



## Правила доступа клиентов кредитной организации к услугам ДБО с указанием мер информационной безопасности

Для снижения рисков, возникающих при дистанционном банковском обслуживании, особенно с применением интернет-технологий, КБ «КБР БАНК» (ООО) настоятельно рекомендует Вам выполнять следующие требования:

### **Общие требования безопасности при работе в сети интернет:**

- При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- Своевременно обновлять операционную систему (установка патчей, критических обновлений).
- Не использовать права администратора при отсутствии необходимости. В повседневной работе входить в систему как пользователь, не имеющий прав администратора.
- Периодически просматривать журнал событий операционной системы и реагировать на ошибки.
- Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (ПО) (AVAST, NOD32, Kaspersky, Symantec AntiVirus и т.д.).
- Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
- При выходе в Интернет использовать сетевые экраны (встроенный в MS Windows, аппаратные межсетевые экраны, Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам сети Интернет.
- Запретить в межсетевом экране соединение с сетью Интернет по протоколу smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
- Не давать разрешения неизвестным программам выходить в сеть Интернет.
- При работе в интернет не соглашаться на установку каких-либо дополнительных программ.

### **Требования к персональному компьютеру, используемому при работе в системе «Клиент-Банк»:**

- Должен быть установлен и обновлен антивирус.
- Должен быть установлен и настроен межсетевой экран.
- Пароли учетных записей, обладающих правами администратора, должны быть сложными (содержать заглавные и строчные буквы, цифры, спецсимволы, длина не менее 8 символов).
- Учетная запись «Гость» должна быть выключена.
- Не должно быть учетных записей с пустыми паролями.
- Должны быть установлены все критические обновления к установленной операционной системе.
- Воздерживаться от использования программ онлайн-общения (таких, как ICQ) на компьютере, используемом для работы в системе «Банк-Клиент».

### **Комплекс мер безопасности при работе в системе «Клиент-Банк»:**

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

- При первоначальном получении ПО «Клиент-Банк» и «Интернет-Клиент» в состав входят **технологические ключи ЭЦП**, необходимые для **выработки рабочих ключей ЭЦП абонентом самостоятельно** и не дающие права подписи платежных документов;
- После выработки **рабочих ключей ЭЦП** необходимо создать резервную копию ключевого носителя, хранимую в сейфе;
- Ключевой носитель с **рабочими ключами ЭЦП** нельзя передавать третьим лицам, оставлять без присмотра, хранить в доступном месте;



- На электронном носителе (дискета, флеш-карта, CD), на котором расположены ключи ЭЦП, не должно быть **другой информации**;
- Хранение закрытого ключа ЭЦП на жёстком диске **НЕДОПУСТИМО**.
- Для просмотра выписки использовать систему **"Выписка on-line"**, не требующую использования ключей ЭЦП.
- По истечении срока действия ключа ЭЦП, необходимо провести его плановую замену.
- Настоятельно не рекомендуется использовать компьютер, на котором установлена система ДБО для выполнения поиска в сети интернет, посещения развлекательных и прочих ресурсов, официальный владелец которых не известен или не вызывает доверия.
- Работа с системой ДБО с гостевых рабочих мест (интернет-кафе и т.д.) значительно увеличивает риск хищения и дальнейшего неправомерного использования ключей ЭЦП и другой аутентификационной информации.

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

- Сменить пароль доступа;
- Произвести регенерацию ключей ЭЦП при содействии сотрудников Банка.

**Для дополнительной защиты Ваших денежных средств настоятельно рекомендуем как можно чаще контролировать состояние счёта (путем просмотра выписки) при помощи систем "Выписка on-line" или "Телефон-Клиент".**

**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 «Банк-Клиент» по неизвестным причинам.

Обращаем Ваше внимание, что **своевременное** обращение в Банк позволит принять оперативные меры по предотвращению мошенничества. Сотрудники Отдела автоматизации готовы оказать помощь по вопросам соблюдения требований безопасности при работе в сети Интернет и использования систем ДБО «Клиент-Банк» и «Интернет-Клиент».