КЛАССИК ЭКОНОМ БАНК
АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК
(Закрытое Акционерное Общество)
362025, РСО - Алания, г. Владикавказ,ул. Фрунзе,24
(8672) – 540417,540418, т/ф (8672) – 540419

Правила безопасности при использовании банк-клиента.

1. Для обеспечения безопасности ваших персональных данных и предотвращения несанкционированного доступа к вашему счету необходимо соблюдать ряд правил:

1) Клиент обязан не передавать третьим лицам носитель с установленными сертификатом и ключом.
2) Клиент обязан хранить в секрете и никому не сообщать пароль для подключения к ДБО «iBank2».
3) Клиент должен не использовать подозрительное ПО при работе с ДБО «iBank2».
4) Не рекомендовано хранить копии сертификата и ключа на локальном диске ПК.
5) Клиент должен не оставлять ПК, подключенный к ДБО «Название», без присмотра.
6) Клиент обязан сообщать в банк о попытках несанкционированного доступа в ДБО «iBank2».
7) Клиент должен обеспечивать целостность и сохранность программного комплекса ДБО «iBank2».
8) Клиент обязан допускать к работе с ДБО «iBank2» только сотрудников, имеющих соответствующую подготовку.
9) Клиент обязан по требованию банка сгенерировать новую пару сертификат-ключ и сменить секретный пароль.
10) Если Вы обнаружили в сети Интернет ложный Web-сайт АКБ «КЭБ» (ЗАО), отличный от www.akbkeb.ru, или с Вами пытаются связаться по электронной почте или иным способом лица, с требованиями о предоставлении персональных идентификаторов доступа к системе дистанционного банковского обслуживания, просьба немедленно сообщить об этом в Отдел автоматизации АКБ “КЭБ» (ЗАО) по телефону: 8 (8672) 53-73-22.

2. Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

При подключении к сети Интернет велика вероятность заражения используемого оборудования вредоносными программами, которые распространены в сети и используются злоумышленниками для кражи у пользователей систем дистанционного банковского обслуживания файлов с секретными ключами электронной цифровой подписи (ЭЦП) и паролей. Использование лицензионного антивирусного программного обеспечения со своевременным автоматическим обновлением позволит существенно снизить риски потери защищаемой информации. Пользователям систем дистанционного банковского обслуживания необходимо использовать дополнительные организационные меры по обеспечению информационной безопасности:

1) Ключевые носители системы дистанционного банковского обслуживания (дискета или флешка) должны храниться в сейфе, доступ к которому должен быть строго ограничен и предоставляться только уполномоченным лицам. Хорошей практикой является хранение вышеуказанных носителей в сейфе в опечатанном контейнере. Целостность печати (пломбы) должна ежедневно, в начале рабочего дня, контролироваться руководителем организации или уполномоченным лицом. После завершения работы ключевой носитель помещается в контейнер и заново опечатывается (пломбируется) уполномоченным лицом.

2) Не рекомендуется использовать компьютер, на котором развернута программа дистанционного банковского обслуживания (далее - компьютер), для просмотра посторонних (не относящихся к системе дистанционного банковского обслуживания) Интернет сайтов, работы с электронной почтой (особенно через общедоступные почтовые сервера: Mail.ru и т.д.), устанавливать игры и любые программы с пиратских дисков, просматривать видеофильмы, слушать музыку, загружать и устанавливать программы из Интернет, открывать и редактировать непроверенные антивирусом DOC, XLS, PDF файлы.

3) В случае временного перерыва в работе с компьютером (совещание, обед и т.д.) необходимо завершить работу с программой дистанционного банковского обслуживания, убрать в сейф ключевой носитель, выключить компьютер или заблокировать его клавиатуру и экран путем нажатия клавиш Ctrl-Alt-Del.

4) Запрещается записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам. Если есть необходимость – храните все пароли записанными на одном листе, в сейфе, в опечатанном конверте.

5) В случае любых кадровых перестановок лиц, имевших доступ к компьютеру и ключам, при подозрении в несанкционированном доступе (локально или по сети) неуполномоченных лиц к компьютеру, ключам, программе дистанционного банковского обслуживания, паролям или других случаях компрометации системы дистанционного банковского обслуживания Вам необходимо связаться со специалистами кредитной организации, сообщить название Вашей организации, номер счета и детально описать что произошло. Это позволит нам оперативно заблокировать доступ к Вашему счету через систему дистанционного банковского обслуживания.

В случае нарушения вышеуказанных пунктов АКБ «КЭБ» (ЗАО) не несет ответственности за полученный ущерб, причиненный Клиенту.

Ознакомлен: _____ _____

(наименование организации/ФИО) (подпись)

«____» _____ 20 ____г.