

Рекомендации для клиентов по информационной безопасности при работе с Системой дистанционного банковского обслуживания

В целях повышения безопасности работы в системе дистанционного банковского обслуживания (далее – Система ДБО) КМ «Профильный Банк» (АО) (далее – Банк) обращает Ваше внимание на необходимость соблюдения мер предосторожности, которые повысят уровень Вашей информационной и финансовой безопасности.

С целью минимизации рисков доступа третьих лиц к работе с Системой ДБО, а также совершения операций, соответствующих признакам перевода денежных средств без добровольного согласия Клиента, Банк настоятельно рекомендует придерживаться приведенных ниже правил:

- ❖ Для хранения файлов с ключами электронной подписи (далее – Ключ ЭП) использовать специализированные ключевые носители (USB-токены). При этом владелец USB-токена должен хранить его в условиях, исключающих доступ к нему третьих лиц, например, в личном сейфе. Не хранить PIN-код/пароль доступа к Ключу ЭП вместе с USB-токеном и не записывать его на самом носителе

- ❖ Подключить услугу «SMS-подтверждения», позволяющую подтверждать платежные поручения с помощью кода подтверждения, который направляется в виде SMS-сообщения на номер мобильного телефона, указанный в анкете Клиента/представителя Клиента.

- ❖ Ограничить доступ к системе ДБО, указав список компьютеров (IP – адресов), с которых Клиент будет производить работу в Системе ДБО. Данное ограничение позволяет быть уверенным в том, что информация, передаваемая в Банк, будет обработана только в случае совпадения IP - адреса передающего компьютера с IP – адресом Клиента, хранящимся в базе данных Банка.

- ❖ Не допускать использования простых паролей, например, 123456, qwerty, и т.д. для учетных записей, используемых для входа в операционную систему. Осуществлять периодическое изменение паролей, рекомендуемая периодичность изменения паролей не реже 1 (одного) раза в месяц. Использовать сложные пароли длиной не менее 12 символов, включающие заглавные и строчные буквы, цифры и специальные знаки; не использовать один и тот же пароль для разных систем и не передавать его третьим лицам.

- ❖ Не передавать Ключи ЭП своим сотрудникам для проверки работы Системы ДБО и проверки настроек взаимодействия с Банком. При необходимости проведения такой проверки владелец Ключа ЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к Ключу вводится в интерфейс клиентского АРМа Системы ДБО, и ввести пароль, исключая умышленное наблюдение посторонними лицами.

- ❖ Не передавать Ключи ЭП замещающим сотрудникам (заместителям, временно исполняющим обязанности). Для таких сотрудников необходимо получить персональные Ключи ЭП.

- ❖ При увольнении сотрудника, имевшего доступ к Ключу ЭП, обязательно заблокировать его Ключ ЭП.

- ❖ Отключать и извлекать USB-токен с Ключом ЭП из компьютера, если работа в Системе ДБО не производится. USB-токен с Ключом ЭП должен находиться в компьютере только в момент подписания документов и работы в Системе ДБО и извлекаться сразу после подписания.

- ❖ Выделить отдельный компьютер, который будет использоваться только для работы с Системой ДБО, и не использовать его для других задач.

- ❖ Ограничить доступ к компьютерам, используемым для работы с Системой ДБО, и исключить доступ к ним персонала, не работающего с Системой ДБО. Настроить блокировку экрана при отсутствии пользователя на рабочем месте и запретить автоматический вход в операционную систему.

- ❖ При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль за выполняемыми ими действиями.
- ❖ На компьютерах, используемых для работы с Системой ДБО, исключить посещение интернет-сайтов сомнительного содержания. По возможности полностью запретить все соединения с информационно–телекоммуникационной сетью «Интернет» (далее – сеть Интернет), разрешив только доступ к необходимым ресурсам.
- ❖ Использовать только лицензионное программное обеспечение, обеспечив автоматическое обновление системного и прикладного программного обеспечения.
- ❖ Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечив возможность автоматического обновления антивирусных баз, а также проведение еженедельной полной антивирусной проверки.
- ❖ Осуществлять антивирусную проверку любых файлов, загружаемых из сети Интернет, полученных по электронной почте или с внешних носителей (дискеты, флеш-накопители, CD/DVD и др.). Не подключать к компьютеру ДБО неизвестные USB-устройства.
- ❖ Не допускать работу в операционной системе под учетной записью, имеющей права администратора. Необходимо использовать учетную запись с ограниченными правами в операционной системе, установленной на компьютере.
- ❖ Запрещать использование любых средств удаленного (дистанционного) доступа, которые обычно используются ИТ-специалистами для удаленной поддержки. Заблокировать возможность использования таких средств с помощью файрвола (программного и/или аппаратного).
- ❖ При возникновении подозрений на несанкционированное использование Ключей ЭП или на наличие в компьютере вредоносных программ – обязательно обратиться в Банк для блокировки Ключей ЭП.
- ❖ Если Вы заметили проявление необычного поведения программного обеспечения Системы ДБО или какие-либо изменения в интерфейсе программы, позвоните в Банк и выясните, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – обратитесь в Банк для блокировки Ключей ЭП. Банк обращает внимание на следующее:
 - ✓ Банк не имеет доступа к Вашим Ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным поручением;
 - ✓ Банк не осуществляет рассылку электронных писем с просьбой прислать Ваш Ключ ЭП или пароль;
 - ✓ Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. В случае если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление Ключей ЭП/паролей, необходимо незамедлительно сообщить об этом в Банк.
 - ✓ Ответственность за конфиденциальность Ваших Ключей ЭП лежит на Вас как на единственных владельцах Ключей ЭП;
 - ✓ Если Вы сомневаетесь в конфиденциальности своих Ключей ЭП или есть подозрение на их компрометацию (несанкционированном использовании), Вы должны незамедлительно заблокировать Ваши Ключи ЭП;
 - ✓ Изменение пароля доступа к Ключу ЭП не защищает Вас от использования злоумышленниками Вашего Ключа ЭП, если они ранее уже получили дистанционный доступ к Вашему компьютеру.

Для получения дополнительной информации по техническим вопросам Вы можете обратиться в Банк: +7 (495) 646-73-22, или по электронной почте dbo_support@profilbank.ru.

