

Рекомендации пользователям систем дистанционного банковского обслуживания Клиент-Банк (« Internet-Bank»)

В связи с участвовавшими случаями мошенничества с применением интернет-технологий, ООО «Хакасский муниципальный банк» настоятельно рекомендует Вам выполнять следующие несложные правила при работе в сети Интернет и в системе Клиент-банк.

Общие рекомендации по обеспечению информационной безопасности при использовании сети Интернет.

- Своевременно обновляйте операционную систему и используемое для работы в сети Интернет программное обеспечение (браузеры; почтовые клиенты и пр.).
- При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Установите на компьютере и регулярно обновляйте антивирусное программное обеспечение.
- Необходимо понимать, что ни один антивирус не может обеспечить 100% защиты. В целях увеличения вероятности обнаружения вирусов рекомендуем параллельно с установленным антивирусом использовать бесплатные утилиты для проверки вашего компьютера от других производителей антивирусного ПО.
- Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов. Проверку дополнительными утилитами рекомендуется осуществлять сразу после окончания такой проверки.
- Если у вас возникли подозрения на наличие вирусов на вашем компьютере (неожиданные перезагрузки, зависания, сетевая активность, нарушения связи и пр.), воздержитесь от работы в системе «Internet-Bank» на данном компьютере до проведения полной антивирусной проверки.
- Используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.
- При работе в сети Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.
- Постарайтесь воздержаться от использования программ онлайн-общения (таких, как ICQ, Skype и пр.) на компьютере, используемом для работы в системе «Клиент-Банк».
- Не подключайте к компьютеру внешние накопители данных (USB-флешки, внешние жесткие диски), которые подключались к компьютерам, для которых, возможно, не применяются необходимые меры безопасности.
- На компьютере, используемом для работы в системе «Клиент-Банк», не должно быть учетных записей (пользователей) без пароля. Выбирая пароль для учетной записи, постарайтесь сделать его сложным.
- Исключите обращения к Интернет-ресурсам под пользователем, обладающим правами администратора операционной системы.
- В качестве дополнительной меры компьютеры, используемые для работы в «Клиент-банке» не рекомендуется включать в локальные сети организации.
- Если вы утратили сотовый телефон, используемый Вами для получения одноразовых смс-паролей, либо утратили выданное Банком устройство (OTP-Token, MAC-Token), необходимо незамедлительно сообщить об этом Банку в письменном виде, либо по телефону, с сообщением блокировочного слова, указанном в Договоре на обслуживание Клиента по системе «Клиент-Банк» («Internet-Bank»).
- Если Вы обнаружили в сети Интернет ложный Web-сайт ООО «Хакасский муниципальный банк», отличный от <https://ibank2.kbhmb.ru>, <http://www.kbhmb.ru>, просим Вас незамедлительно сообщить об этом сотрудникам Банка. Категорически запрещается проводить какие-либо операции с помощью таких Web-сайтов.

- Сотрудники ООО «Хакасский муниципальный банк» никогда не запрашивают по телефону, по электронной почте или в СМС-сообщениях следующие данные: реквизиты банковской карты (номер карты и срок ее действия, CVV-код, ПИН-код), пароли от системы «Internet-Bank», одноразовые пароли. Если вы получили подобное сообщение, или вам позвонили с подобными вопросами, просьба незамедлительно сообщить об этом сотрудникам Банка.

Рекомендации по обеспечению информационной безопасности при работе в системе «Internet-Bank».

ЭП – это юридически значимый аналог Вашей собственноручной подписи. Как следствие этого, вопрос хранения ключа ЭП является **очень важным**.

С целью уменьшения риска потери ключа ЭП рекомендуется придерживаться следующих несложных правил:

- Носитель (дискета, USB-флешка и пр.) с ключом ЭП нельзя передавать третьим лицам, оставлять без присмотра, хранить в общедоступном месте.
- Хранение ключа ЭП на жёстком диске недопустимо.
- Никогда не оставляйте рабочее место без присмотра если запущена система «Internet-Bank» (осуществлен вход в систему).
- Сразу после окончания работы в системе «Internet-Bank» извлекайте из компьютера носитель с ключом ЭП.
- Контролируйте состояние счета (путем просмотра выписки) и при обнаружении подозрительных операций незамедлительно обращайтесь в банк для их отмены и блокирования ключей проверки ЭП.
- Обращайте внимание на дату и время последнего входа в систему (данные фиксируются на странице после входа в систему).
- В случае компрометации или подозрения на компрометацию следует немедленно произвести замену ключа ЭП. В качестве события, рассматриваемого как компрометация ключа, может выступать как потеря ключевого носителя (даже с последующим обнаружением), так и увольнение или смена лиц, допущенных к этим ключам.
- В случае использования системы «Internet-Bank» с публичных компьютеров (библиотека, Интернет-кафе) риск хищения и последующего неправомерного использования ключа ЭП и другой аутентификационной информации (имя / пароль) **значительно** возрастает.
- Используйте встроенный в систему «iBank 2» механизм SMS-информирования клиентов о входе в систему, поступлении документов, движении денежных средств по счетам, который настраивается на стороне Клиента при подключенной услуге «SMS-banking».

Просим Вас незамедлительно обращаться в Банк при возникновении следующих ситуаций:

- В выписке обнаружены несанкционированные Вами расходные операции.
- Утерян или похищен ключевой носитель с ключом ЭП.
- У Вас не работает система «Internet-Bank» по неизвестным причинам.

Телефоны для связи:

По техническим вопросам: +7(983)370-25-16

По вопросам регистрации или блокировки ключей: +7(983)370-18-48, +7(913)545-86-41

По вопросам прохождения платежей: +7(983)370-05-52

Обращаем Ваше внимание, что **своевременное** обращение в Банк позволит принять оперативные меры по предотвращению мошенничества.