Памятка по информационной безопасности в системе дистанционного банковского обслуживания (ДБО)

ООО КБ «Кредитинвест»

В связи с участившимися попытками злоумышленников получения доступа к системам дистанционного банковского обслуживания (ДБО) и проведения несанкционированных финансовых операций, Банк считает необходимым соблюдать приведенные ниже рекомендации по информационной безопасности в системе ДБО:

1. Использовать для хранения файлов с секретными ключами ЭЦП **только** отчуждаемые носители: дискеты, флеш-диски, специализированные устройства – USB-токены «iBank 2 Key».

2. Отключать, извлекать носители с ключами ЭЦП, если они не используются для работы с ДБО.

3. Никому не сообщать пароли для работы в системе ДБО, включая сотрудников Банка. Банк Никогда не обратится к Вам для получения подобной информации. Если к Вам обращаются от имени Банка с просьбой сообщить пароли – немедленно информируйте об этом факте службу поддержки Банка.

4. Ограничить доступ к компьютерам, используемым для работы с ДБО. Исключить доступ к компьютерам персонала, не имеющего отношения к работе с ДБО.

5. На компьютерах, используемых для работы с ДБО, исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т. п.

6. Не рекомендуется устанавливать на компьютерах, используемых для работы с ДБО, иное программное обеспечение, кроме необходимого для работы в системе ДБО.

7. Используйте только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечьте автоматическое обновление системного и прикладного ПО. Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера Вашего компьютера, что значительно повысит его уровень безопасности.

8. Установить и настроить персональный брандмауэр (firewall) на Вашем компьютере. Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа.

9. Применяйте на рабочем месте лицензионные средства антивирусной защиты, обеспечьте возможность автоматического регулярного обновления антивирусных баз. Действие вирусов может быть направлено на перехват Вашей персональной информации и передаче её злоумышленникам.

10. Применяйте на рабочем месте специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.

11. Исключите обслуживание компьютеров, используемых для работы с ДБО, нелояльными ИТ-сотрудниками.

12. При обслуживании компьютера ИТ-сотрудниками – обеспечивайте контроль за выполняемыми ими действиями. Не привлекайте для администрирования и обслуживания компьютера с Системой ДБО технических специалистов на условиях предоставления им удаленного доступа к компьютеру.

13. Не рекомендуется осуществлять платежи за час до окончания операционного времени в пятницу и в предпраздничные дни

14. Права пользователя, работающего с системой ДБО, на данном компьютере должны быть минимально необходимыми (наличие администраторских прав нежелательно).

15. В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО Банка, обратитесь в службу поддержки Банка, отложив при этом

совершение операций.

16. В случае сбоев в работе компьютера или его поломки во время работы с системой ДБО или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует НЕМЕДЛЕННО обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.

17. Никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы системы ДБО, проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа системы ДБО, и лично ввести пароль, исключая его подсматривание.

18. При увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭЦП, обязательно позвонить в банк и заблокировать ключ ЭЦП.

19. При увольнении сотрудника, имевшего технический доступ к секретному ключу ЭЦП, обязательно позвонить в банк и заблокировать ключ ЭЦП.

20. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой ДБО, принять меры для обеспечения отсутствия вредоносных программ на компьютерах.
21. При возникновении любых подозрений на компрометацию (копирование) секретных ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить в банк и заблокировать ключи ЭЦП.

22. Если Вы заметили проявление необычного поведения ПО системы ДБО или какие-то изменения в интерфейсе программы – нужно незамедлительно позвонить в банк и выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет – заблокировать ключи ЭЦП.

23. Категорически не рекомендуется работать с системой ДБО с недоверенных компьютеров (интернет- кафе и т.п.), так как это существенно увеличивает риск кражи Ваших учетных и ключевых данных.