

Утверждено

Правлением ПАО Комбанк «Химик»

Протокол заседания №48
от «15» августа 2024г.

**РЕГЛАМЕНТ
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
В СИСТЕМЕ «iBank» ПАО КОМБАНК «ХИМИК»**

Дзержинск
2024 г.

Термины и определения

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

АБС - Автоматизированная банковская система обработки расчетных документов Клиента.

Банк – Публичное акционерное общество Коммерческий банк «Химик» (ПАО 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 ЭП - физическое лицо, на имя которого Банком выдан сертификат ключа ЭП и которое владеет закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную 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 на обслуживание клиентов в Системе «iBank» (Договор) - Договор на обслуживание клиентов в Системе «iBank», включая Приложения к нему и Регламент электронного документооборота в системе «iBank» ПАО Комбанк «Химик», определен как стандартный утвержденный формуляр и, в соответствии с положениями ст. 428 Гражданского кодекса РФ, является договором присоединения.

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

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

Клиент - юридическое лицо (не являющееся кредитной организацией)/ индивидуальный предприниматель / **физическое лицо, занимающееся** частной практикой в порядке, установленном действующим законодательством Российской Федерации, ознакомленное и согласное с условиями настоящего Регламента и заключившее с Банком договор об обслуживании с использованием системы «iBank».

Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

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;
- случаи, когда нельзя достоверно установить, что произошло с техническими, программными, коммуникационными ресурсами, используемыми для доступа в ДБО и/или ключевому носителю (в том числе, выход из строя, когда доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц).

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

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 ЭП - подтверждение соответствующим сертифицированным средством ЭП с использованием сертификата ключа ЭП принадлежности ЭП в ЭД владельцу сертификата ключа ЭП и отсутствия искажений в подписанном данной ЭП ЭД, а также соответствия полномочий владельца сертификата ключа ЭП 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 проверки ЭП - документ на бумажном носителе с указанным в шестнадцатеричном виде Ключом проверки ЭП Уполномоченного лица Клиента (распечатывается из системы ДБО).

Сертификат действует на определенный момент времени (действующий сертификат) если: наступил момент времени начала его действия (дата выдачи или иная дата начала действия, указанная в нем);

срок его действия не истек;

не аннулирован (не прекращен) и действие его не приостановлено;

между Банком/Оператором и владельцем сертификата отсутствуют иные условия прекращения действия сертификата, нежели предусмотренные законом.

Система «iBank» (далее - Система) - корпоративная система электронного документооборота, включающая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи электронных документов и средств электронной 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 ЭП 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 ЭП (СЭП) - программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание ЭП в ЭД с использованием закрытого ключа ЭП, подтверждение подлинности ЭП с использованием открытого ключа ЭП, создание закрытых и открытых ключей ЭП.

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 электронный вид с учетом требований настоящего Регламента к форме таких документов, заверенный ЭП (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 подпись (ЭП) - реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭП и позволяющий идентифицировать владельца сертификата ключа ЭП, а также установить отсутствие искажения информации в ЭД.

Мобильное устройство – смартфоны, мобильные телефоны, планшеты и прочие устройства, на которых есть доступ в Интернет, которые используются Уполномоченным лицом Клиента для получения SMS-кода от Оператора, которые привязаны к зарегистрированному номеру телефона.

Зарегистрированный номер – номер телефона сотовой связи Уполномоченного лица Клиента, зарегистрированный в ДБО.

SMS-код – уникальный одноразовый цифровой код, предоставляемый Оператором посредством SMS-сообщения на Зарегистрированный номер Уполномоченного лица Клиента.

Устройство Рутокен ЭЦП (Рутокен) — предоставляемое Банком персональное средство защищенной генерации и хранения ключей шифрования и Ключа ЭП, выполнения шифрования и создания ЭП, хранения Сертификатов ключа проверки ЭП, выполненное в формате USB-брелок.

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 типовым для всех Клиентов, заключивших Договор. Заключение Договора осуществляется после подачи Заявления о присоединении к Договору на обслуживание клиентов в Системе «iBank» по установленной форме, приведенной в Приложение №2 к настоящему Регламенту (далее – Заявление).
- 2.3. Стороны признают используемые в Системе Средства ЭП достаточными для защиты от несанкционированного доступа к информации, передаваемой с использованием Системы.
- 2.4. Стороны признают используемые в Системе Средства ЭП достаточными для подтверждения подлинности ЭП, идентификации Владельцев сертификатов ключей ЭП и отсутствия искажений в ЭД.
- 2.5. Подключение Клиента к Системе осуществляется на условиях, предусмотренных настоящим Регламентом. Клиент указывает вариант подключения к Системе в Заявлении. Требования к программно-техническим средствам, необходимым Клиенту для подключения к Системе «iBank» Клиента определяются в Приложении №4 к настоящему 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 Системе (в частности Сертификата ключа проверки ЭП).
- 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 совокупности следующих действий:
 - ознакомление Клиентом и согласие с условиями настоящего Регламента путем передачи им в Банк подписанного Заявления;
 - установка Клиентом необходимых программно-технических средств, клиентского программного и информационного обеспечения в соответствии с Приложением №4 к настоящему Регламенту;
 - получение Клиентом в Банке под роспись в журнале учета СКЗИ и установка криптобиблиотек и другой информации для доступа к СЭД;
 - генерация Клиентом ключей ЭП Клиента (в количестве, определенном Клиентом) и изготовление Сертификатов ключей проверки ЭП Клиента;
 - передача подписанных Владельцами Сертификатов ключей проверки ЭП на бумажном носителе в Банк для регистрации;
 - регистрация Банком ключей ЭП Клиента после принятия и проверки, оформленных в соответствии с требованиями Приложения №3 к настоящему Регламенту, Сертификатов ключей ЭП на бумажном носителе.

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, Договором, 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 ключей ЭП, а также повреждениях программно-технических средств обработки, хранения, передачи ЭД и Средств ЭП.

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 Владельцев сертификатов ключей ЭП произвести смену ключей ЭП 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. Риски возможных неблагоприятных последствий, вызванных уведомлением/несвоевременным уведомлением Банка о Компрометации, несет Клиент.
- 3.2.9. Использовать полученные у Банка программно-технические средства и ключи ЭП 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. Неукоснительно выполнять «Рекомендации клиентам ПАО Комбанк «Химик» по защите информации при пользовании системами дистанционного банковского обслуживания», изложенные в Приложении № 9 к Регламенту.
- 3.2.11. Не производить модификацию программных средств, не совершать относительно указанных программно-технических средств других действий, нарушающих действующее законодательство Российской Федерации.
- 3.2.12. 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.
- 3.2.13. Выполнять все обновления, проводимые Банком в Системе. В случае неисполнения Клиентом этих обязанностей Банк осуществляет действия, указанные в п. 3.3.25 настоящего Регламента.
- 3.2.14. Проводить смену ключей ЭП Клиента в случае, если Банк уведомит Клиента о необходимости этого.
- 3.2.15. 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.
- 3.2.16. Незамедлительно информировать Банк об изменениях, внесенных в учредительные и иные документы Клиента, в том числе об изменении своего места нахождения, почтового адреса, номеров телефона, факса; об изменениях в составе уполномоченных лиц Клиента и/или их правах доступа в Систему, в частности об увольнении, а также о любых других изменениях, влияющих или могущих повлиять на исполнение Сторонами своих обязательств по настоящему Регламенту, с предоставлением соответствующих подтверждающих документов (в случае наличия таковых). Непредоставление соответствующей информации Банк расценивает как неизменность сведений о Клиенте, установленных ранее при его идентификации. Неисполнение/несвоевременное исполнение Клиентом вышеуказанных обязательств является основанием для приостановления участия Клиента в ЭДО.

Клиент имеет право:

- 3.2.17. Получать квалифицированную помощь специалиста Банка для установки, переустановки или восстановления работоспособности Системы по телефону технической поддержки.
- 3.2.18. Получать необходимую информацию по использованию Системы.
- 3.2.19. Самостоятельно осуществить настройку программы в соответствии с технологической инструкцией системы, импорта-экспорта ЭД в собственную бухгалтерскую программу согласно инструкции, передаваемой Клиенту.
- 3.2.20. Клиент имеет право блокировать ключ ЭП Клиента, т.е. приостановить свою работу в системе «Клиент-Банк», направив письменное уведомление по форме Приложения №6 к настоящему Регламенту. Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.
- 3.2.21. Требовать замену Ключа ЭП в случае потери доверия к нему.
- 3.2.22. Досрочно прекращать действие ключей ЭП Клиента, направив письменное уведомление по форме Приложения №6 к настоящему Регламенту. Для продолжения дальнейшей работы в системе «Клиент-Банк» уполномоченный представитель Клиента должен сгенерировать новый ключ ЭП Клиента и выполнить действия, описанные в Приложении №1 к настоящему Регламенту.
- 3.2.23. 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.

- 3.2.24. Иметь возможность приостановления (блокирования) и возобновления (разблокирования) работы со счетом путем отправки Заявки на приостановку или возобновление. Заявка на приостановку работы со счетом принимается по телефону (с использованием блокировочного слова), факсу или в письменной форме. Заявка на возобновление работы со счетом принимается только по факсу или в письменной форме.
- 3.2.25. Иметь возможность на основании письменного Заявления в Банк в произвольной форме установить:
- максимальную сумму перевода денежных средств в системе ДБО;
 - перечень возможных получателей денежных средств в системе ;
 - перечень IP-адресов, с использованием которых может осуществляться доступ к системе ДБО ;
 - перечень услуг, предоставляемых с использованием системы ДБО.

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 и инструкцию по работе и подключению к системе.
- 3.3.2. Организовать 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 ЭП Клиента, в соответствии с условиями Договора, Договора банковского счета и действующим законодательством.
- 3.3.5. При получении от Клиента распоряжения по телефону (с названием блокировочного слова, указанного в Заявке) о блокировании работы в Системе, факса или Заявки по форме Приложения № 6 к настоящему Регламенту временно блокировать работу Клиента в системе «iBank».
- 3.3.6. Обеспечить строго контролируемый и ограниченный доступ к программно-аппаратным средствам, содержащим контрольные архивы системы «iBank».
- 3.3.7. Хранить в секрете и не передавать третьим лицам ключ ЭП Банка и ключ ЭП Клиента, используемые при работе в системе «iBank». Риск неблагоприятных последствий, связанных с использованием Ключа ЭП 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 ЭП, провести мероприятия, определенные настоящим Регламентом.
- 3.3.10. В кратчайшие сроки устранить неисправности Системы, возникшие по вине Банка.
- 3.3.11. В случае неисполнения Клиентом обязанностей, изложенных в п.3.2 настоящего Регламента, приостановить прием и исполнение ЭД, подписанных ЭП, срок действия которых истек, до момента генерации и сертификации новых ключей в соответствии с Регламентом.
- 3.3.12. Исполнение документов осуществлять в сроки, установленные Договором банковского счета.
- 3.3.13. При получении электронного документа Банк проводить проверку:
- корректности ЭП Клиента открытым ключом ЭП Клиента;
 - правильности заполнения реквизитов электронного документа.
- 3.3.14. При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный электронный документ системой «iBank» не принимается и автоматически возвращается Клиенту с соответствующим статусом, поручение, содержащееся в нем, Банком не исполняется. Иного информирования Клиента о неисполнении переданного им по системе «iBank» электронного документа Банком не осуществляется. Свидетельством того, что документ исполнен, является содержащая ЭП Банка электронная квитанция о проведении его банком. Отсутствие у Клиента указанной электронной квитанции означает, что электронный документ Банком проведен не был.
- 3.3.15. Осуществлять прием расчетных документов, передаваемых по электронной системе «iBank» в период времени, указанный в Договоре ДБО. Использование системы «iBank» не лишает Клиента права предоставлять Банку иные электронные документы, а также расчетные и иные документы на бумажном носителе в течение всего рабочего времени, установленного Банком.
- 3.3.16. 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:

- 3.3.17. Не подключать Клиента к Системе в случае несоответствия имеющихся у него аппаратных средств требованиям Приложения №4 к Регламенту до момента приведения их в соответствие.
- 3.3.18. Не принимать к исполнению ЭД, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных актов Банка России, Договоров банковского обслуживания и Регламента.

- 3.3.19. Оформлять бумажные копии принятых ЭД Клиента и заверять их в соответствии с внутренними нормативными документами Банка.
- 3.3.20. Проводить плановую смену ключей ЭП Банка и Клиента (не чаще одного раза в год), о чем извещает Клиента по Системе за две недели до даты начала смены ключей.
- 3.3.21. Производить обновления версий Системы.
- 3.3.22. В случае неоплаты Клиентом услуг Банка в соответствии с п. 4.1. 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.
- 3.3.23. Вносить изменения в Регламент в одностороннем порядке.
- 3.3.24. В случае неисполнения Клиентом обязанностей, предусмотренных Регламентом, заблокировать проведение операции Клиента в Системе.
- 3.3.25. После предварительного предупреждения отказать Клиенту в приеме от него распоряжения на проведение операции по банковскому счету (вкладу), подписанному аналогом собственноручной подписи в случае выявления Банком в деятельности Клиента критериев сомнительных операций, на основании которых в отношении операций Клиента возникают подозрения, что они осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма либо в случае наличия данных о Клиенте или его счетах/корпоративных карт в базе данных о случаях и попытках осуществления ~~переводов~~ денежных средств без добровольного согласия ~~клиента~~ в соответствии с, а также в иных случаях, установленных Федеральным законом от 27.06.2018~~2011~~ N 167-ФЗ: «О национальной платежной системе», либо непредоставления сведений и/или документов по запросу Банка в целях проведения идентификации Клиента, установления экономического смысла проводимых Клиентом операций/сделок, либо предоставления недостоверных документов, документов с признаками фальсификации по вышеуказанному запросу Банка, а также в случае, если Клиент является лицом, в отношении которого в единый государственный реестр юридических лиц внесена запись о недостоверности сведений о юридическом лице, или наличии информации о дисквалификации единоличного исполнительного органа Клиента, в иных случаях. При этом Банк принимает от такого Клиента надлежащим образом оформленные платежные документы на бумажном носителе (за исключением случаев, когда не завершено обновление сведений о Клиенте, представителе Клиента, выгодоприобретателе, бенефициарном владельце, при наличии у Банка информации об изменении информации, ранее предоставленной Клиентом, а также если в отношении Клиента в единый государственный реестр юридических лиц внесена запись о недостоверности сведений о юридическом лице, при наличии информации о дисквалификации единоличного исполнительного органа Клиента и прочее).
- 3.3.26. В случае приостановления обслуживания Клиента с использованием Системы по основанию, указанному в п. 3.3.25 настоящего Регламента, возобновить прием и исполнение ЭД, подписанных ЭП, после устранения Клиентом нарушений условий настоящего Регламента и предоставления всех необходимых документов по запросам Банка в целях соблюдения законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма либо после ~~получения~~ отключения данных о Клиенте или его счетах/корпоративных карт из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

4. ФИНАНСОВЫЕ ВЗАИМООТНОШЕНИЯ.

- 4.1. Оплата за установку и обслуживание по системе «iBank» производится в соответствии с Договором 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 Заявления 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 настоящему Регламентом и Договорам банковского обслуживания. ЭД должен быть сформирован в формате, предусмотренном разработчиками системы «iBank» или Договорами банковского обслуживания и заверен ЭП, имеющей сертифицированный Банком ключ ЭП. ЭД без ЭП или имеющий формат, не отвечающий установленным правилам, в качестве ЭД в соответствии с настоящим Регламентом не рассматривается.

5.2. Использование ЭП и шифрования в ЭДО.

- 5.2.1. Используемые при информационном взаимодействии Сторон ЭД, заверенные ЭП 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 ЭП 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 ЭП, сертификат открытого ключа которой зарегистрирован в СЭД в порядке, установленном настоящими Правилами.

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

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

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

6. ОРГАНИЗАЦИЯ ЭДО.

6.1. ЭДО включает:

- 1) формирование ЭД;
- 2) отправку и доставку ЭД;
- 3) проверку ЭД;
- 4) подтверждение получения ЭД;
- 5) информирование Клиента о движении денежных средств на счете Клиента;
- 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 ЭП, передачи, проверки, получения и исполнения Сторонами ЭД в Системе сопровождается изменением статуса ЭД.

6.2.2. Таблица статусов ЭД в Системе с комментариями.

| Статус | Пояснения |
|---------------|---|
| Новый | Присваивается при создании и сохранении нового документа Клиентом, при редактировании и сохранении существующего документа, а также при импорте документа из файла, сформированного в одной из бухгалтерских программ Клиента. Документ в статусе «Новый» Банк не рассматривает и не обрабатывает. |
| Подписан | Присваивается в случае, если Электронный документ подписан, но число подписей под ним недостаточно для рассмотрения данного документа Банком. При внесении изменений в документ в таком статусе и его последующем сохранении статус документа меняется на «Новый». |
| Доставлен | Присваивается документу, когда число подписей под документом достаточно для его рассмотрения Банком и выполнены все дополнительные условия в соответствии с настройками Системы, выполненными самостоятельно Клиентом или Банком по заявлению Клиента. Статус «Доставлен» означает, что Электронный документ получен Банком в момент установки этого статуса, и является для банка указанием начать обработку Электронного документа. |
| На обработке | Обработка документа начата сотрудником или автоматизированной системой Банка. Решение об исполнении или отвержении данного документа ещё не принято. |
| На исполнении | Банком принято решение об исполнении данного Электронного документа. |
| Исполнен | Документ исполнен Банком. Для платёжных документов статус «Исполнен» означает успешное завершение соответствующей расчётной операции. Для прочих документов статус «Исполнен» означает принятие Банком данного документа в соответствии с действующим законодательством Российской Федерации, нормативными документами государственных органов, регламентирующими документооборот соответствующего вида электронных или бумажных документов, а также договорами и соглашениями, заключенными между Сторонами. |

| | |
|-------------------------|---|
| Отвергнут | Присваивается документу, не принятому к исполнению. Причина отвержения документа указывается в описании статуса. Клиент может или отредактировать и сохранить документ (ему будет присвоен статус «Новый»), или удалить документ (ему будет присвоен статус «Удален»). |
| Удалён | Присваивается документу, удаленному сотрудником Клиента. Удалению подлежат только документы в статусе «Новый», «Подписан» или «Отвергнут». Документы в статусе «Новый» и «Подписан» удаляются из Системы безвозвратно. Документы, имеющие статус «Отвергнут» после удаления, сохраняются в Системе и доступны для просмотра. |
| На акцепт | При использовании модуля «Центр финансового контроля» (ЦФК) присваивается платежному поручению или заявлению на перевод в случаях нарушения правил контроля, заданных в ЦФК. Статус также присваивается, если установлено принудительное акцептование. |
| Требуется подтверждения | Присваивается Электронному документу после получения необходимого для доставки в Банк количества подписей в случае использования дополнительных мер защиты документа. Для доставки в банк такого документа клиенту необходимо ввести код подтверждения. Необходимость и способ получения кода подтверждения устанавливается на основании заявления Клиента. |
| В картотеке | Присваивается платежному поручению при недостаточности средств на счете Клиента. Порядок обработки таких платёжных поручений определен действующим законодательством и соответствующими нормативными документами Банка России. |

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 ЭП.

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 ЭП 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 «Исполнен». 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 непринятых ЭД.

6.7. Получение Клиентом выписки по счету.

6.7.1. 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).

6.8. Регистрация действий клиентов и операционистов

Все действия операционистов и клиентов автоматически регистрируются в Журнале работы банковской части системы ДБО. Срок хранения журнала — не менее 5 лет, начиная с даты осуществления действия.

6.8.1. В действиях операционистов фиксируется следующая информация :

- дата и время действия;
- идентификатор операциониста;
- выполняемое действие.

6.8.2. В действиях клиентов фиксируется следующая информация:

- дата и время действия;
- идентификатор клиента;
- выполняемое действие;
- IP адрес клиента;
- MAC адрес устройства клиента;
- ID документа(при передаче документа).

7. ОТВЕТСТВЕННОСТЬ СТОРОН

- 7.1. За неисполнение или ненадлежащее исполнение обязательств по Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.
- 7.2. Клиент несет ответственность за передачу соответствующих ключевых носителей и их использование лицами, не являющимися Владельцами сертификатов ключей ЭП.
- 7.3. 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 «iBank»

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. В Системе электронного документооборота, осуществляемого в соответствии с Регламентом используются сертифицированные средства криптографической защиты информации (СКЗИ "**Крипто-КОМ 3.5**"), предназначенные для защиты интернет-приложения. Защита подразумевает под собой шифрование передаваемой информации и наложение электронной подписи (ЭП), обеспечивающей конфиденциальность и целостность подписываемого документа. .
- 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 ЭП Клиента имеет свои закрытые ключи ЭП, а также соответствующие им открытые ключи ЭП. Открытые ключи ЭП передаются Клиентом в Банк.
- 1.5. Документом, подтверждающим принадлежность открытого ключа ЭП уполномоченному лицу Клиента, является сертификат ключа ЭП. Сертификат ключа ЭП 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 ЭП отправителя ЭД и открытого ключа ЭП получателя ЭД, для электронной подписи ЭД необходим только собственный закрытый ключ ЭП. Для расшифрования ЭД получателем ЭД используется открытый ключ ЭП отправителя ЭД и собственный закрытый ключ ЭП, для проверки ЭП электронного документа необходим только открытый ключ владельца ЭП, подписавшего ЭД. Реализованные в СКЗИ алгоритмы шифрования и электронной подписи гарантируют невозможность восстановления закрытых ключей ЭП и шифрования отправителя ЭД по его открытым ключам.
- 1.7. Открытый ключ ЭП Клиента считается зарегистрированным в Банке с даты, проставленной Банком на распечатке сертификата ключа ЭП, оформленной в соответствии с Приложением №3 к настоящему Регламенту.
- 1.8. Открытый ключ ЭП Клиента считается действующим в момент проверки ЭП при одновременном выполнении следующих условий:
 - сертификат ключа ЭП зарегистрирован в Банке;
 - период действия сертификата ключа ЭП не истек;
 - действие сертификата ключа ЭП не отменено.
- 1.9. Для отмены действия открытого ключа ЭП Клиент передает в Банк письменное уведомление об отмене действия сертификата этого открытого ключа ЭП.
- 1.10. Открытый ключ ЭП Клиента считается отмененным с момента регистрации в Банке уведомления об отмене действия сертификата открытого ключа ЭП.
- 1.11. Открытый ключ ЭП 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 ЭП Клиента на автоматизированном рабочем месте Клиента. Клиент обязан обеспечить конфиденциальность при изготовлении закрытых ключей ЭП.

2. ПОРЯДОК ПЕРВИЧНОЙ ВЫДАЧИ ПРОГРАММНЫХ КОМПОНЕНТОВ СКЗИ

- 2.1 Клиент оформляет заявление по форме Приложения №2 к настоящему Регламенту.
- 2.2 Банк в соответствии с заявлением передает Клиенту адрес сайта банка в сети Интернет, необходимый для формирования его ЭП.
- 2.3 Генерация и регистрация криптографических ключей Клиента осуществляется в следующей последовательности:
 - 2.4.1 Клиент:
 - каждое должностное лицо уполномоченное ставить ЭП под ЭД самостоятельно с помощью браузера, следуя указаниям на сайте банка создает на ключевом носителе ключ ЭП, и формирует сертификат открытого ключа ЭП на бумажном носителе в 2-х экземплярах по форме Приложения №3 к настоящему Регламенту, при этом Клиент контролирует правильность заполнения полей сертификата ключа ЭП;
 - заверяет оба экземпляра распечатки сертификата ключа ЭП подписями Владельца сертификата ключа ЭП и скрепляет печатью;
 - передает в Банк распечатанные по форме Приложения №3 к настоящему Регламенту и заверенные подписью и печатью сертификаты всех ключей ЭП в одном экземпляре.
 - 2.4.2 Банк:
 - принимает оформленные сертификаты ключа ЭП у Клиента на бумажном носителе;
 - проверяет содержание распечаток сертификата Открытого ключа ЭП на соответствие Открытого ключа ЭП, сохраненного в базе Банка, а также проверяет правильность заполнения полей сертификата ключа ЭП и соответствие подписей владельца сертификата ключа ЭП, указанным в карточке с образцами подписей и оттиска печати;
 - в случае положительного результата проверки регистрирует открытый ключ Клиента, полученный в электронном виде.
 - 2.4.3 Клиент:
 - начинает работу по системе ДБО.

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 ЭП.
- 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.
- 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 ЭП удаляются.
- 3.5. 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.
- 4.2. Требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ:
 - 4.2.1. 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.
 - 4.2.2. Руководитель организации или лицо, им уполномоченное, должно иметь представление о возможных угрозах при обработке, передаче и хранении информации, методах и средствах защиты информации.
- 4.3. 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.
- 4.4. Внесение изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ осуществляется только администратором ИБ после получения соответствующих изменений от разработчика СКЗИ с проверкой контрольной суммы дистрибутива.
- 4.5. При завершении эксплуатации системы, все средства СКЗИ и ключи ЭП должны быть уничтожены на всех носителях с составлением Акта уничтожения ключевой информации.

Заявление о присоединении к системе «iBank»

| | | | | | |
|--|--|-------------------------|--|--------|--|
| Полное и сокращенное наименование Клиента (для ЮЛ) /Фамилия, имя, отчество (при его наличии) (для ИП) | | | | | |
| Наименование на английском языке (при открытии счетов в иностранной валюте) | | | | | |
| Должность и фамилия, имя, отчество (при его наличии) руководителя | | | | | |
| ОГРН / ОГРНИП | | ИНН / КПП | | | |
| Контактный Моб. телефон | | Иной Контактный телефон | | E-mail | |

Руководствуясь действующим законодательством Российской Федерации, правилами и требованиями, установленными Договором на обслуживание клиентов в Системе «iBank» в ПАО Комбанк «Химик» (далее - «Банк»), Клиент предьявляет настоящее Заявление о присоединении (далее – «Заявление о присоединении») к Договору на обслуживание клиентов в Системе «iBank» в ПАО Комбанк «Химик» (далее - «Договор») и присоединяется к Договору, руководствуясь положениями ст. 428 Гражданского кодекса РФ и поручает Банку произвести подключение к системе «iBank» для совершения операций по счету _____.

1. Необходимые действия:

Первоначальное подключение

Смена ЭП

2. Блокировочное слово _____

3. Подключить СМС-информирование и СМС-авторизацию по телефону телефон _____

4. Подключить оповещение по электронной почте адрес электронной почты _____

5. Передача программных средств Системы, СКЗИ (в случае передачи через Представителя Клиента необходимо представить доверенность на получение ключевых материалов, СКЗИ)

ФИО Представителя клиента, Должность

Настоящим подтверждаю, что с Договором на обслуживание клиентов в Системе «iBank», Регламентом электронного документооборота в системе «iBank» ПАО Комбанк «Химик», Тарифами ПАО Комбанк «Химик» на подключение и обслуживание системы «iBank» ознакомлен, согласен и обязуется неукоснительно их выполнять. Оплату гарантируем.

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

ОТМЕТКИ БАНКА О ПРИНЯТИИ ЗАЯВЛЕНИЯ

уполномоченный сотрудник Банка: должность, ФИО, подпись

Принято " ____ " _____ 20 ____ г.

Договор на обслуживание клиентов в Системе «iBank» и Регламент электронного документооборота в системе «iBank» ПАО Комбанк «Химик» размещены на сайте по ссылке: <https://www.bankhimik.ru/docs.html#5>.

Требования к программно-техническим средствам Клиента.

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

Для работы с **Системой «iBank»** сервисом пользователю необходимы:

- Современный компьютер с операционной системой. Работа с сервисом возможна на следующих ОС:
 - Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
 - Apple Mac OS X: 10.7 и выше;
 - Ubuntu и прочие deb-дистрибутивы (последние версии x64).
- Монитор с разрешением не менее 1280x1024;
- Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере пользователя. СКЗИ используется для реализации функций формирования ключей шифрования и электронной подписи, выработки и проверки электронной подписи, шифрования и имитозащиты информации.
- Web-браузер с поддержкой BIFIT Signer для использования электронной подписи. Поддержка BIFIT Signer обеспечена в следующих браузерах:
 - Microsoft Edge;
 - Google Chrome;
 - Яндекс.Браузер;
 - Firefox;
 - Opera;
 - Atom;
 - Safari (при условии, что браузер используется совместно с Mac OS X).Рекомендуется использовать последние версии браузеров.
- Рекомендуется наличие в компьютере пользователя USB-порта для подключения аппаратных устройств.
- Доступ в Интернет. Рекомендуемая скорость соединения — 33,6 Кбит/сек и выше. В случае доступа в Интернет по телефонной коммутируемой линии необходимо наличие современного модема.
- Рекомендуется наличие принтера.

Уведомление

г. Дзержинск

«__» _____ 20__ г.

(наименование клиента)

(номер счета)

Уведомляет о:

Приостановлении работы в системе «iBank» («Клиент-WEB») (на срок до 3-х месяцев)

Срок: с «__» _____ г. по «__» _____ г.

Причина: _____

Отключении от обслуживания по системе «iBank» («Клиент-WEB»)

Причина: _____

Смене ЭП в связи с:

Сменой руководителя или других реквизитов

Старые реквизиты:

Новые реквизиты:

Компрометацией ключей:

Описание: _____

Иное: _____

Смене пароля в связи с: _____

Настоящим подтверждаем, что с Регламентом электронного документооборота в системе «iBank» ПАО Комбанк «Химик», Тарифами ПАО Комбанк «Химик» на подключение и обслуживание системы «iBank» ознакомлены, согласны и обязуемся неукоснительно их выполнять. Оплату гарантируем.

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

М.П.

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

ДОВЕРЕННОСТЬ № _____

«__» _____ 20__ г.

_____ ,
полное наименование Клиента

далее – Клиент, в лице _____ ,
должность, фамилия, имя, отчество

действующего на основании _____ ,

уполномочивает _____ ,
должность, фамилия, имя, отчество ответственного лица

_____ ,
паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи

_____ ,
телефон для связи

на выполнение следующих действий:

- получать программное обеспечение;
- получать логины и пароли для генерации рабочих ключей;
- получать ключевые носители;
- получать сертификаты рабочих ключей.

Настоящая доверенность выдана без права передоверия и действительна по «__» _____ 20__ года включительно.

Подпись _____ удостоверяю.

ФИО доверенного лица

личная подпись

Руководитель _____ (_____)
наименование должности *личная подпись*

М.П.

УТВЕРЖДАЮ
От Банка:
Председатель Правления
ПАО Комбанк "Химик"

_____ Кастров Т.Н.
(подпись)

М.П.

УТВЕРЖДАЮ
От Клиента:
Директор
ООО «Пример»

_____ Ф.И.О.
(подпись)

М.П.

АКТ
о вводе в эксплуатацию системы «iBank»

Мы, нижеподписавшиеся, представитель Банка, _____,
с _____ одной стороны, _____ и _____ представитель
Клиента, _____, действующий на основании
_____ с другой стороны, составили
настоящий Акт о том, что _____ передано программное обеспечение и
СКЗИ «Крипто-КОМ 3.5» для системы «iBank». Система "iBank" с доступом через интернет
введена в эксплуатацию.

Стоимость установки _____ рублей (_____ рублей 00 копеек). НДС не
облагается.

От Банка:

« ____ » _____ Г.

От Клиента:

« ____ » _____ Г.

Рекомендации клиентам ПАО комбанк «Химик» по защите информации при пользовании системами дистанционного банковского обслуживания.

Установить пароли на учётные записи пользователей операционной системы на компьютере, где используется «Интернет-Банк».

В случае компрометации или подозрении на компрометацию закрытого ключа ЭП, для предотвращения несанкционированного доступа к управлению счетом, в том числе при утрате (потере, хищении) ключевого носителя, с использованием которого Клиент осуществляет перевод денежных средств, Клиенту необходимо незамедлительно обратиться в Банк для блокирования скомпрометированных ключей.

Ключевая информация – это аналог Вашей личной подписи, при ее использовании соблюдайте следующие правила:

- ключевой носитель нельзя передавать третьим лицам, оставлять без присмотра, хранить в доступном месте;
- при получении ключевого носителя необходимо создать резервную копию, хранимую в сейфе;
- на электронном носителе (обычно Флэш-карта), на котором расположены ключи, не должно быть другой информации;
- хранение закрытого ключа ЭП на жёстком диске НЕДОПУСТИМО;
- необходимо отключать, извлекать ключевой носитель и хранить его в сейфе, если он не используется для работы в ДБО.

При смене, увольнении лица, имеющего, даже потенциально, доступ к ключевому носителю (например, системного администратора), необходимо незамедлительно:

произвести замену ключевого носителя при содействии Отдела автоматизации ПАО комбанк «Химик»: тел.: (8313)39-30-80.

Для того чтобы защитить Ваши денежные средства, настоятельно рекомендуем контролировать состояние счёта (путем просмотра выписки);

Просим вас незамедлительно обращаться в банк при возникновении следующих ситуаций:

- на компьютере, используемом для работы в интернет-банке, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.);
- обнаружены факты проникновения в систему посторонних лиц;
- в выписке обнаружены несанкционированные Вами расходные операции;
- у Вас не работает система «Интернет-Банк» по неизвестным причинам.

Рекомендации по защите информации от воздействия вредоносного кода.

Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

Своевременно обновляйте установленное программное обеспечение и операционную

систему (патчи, критичные обновления).

Обязательно установите на компьютере лицензионное антивирусное программное обеспечение, и настройте автоматическое обновление антивирусных баз.

Не отключайте антивирусное программное обеспечение.

Регулярно выполняйте полную проверку компьютера на наличие вредоносного программного обеспечения, но не реже одного раза в неделю.

Не используйте зараженный компьютер до полного излечения от вирусов.

Не используйте права администратора при отсутствии необходимости. Входите в систему с учетной записью пользователя, не имеющего прав администратора.

При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.

Воздерживайтесь от использования программ онлайн общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.

Ограничьте круг лиц, имеющих доступ к компьютеру. Не оставляйте без контроля включенный компьютер.

Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.

Ограничьте информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты.

При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, особенно если получения подобной корреспонденции не ожидается. Не переходите по содержащимся в таких письмах ссылкам. Не открывайте вложения.

Не оставляйте хранилище секретного ключа постоянно подключенным к компьютеру. Подключайте устройство только для входа в систему или подписи документов.

Не используйте на компьютере посторонние съемные носители информации (usb-накопители, CD/DVD-диски, дискеты). При необходимости использования подобных носителей необходимо провести полную проверку на наличие вредоносного кода.

Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

Придумайте сложный пароль из букв и цифр, который вы больше нигде не применяете.

Никому не сообщайте Ваши логин и пароль, в том числе сотрудникам Банка.

Не сохраняйте логины/пароли в браузере.

Не храните логин и пароль в компьютере или мобильном телефоне.

Не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

Завершайте работу в интернет-банке выходом из системы.

Не используйте на устройстве, предназначенного для доступа к системе ДБО, средства удаленного администрирования.

Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные. Банк никогда не связывается по телефону и не осуществляет рассылку сообщений по SMS или e-mail с таким запросом.

Не открывайте подозрительные файлы, поступившие вам по электронной почте. Банк никогда не рассылает программы в своих электронных письмах и не связывается с просьбой установить или обновить программное обеспечение.

Не отвечайте на полученное подозрительное сообщение от имени Банка и не переходите по ссылкам, указанным в сообщении.

ПОМНИТЕ!!! Банк ни при каких обстоятельствах и ни в какой форме не запрашивает у клиентов конфиденциальную информацию о секретных ключах и паролях и не направляет обновления программного обеспечения по почте. Если Вы получили подобное сообщение, проигнорируйте его и немедленно поставьте в известность об этом факте Вашу службу безопасности и Банк, позвонив в службу технической поддержки системы «Банк-Клиент» по телефону

Во избежание инцидентов, связанных с неправомерным использованием Вашей компьютерной техники, используемой для работы в системе «Банк-Клиент», убедительно просим Вас неукоснительно соблюдать рекомендуемые выше правила безопасности.

Только комплексное соблюдение описанных правил безопасности позволит Вам не стать жертвой мошенников и иных злоумышленников и поможет обеспечить защиту **ВАШИХ ДЕНЕЖНЫХ СРЕДСТВ.**