № 2 к Договору временно блокировать работу Клиента в системе «Клиент-Банк» или же снять блокировку.
- 3.3.6. Банк обязан обеспечить строго контролируемый и ограниченный доступ к программно-аппаратным средствам, содержащим контрольные архивы системы «Клиент-Банк».
- 3.3.7. Банк обязан хранить в секрете и не передавать третьим лицам закрытый ключ ЭЦП Банка и открытый ключ ЭЦП Клиента, используемые при работе в системе «Клиент-Банк». Риск неблагоприятных последствий, связанных с использованием закрытого Ключа ЭЦП Банка третьими лицами, несет Банк
- 3.3.8. В обычном порядке осуществлять операции на основании ЭД Клиента, поступивших с использованием Системы, соответствующих требованиям Регламента и принятых для исполнения Банком. Исполнение документов проводится в сроки, определенные Договорами банковского обслуживания.
- 3.3.9. В течение 2 (Двух) рабочих дней с даты получения от Клиента Заявки на смену ключей ЭЦП, провести мероприятия, определенные настоящим Регламентом.
- 3.3.10. В течение 7 (Семи) рабочих дней с даты получения письменного запроса/Заявки Клиента направить специалиста для переустановки или восстановления работоспособности Системы.
- 3.3.11. В кратчайшие сроки устранить неисправности Системы, возникшие по вине Банка.
- 3.3.12. В случае не исполнения Клиентом обязанностей, изложенных в п.3.2 настоящего Регламента, приостановить прием и исполнение ЭД, подписанных ЭЦП, срок действия которых истек, до момента генерации и сертификации новых ключей в соответствии с Регламентом.
- 3.3.13. Исполнение документов осуществлять в сроки, установленные Договором банковского счета.
- 3.3.14. При получении электронного документа Банк производит проверку:
- корректности ЭЦП Клиента открытым ключом ЭЦП Клиента;
 - правильности заполнения реквизитов электронного документа
- 3.3.15. При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный электронный документ системой «Клиент-Банк» не принимается и автоматически возвращается Клиенту, поручение, содержащееся в нем, Банком не исполняется. Иного информирования Клиента о неисполнении

переданного им по системе «Клиент-Банк» электронного документа Банком не осуществляется. Свидетельством того, что документ исполнен, является содержащая ЭЦП Банка электронная квитанция о проведении его банком. Отсутствие у Клиента указанной электронной квитанции означает, что электронный документ Банком проведен не был.

3.3.16. Банк обязан осуществлять прием документов, передаваемых по электронной системе «Клиент-Банк», с понедельника по четверг с 9:00 до 16:00 часов, в пятницу с 9:00 до 15:00 московского времени. Использование системы «Клиент-Банк» не лишает Клиента права предоставлять Банку расчетные и иные документы на бумажном носителе.

3.3.17. Соблюдать режим конфиденциальности информации, касающейся паролей, идентификаторов, а также криптографических ключей, которая становится доступной Банку в связи с выполнением им своих функций в соответствии с настоящим Регламентом.

Банк имеет право

3.3.18. Не подключать Клиента к Системе в случае несоответствия имеющихся у него аппаратных средств требованиям Приложения №4 к Регламенту до момента приведения их в соответствие.

3.3.19. Не принимать к исполнению ЭД, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных актов Банка России, Договоров банковского обслуживания и Регламента.

3.3.20. Оформлять бумажные копии принятых ЭД Клиента и заверять их в соответствии с внутренними нормативными документами Банка.

3.3.21. Проводить плановую смену ключей ЭЦП Банка и Клиента (не чаще одного раза в год), о чем извещает Клиента по Системе за две недели до даты начала смены ключей.

3.3.22. Производить обновления версий Системы.

3.3.23. В случае не оплаты Клиентом услуг Банка в соответствии с п. 4.3. настоящего Регламента, а также, если остаток денежных средств на счете Клиента, имеющего счет в Банке, не позволяет Банку в срок и в размере, определенными настоящим Регламентом и действующими Тарифами, произвести списание платы за услуги Банка, приостановить обслуживание Клиента с использованием Системы до момента полного погашения задолженности Клиентом.

3.3.24. Вносить изменения в Регламент в одностороннем порядке.

3.3.25. В случае неисполнения Клиентом обязанностей, предусмотренных Регламентом, заблокировать проведение операции Клиента в Системе.

4. ФИНАНСОВЫЕ ВЗАИМООТНОШЕНИЯ.

4.1. Порядок оплаты производится в соответствии с Дополнительным соглашением к Договору об электронном обмене, стоимость услуг, предоставляемых Клиенту в соответствии с Договором, устанавливается действующими Тарифами Банка.

4.2. Тарифы доводятся до сведения Клиента при подаче Клиентом Заявки в Банк, а также по первому требованию Клиента.

5. ОФОРМЛЕНИЕ ЭД.

5.1. Требования, предъявляемые к ЭД.

5.1.1. ЭД, сформированный в СЭД, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия при его соответствии настоящим Регламентом и Договорам банковского обслуживания. ЭД должен быть сформирован в формате, предусмотренном разработчиками системы Клиент-Банк или Договорах банковского обслуживания и заверен ЭЦП, имеющей сертифицированный Банком ключ ЭЦП. ЭД без ЭЦП или имеющий формат, не отвечающий установленным правилам, в качестве ЭД в соответствии с настоящим Регламентом не рассматривается.

5.2. Использование ЭЦП и шифрования в ЭДО.

5.2.1. Используемые при информационном взаимодействии Сторон ЭД, заверенные ЭЦП имеют равную юридическую силу с документами на бумажном носителе, подписанными уполномоченными представителями и скрепленными печатями Сторон (независимо от того, существуют такие документы на бумажных носителях или нет).

5.2.2. Стороны признают, что используемые ими СКЗИ, которые реализуют функции ЭЦП и шифрования, достаточны для обеспечения конфиденциальности содержания ЭД Сторон, а также подтверждения того, что ЭД:

- исходит от Клиента (подтверждение авторства);
- не претерпел изменений при обмене ЭД в ходе информационного взаимодействия (подтверждение целостности).

5.2.3. ЭД может быть заверен только той ЭЦП, сертификат открытого ключа которой зарегистрирован в СЭД в порядке, установленном настоящими Правилами.

5.2.4. Замена ключей ЭЦП не влияет на юридическую силу ЭД, если он был заверен действующим на момент подписания ключом ЭЦП в соответствии с настоящим Регламентом.

5.2.5. При получении зашифрованного ЭД, он расшифровывается в соответствии с применяемой технологией, затем проверяется ЭЦП ее владельца, сформировавшего ЭД.

5.2.6. Предусмотренные для данного ЭД правовые последствия могут наступить, только если получен положительный результат проверки ЭЦП.

6. ОРГАНИЗАЦИЯ ЭДО.

6.1. ЭДО включает:

- 1) формирование ЭД;
- 2) отправку и доставку ЭД;
- 3) проверку ЭД;
- 4) подтверждение получения ЭД;
- 5) отзыв ЭД;
- 6) хранение ЭД (ведение архивов ЭД);
- 7) создание дополнительных экземпляров ЭД;
- 8) создание бумажных копий ЭД.

6.2. Статус ЭД

6.2.1. Процесс формирования, заверения ЭЦП, передачи, проверки, получения и исполнения Сторонами ЭД в Системе сопровождается изменением статуса ЭД.

6.2.2. Таблица статусов ЭД в Системе с комментариями.

| Статус ЭД | Комментарий |
|---|--|
| новый | новый ЭД |
| подписан | ЭД подписанный ЭЦП |
| На обработке | Отправлен в банк, ожидается решение по документу; |
| Выгружен для ВП или Выгружен для ОД | Ставится после получения документа программой внешней проверки или программой опередня банка, подтверждает доставку документа непосредственно в банковские системы |
| Принят/Не принят/ Отложен | Отражает решение по документу |

6.3. Формирование ЭД

6.3.1. Формирование ЭД осуществляется в следующем порядке:

- формирование электронного сообщения в формате, установленном для данного ЭД;
- заверение сформированного электронного сообщения ЭЦП.

6.4. Отправка и доставка электронного документа

6.4.1. Особенности отправки, доставки и получения ЭД зависят от типа системы.

6.5. Проверка подлинности доставленного ЭД

6.5.1. Проверка ЭД включает:

- проверку подлинности всех ЭЦП ЭД;
- проверку ЭД на соответствие установленному для него формату.

6.5.2. В случае положительного результата проверки ЭД, данный ЭД принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный ЭД считается не полученным, о чем получатель должен послать уведомление отправителю.

6.6. Подтверждение получения ЭД

6.6.1. Подтверждение о получении ЭД производится путем автоматической отправки электронных сообщений от Получателя ЭД Отправителю ЭД, содержащего информацию об изменении статуса ЭД.

6.6.2. ЭД считается полученным противоположной Стороной и порождает соответствующие обязательства по Договорам банковского обслуживания только в случае, если он имеет статус «Проведен банком». Все другие статусы ЭД в Системе имеют исключительно информационный характер.

6.6.3. При отсутствии изменения статуса отправленного ЭД отправляющая Сторона должна уведомить принимающую Сторону о данном факте в день отправки документа любым доступным способом. Принимающая Сторона не несет ответственности за неисполнение неполученных или не принятых ЭД.

6.7. Получение Клиентом выписки по счету.

6.8. Банк формирует для Клиента выписку по запросу, для обновления остатка и просмотра актуальных движений по счету Клиент должен запрашивать выписки за каждый рабочий день (или за каждый период).

6.9. Отзыв ЭД

6.9.1. Клиент вправе отозвать отправленный ЭД только до начала его исполнения получателем.

6.9.2. Отзыв ЭД Клиентом производится путем создания ЭД «Запрос на отзыв документа», в котором указываются реквизиты отзываемого ЭД и причину его отзыва. Данный «Запрос на отзыв документа» подписывается ЭЦП Клиента и отсылается в Банк, после чего ЭД будет отозван в автоматическом режиме (в том случае, если на момент получения Запроса на отзыв документа расчетный документ не принят Банком к исполнению). В случае системы с доступом через интернет Клиент обязан уведомить о направлении Запроса сотрудников

отдела автоматизации.

- 6.9.3. В случае, когда отозвать ЭД в автоматическом режиме не представляется возможным необходимо связаться с уполномоченными сотрудниками Банка, выяснить текущий этап обработки ЭД и, при возможности отзыва, уведомить уполномоченного сотрудника Банка о намерении его отозвать. В течение 15 минут после уведомления уполномоченного сотрудника Банка подготовить и отправить через Систему в Банк ЭД произвольного формата с просьбой отозвать ЭД с точным указанием его даты, номера, суммы и реквизитов получателя.
- 6.9.4. Отзыв Клиентом ЭД по валютному контролю возможен только после согласования с уполномоченным сотрудником валютного контроля Банка по телефону до окончания рабочего дня, в течение которого он был принят Банком.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

- 10.1. За неисполнение или ненадлежащее исполнение обязательств по Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.
- 10.2. Клиент несет ответственность за передачу соответствующих ключевых носителей и их использование лицами, не являющимися Владельцами сертификатов ключей ЭЦП.
- 10.3. Банк несет ответственность за несоблюдение сроков проведения операций на основании надлежащим образом оформленных и своевременно переданных с использованием Системы ЭД Клиента в соответствии с действующим законодательством Российской Федерации и Договорами банковского обслуживания.

ПОРЯДОК ИСПОЛЬЗОВАНИЯ СКЗИ В СИСТЕМЕ «КЛИЕНТ-БАНК»

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1.** В Системе электронного документооборота, осуществляемого в соответствии с Регламентом, используются сертифицированные средства криптографической защиты информации СКЗИ "Бикрипт-Клиент" предназначен для защиты интернет-приложения "Клиент-WEB" фирмы ЗАО "РФК", использующего в работе протокол HTTP. Защита подразумевает под собой шифрование передаваемой информации согласно ГОСТу 28147-89 и наложение электронной цифровой подписи (ЭЦП) согласно ГОСТу Р 34.10-94. При создании программы было использовано криптографическое программное обеспечение, разработанное фирмой "ИнфоКрипт"..
- 1.2. После заключения Договора Банк предоставляет Клиенту для использования исключительно в целях осуществления ЭДО в соответствии с Регламентом программные компоненты СКЗИ.
- 1.3. В процессе эксплуатации СКЗИ Клиент обязуется:
- обеспечить сохранность ПО СКЗИ;
 - не передавать ПО СКЗИ третьим лицам;
 - не проводить декомпиляции или модификации модулей ПО СКЗИ;
 - по требованию Банка предоставлять возможность уполномоченным им лицам проводить проверку сохранности, обновление или уничтожение СКЗИ, включая их резервные копии;
 - обеспечить всеми доступными средствами соблюдение уполномоченными лицами Клиента перечисленных обязательств, в том числе и после увольнения уполномоченного лица из организации Клиента.
- 1.4. При обеспечении криптографической защиты информации в системе ЭДО используются СКЗИ с открытым распределением ключей. При этом каждый Владелец сертификата ключа ЭЦП Клиента имеет свои закрытые ключи ЭЦП, а также соответствующие им открытые ключи ЭЦП. Открытые ключи ЭЦП передаются Клиентом в Банк.
- 1.5. Документом, подтверждающим принадлежность открытого ключа ЭЦП уполномоченному лицу Клиента, является сертификат ключа ЭЦП. Сертификат ключа ЭЦП Клиента подписывается ответственным должностным лицом Банка и заверяется печатью Банка (Приложение №3 к настоящему Регламенту).
- 1.6. Для шифрования ЭД программным обеспечением вырабатывается ключ шифрования с использованием собственного закрытого ключа ЭЦП отправителя ЭД и открытого ключа ЭЦП получателя ЭД, для электронной цифровой подписи ЭД необходим только собственный закрытый ключ ЭЦП. Для расшифрования ЭД получателем ЭД используется открытый ключ ЭЦП отправителя ЭД и собственный закрытый ключ ЭЦП, для проверки ЭЦП электронного документа необходим только открытый ключ владельца ЭЦП, подписавшего ЭД. Реализованные в СКЗИ алгоритмы шифрования и электронной цифровой подписи гарантируют невозможность восстановления закрытых ключей ЭЦП и шифрования отправителя ЭД по его открытым ключам.
- 1.7. Открытый ключ ЭЦП Клиента считается зарегистрированным в Банке с даты, проставленной Банком на распечатке сертификата ключа ЭЦП, оформленной в соответствии с Приложением №3 к настоящему Регламенту.
- 1.8. Открытый ключ ЭЦП Клиента считается действующим в момент проверки ЭЦП при одновременном выполнении следующих условий:
- сертификат ключа ЭЦП зарегистрирован в Банке;
 - период действия сертификата ключа ЭЦП не истек;
 - действие сертификата ключа ЭЦП не отменено.
- 1.9. Для отмены действия открытого ключа ЭЦП Клиент передает в Банк письменное уведомление об отмене действия сертификата этого открытого ключа ЭЦП.
- 1.10. Открытый ключ ЭЦП Клиента считается отмененным с момента регистрации в Банке уведомления об отмене действия сертификата открытого ключа ЭЦП.
- 1.11. Открытый ключ ЭЦП Клиента может быть временно заблокирован Банком по собственной инициативе в случае возникновения подозрений в его компрометации.
- 1.12. Генерация ключей производится лично Владелец сертификата ключа ЭЦП Клиента на автоматизированном рабочем месте Клиента. Клиент обязан обеспечить конфиденциальность при изготовлении закрытых ключей ЭЦП.

2. ПОРЯДОК ПЕРВИЧНОЙ ВЫДАЧИ ПРОГРАММНЫХ КОМПОНЕНТОВ СКЗИ

- 2.1. Клиент определяет количество ЭЦП, необходимое для заверения каждого своего ЭД в заявке, оформляемой по форме Приложения №2 к настоящему Регламенту.
- 2.2. Банк в соответствии с заявкой передает Клиенту ключ шифрования, необходимый для формирования его ЭЦП вместе с ПО СКЗИ.
- 2.3. Инсталляция ПО СКЗИ производится Клиентом самостоятельно в соответствии с передаваемой ему документацией.
- 2.4. Генерация и регистрация криптографических ключей Клиента осуществляется в следующей последовательности:
 - 2.4.1. Клиент:
 - самостоятельно с помощью программного модуля генерации ключей ЭЦП ПО СКЗИ по переданной Инструкции создает на ключевом носителе закрытый и открытый ключи ЭЦП, и формирует сертификат открытого ключа ЭЦП на бумажном носителе в 2-х экземплярах, при этом Клиент контролирует правильность заполнения полей сертификата ключа ЭЦП (организация, ФИО директора, уполномоченного ставить ЭЦП под ЭД);
 - Заверяет оба экземпляра распечатки сертификата ключа ЭЦП подписями Владельца сертификата ключа ЭЦП и скрепляет печатью;
 - Используя переданную Инструкцию отправляет открытый ключ в электронном виде на дискету или по электронной почте передает в Банк на регистрацию.
 - Обязательно передает в Банк распечатаны и заверенный подписью и печатью директора сертификата ключа ЭЦП в 2-х экземплярах.
 - 2.4.2. Банк:
 - принимает оформленные сертификаты ключа ЭЦП у Клиента на бумажном носителе;
 - проверяет содержание распечаток сертификата ключа ЭЦП на соответствие выпущенному Банком сертификату ключа ЭЦП, а также проверяет правильность заполнения полей сертификата ключа ЭЦП (реквизиты Клиента, Ф.И.О. и паспортные данные владельца сертификата ключа ЭЦП), и соответствие подписей владельца сертификата ключа ЭЦП, указанным в карточке с образцами подписей и оттиска печати;
 - в случае положительного результата проверки заверяет оба экземпляра распечатки сертификата ключа ЭЦП Клиента подписью и скрепляет печатью.
 - передает один экземпляр распечатки сертификата ключа ЭЦП (на бумажном носителе) Клиенту.
 - Регистрирует открытый ключ Клиента, полученный в электронном виде
 - 2.4.3. Клиент:
 - получает сертификат ключа ЭЦП;
 - начинает работу по системе «Клиент-Банк»

3. ПОРЯДОК ПРОВЕДЕНИЯ СМЕНЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

- 3.1. Внеплановая смена криптографических ключей в СЭД производится по желанию Клиента, или при компрометации ключей, или смене владельца сертификата ключа ЭЦП.
- 3.2. К моменту завершения срока действия ключей Клиент должен произвести генерацию и сертификацию новых ключей. Для этого он должен выполнить все пункты раздела 2 настоящего Приложения, за исключением получения комплекта ПО.
- 3.3. При смене ключей дата и время ввода новых ключей определяется Банком и согласуется с Клиентом.
- 3.4. При вводе в действие новых ключей старые сертификаты ключей ЭЦП удаляются.
- 3.5. Закрытые ключи ЭЦП после вывода из действия должны быть уничтожены.
- 3.6. В случае несоблюдения Клиентом порядка, предусмотренного в данном разделе, ответственность за возможные убытки, связанные с этим, несет Клиент.

4. ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ

- 4.1. В организации должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, обрабатываемой с помощью СКЗИ, а также ключевой информации.
 - 5.1. Требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ:
 - 5.1.1. К работе с СКЗИ допускаются решением руководства организации только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.
 - 5.1.2. Руководитель организации или лицо, им уполномоченное, должно иметь представление о возможных угрозах при обработке, передаче и хранении информации, методах и средствах защиты информации.
 - 5.2. Участник СЭД имеет право самостоятельно устанавливать на клиентском рабочем месте сертифицированные, в соответствии с действующим законодательством РФ, дополнительные программные (программно-технические) средства защиты от несанкционированного доступа.

Заявка на подключение к системе «Клиент-Банк»

_____, в лице _____,
(наименование Клиента) (должность и Ф.И.О.)

_____, действующего на основании _____
(наименование документа)

порукает ОАО Комбанк «Химик» (далее – Банк) произвести подключение к системе «Клиент-Банк» (выполнить смену ключей ЭЦП) для совершения операций по счету _____, с учетом следующих параметров:

1. Реквизиты Клиента:

ИНН _____

КПП _____

ОКПО _____

Установка системы «Клиент-Банк» будет произведена по адресу:

г. _____, ул. _____, д. __, к. __, тел. (_____) _____

2. Подключение:

Первоначальное

Восстановление работоспособности Системы

Переустановка

Смена ЭЦП

3. Тип Системы:

«Интернет»

«Классическая»

4. Генерация ключа на:

Дискету

Flash-накопитель (флэшка)

5. Передача программных средств Системы (в случае передачи через Представителя Клиента необходимо предоставить доверенность на получение ключевой дискеты)

ФИО Представителя клиента, Должность

Настоящим подтверждаем, что с Регламентом электронного документооборота в системе «Клиент-Банк» ОАО Комбанк «Химик», Тарифами ОАО Комбанк «Химик» на подключение и обслуживание системы «Клиент-Банк» ознакомлен, согласен и обязуемся неукоснительно их выполнять. Оплату гарантируем.

Количество ЭЦП, необходимое для заверения электронных документов _____

| | | |
|---|----------------|--|
| 1 | Директор | |
| 2 | Зам. директора | |
| 3 | Гл. бухгалтер | |
| | | |

Директор / _____ / _____ /
(подпись) (Ф.И.О.)

М.П.

| ОТМЕТКИ БАНКА О ПРИНЯТИИ ЗАЯВКИ | |
|---------------------------------|--|
| _____ (подпись) | Контактное лицо Клиента: Ф.И.О. _____ Тел.: (_____) _____ |
| Принято " " 201 г. | |

Требования к программно-техническим средствам Клиента.

Требования к программно-техническим средствам, необходимым Клиенту для подключения к Системе «Клиент-Банк»:

Для «Классической» версии Системы:

1. Персональный компьютер IBM PC/AT или 100% совместимый с ним следующей конфигурации:
 - Цветной дисплей с адаптером XGA;
 - Накопитель на жестких магнитных дисках (НЖМД) любого типа;
 - Накопитель на гибких магнитных дисках (НГМД) 3,5";
 - Клавиатура со 101 клавишей, русско-латинская;
 - Процессор не ниже PIII-600 (рекомендуется PIV-1.7 или лучший);
 - Не менее 128 Мбайт оперативной памяти и не менее 40 Гбайт на НЖМД;
 - Операционная система MS Windows 2000/XP;
2. Модем для работы по коммутируемому каналу со скоростью передачи данных не ниже 36600 bps с протоколом v.34 (иногда встречаются конфликты с модемом Zuxel Omni 56K);
3. Телефонная коммутируемая линия связи (меры по обеспечению нормального функционирования модема в случае подключения через АВУ, блокиратор, УТК и т.п. устройства, или при наличии спаренных телефонных аппаратов, должны быть предприняты Клиентом до подключения к системе “Клиент-Банк”);

Для «Интернет» версии Системы:

- Персональный компьютер IBM PC/AT или 100% совместимый с ним следующей конфигурации:
- Процессор не ниже PIII-350;
- Не менее 128 Мбайт оперативной памяти;
- Не менее 50Мв свободного места на НЖМД;
- Доступ в интернет;
- Устройство для доступа к ключевому носителю 3,5" (если Клиент планирует использовать в качестве ключевого носителя дискету);
- Накопитель на гибких магнитных дисках (НГМД) 3,5" (если Клиент планирует использовать в качестве ключевого носителя дискету);
- Flash-накопитель («флэшка») минимального объема от 128 МБ, предназначенный для хранения ключей (если Клиент планирует использовать в качестве ключевого носителя флэшку)
- Цветной дисплей с адаптером XGA;
- Для возможности печати документов необходимо наличие графического принтера;
- Устройство для чтения компакт-диска (CD-ROM) или разъем USB для установки системы.
- Операционная система Microsoft Windows: 2000 Professional/ 2000 Server/ XP.
- **Браузер Microsoft Internet Explorer версии не ниже 6.0**

ЗАЯВКА
на выезд специалиста Банка

г. Дзержинск

« ____ » _____ 20__ г.

(наименование клиента)

(номер счета)

просит обеспечить выезд специалиста Банка для :

Первоначальной установки и настройки системы «Клиент-Банк»

Восстановления работоспособности системы «Клиент-Банк»

Обучения Клиента работе в системе «Клиент-Банк»

(цель выезда специалиста Банка)

по адресу Клиента г. _____, ул. _____, Д. _____,
офис. _____, тел. (_____) _____

Контактное лицо _____
(ФИО, должность)

Контактный телефон _____

Настоящим подтверждаем, что с Тарифами ОАО Комбанк «Химик» на оказание услуги выезда специалиста для установки, настройки, обучения персонала Клиента по работе с системой «Клиент-Банк» ознакомлены. Оплату гарантируем

Директор / _____ / _____ /
(подпись) (Ф.И.О.)
М.П.

Отметки банка

Выезд специалиста _____ осуществить
(Ф.И.О. специалиста)

« ____ » _____ 20__ г.

Согласовано

_____ И.Ю. Волкова
(начальник Отдела автоматизации: подпись, Ф.И.О.)