БАНК ДОЛИНСК

Рекомендации

Для клиентов КБ «Долинск» ЗАО использующих средства криптографической защиты информации при осуществлении электронного документооборота по системе iBank2 или Клиент-Банк

(Версия 1.0)

г. Южно-Сахалинск
2015 год

Введение

Система «Клиент-Банк» позволяет Клиенту просматривать информацию и осуществлять платежи со счетов в Банке, не покидая своего офиса в режиме on-line. Система полностью автоматизирует документооборот между бухгалтерией Клиента и Банком, обеспечивает гарантированный уровень безопасности, применяя различные средства и методы защиты информации - от паролей до многоуровневых систем безопасности на основе современных криптографических протоколов и алгоритмов.

Система «Клиент-Банк» обеспечивает безопасность и конфиденциальность документооборота с банком, используя программное средство криптографической защиты информации. При работе с Системой «Клиент-Банк» весь трафик проходит через защищенное соединение. Личность клиента подтверждается паролем и наличием криптоустройства, подключенного к компьютеру.

Для обеспечения аутентичности (доказательство авторства) и целостности документа в Системе «Клиент-Банк» используется механизм электронной подписи (ЭП) под электронными документами. Именно электронный документ с ЭП является основанием для совершения финансовых операций и доказательной базой при разрешении конфликтных ситуаций.

Более подробную информацию Вы можете получить в КБ «Долинск» ЗАО
по адресу 693010, Сахалинская обл., г. Южно-Сахалинск, ул. Комсомольская, 145

Телефоны для справок:
Приемная 8(4242) 49-40-10
Служба технической поддержки 8(4242)49-40-35

Правила пользования электронной подписью

Вы должны осознавать, что все функции ЭП могут быть обеспечены только при условии сохранения Вами в тайне пароля к ключу ЭЦП, ограничении доступа к ПК с iBank2 и ограничении доступа к криптоустройству, выданному нашим Банком. В связи с этим особо обращаем Ваше внимание на некоторые правила пользования электронной подписью:

- **хранение ключей**. Носители ключей необходимо хранить в условиях, исключающих доступ к ним посторонних лиц (например, в металлических хранилищах).

- **защита от вредоносных программ.** Удалить все, не имеющее отношение к работе iBank2 и к обеспечению безопасности, ПО с ПК. Обязательно установить антивирус. Рекомендуется устанавливать последние пакеты обновлений (Service Packs) и актуальные патчи безопасности операционной системы, базы антивирусного ПО, обновление которых должно проводиться регулярно. Отключить функцию AutoRun с внешних носителей.

- **защита в сети.** По возможности, перенести ПК с iBank2 отдельную подсеть для исключения возможности подключения к этому ПК сотрудников Вашей организации. Установить в фильтрах только те IP-адреса и порты организаций, с которыми Вы работаете. Все остальное должно быть закрыто!!! Рекомендуем не использовать удаленный доступ к ПК с iBank2.

- **внимательность.** При получении писем (SMS-сообщений) от неизвестных Вам отправителей – не отвечайте на них, не соглашайтесь ни с какими запросами и предложениями. Не переходите ни по каким ссылкам из таких писем (SMS-сообщений) и не звоните ни по каким указанным там номерам телефонов. Номера телефонов, по которым вы можете получить консультацию, указаны на нашем сайте www.bankdolinsk.ru.

- **использование.** Для безопасного использования СКЗИ рекомендуется принять меры по оборудованию, охране и организации режима в помещении, где установлены СКЗИ. Монитор ПК должен быть установлен таким образом, чтобы исключить возможность визуального снятия информации с экрана. Исключить возможность подглядывания пароля при наборе на клавиатуре. Если пользователь СКЗИ покидает помещение, не выключая компьютер, то его необходимо блокировать (например, сочетанием клавиш «Windows + L»). Выключать ПК с БК по окончании рабочего дня. При завершении работы с iBank2 – убирать носители ключей в хранилище индивидуального пользования запираемое на замок.

- **политика паролей**. При регистрации ключа настоятельно рекомендуется установить пароль доступа к контейнеру хранения ключа ЭП высокой сложности. Так же пароль на вход в iBank2 должен быть высокой сложности. Для каждого пользователя ПК с iBank2 должен быть установлен индивидуальный пароль высокого уровня сложности.

- **взаимодействие с КБ «Долинск» ЗАО**. Пользователь должен незамедлительно сообщать в наш Банк о фактах доступа (вероятного доступа) к закрытому ключу посторонних лиц. При этом до выяснения фактов наличия компрометации ключей действие сертификата приостанавливается. В случае если компрометации ключей не было – сертификат возобновляется, в противном случае – отзывается (аннулируется), с последующим выпуском нового сертификата. В случае неожиданного выхода из строя компьютера, необходимо прекратить работу на ПК, физически выключив его, т.к. такие поломки могут быть следствием работы вредоносного ПО. Срочно сообщить об этом происшествии сотрудникам нашего Банка и проконтролировать через операциониста все поступившие от клиента платежные документы.

Пользователь должен своевременно сообщать в наш Банк об изменении значимых атрибутов (параметров), в том числе включаемых в сертификат (изменение ФИО, паспортных данных, должности, организации и т.п.).

КБ «Долинск» ЗАО не осуществляет рассылку электронных писем с просьбой прислать ключ ЭП, логин и пароль, и не рассылает по электронной почте никакие программы. Вся ответственность за конфиденциальность ключа ЭП клиента полностью лежит на клиенте, как единственном владельце ключа ЭП.

В соответствии с требованиями российского законодательства электронная подпись выдается физическому лицу без права передачи.