Памятка пользователя ДБО подсистемы "Интернет-Клиент"

О мерах по пресечению хищения и использования секретных ключей ЭЦП

АО «Эксимбанк Казахстан» (далее – Банк) информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования секретных ключей ЭЦП и о необходимости ограничения доступа к персональным компьютерам, на которых используется ДБО подсистема «Интернет-Клиент».

Чтобы воспрепятствовать хищению и использованию Вашего секретного ключа ЭЦП злоумышленниками, требуется придерживаться приведенных ниже правил и рекомендаций:

1. Использовать отдельный компьютер для работы только с подсистемой "Интернет-Клиент".
2. Использовать для хранения файлов с секретными ключами ЭЦП отчуждаемые носители: JavaToken
3. Использовать надежные, сложные пароли, содержащие различные буквы, цифры и спецсимволы (например, знаки препинания), а также сочетания заглавных и строчных букв. Рекомендуемая длина пароля – не менее 8 символов. Не используйте учетные записи с «пустыми» паролями.
4. Отключать, извлекать носители с ключами ЭЦП, если они не используются для работы с подсистемой "Интернет-Клиент".
5. Ограничить доступ к компьютеру, используемому для работы с подсистемой "Интернет-Клиент". Исключить доступ к компьютеру персонала, не имеющего отношения к работе с подсистемой "Интернет-Клиент".
6. На компьютере, используемом для работы с подсистемой "Интернет-Клиент", исключить посещение глобальной сети интернета.
7. Обязательно использовать лицензионного ПО (операционные системы, офисные пакеты и пр.).
8. Применять на рабочем месте лицензионные средства антивирусной защиты. Обеспечить возможность автоматического обновления антивирусных баз.
9. Применять на рабочем месте специализированные программные средства безопасности: персональный сетевой экран (Firewall), антишпионское программное обеспечение и т.п.
10. Запрещается передавать ключи ЭЦП ИТ-сотрудникам для проверки работы подсистемой "Интернет-Клиент", проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен подключить носитель к компьютеру.
11. При увольнении сотрудника, имевшего технический доступ к секретному ключу ЭЦП, обязательно произвести внеплановую смену ключей ЭЦП.
12. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютера, используемого для работы подсистемой "Интернет-Клиент", принять меры для проверки вредоносных программ на компьютерах.
13. При возникновении любых подозрений на компрометацию секретных ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно связаться с ответственным сотрудником Банка и заблокировать ключи ЭЦП.
14. Если Вы заметили проявление необычного поведения подсистемой "Интернет-Клиент" или какие-то изменения в интерфейсе программы – позвонить ответственному сотруднику в Банк и выяснить, не связаны ли такие изменения с обновлением версии.
15. В случаи потери носителя с секретными ключами ЭЦП немедленно связаться с ответственным сотрудником Банка и заблокировать ключи ЭЦП.