Памятка по обеспечению информационной безопасности

при использовании системы ДБО BS-Client v.3

1. Обмен информацией между Банком и Клиентом осуществляется с применением средств криптографической защиты информации (далее - СКЗИ), реализующих электронную цифровую подпись (ЭЦП). Данным СКЗИ является Message Pro, на основании алгоритмов которого осуществляется работа с криптографическими ключами во время сеанса работы в системе.

2. Программное обеспечение (ПО) устанавливается и используется согласно инструкции, выдаваемой Банком при подключении Клиента к системе ДБО.

3. Доступ к информации для входа в систему ДБО (логин/пароль), криптографическим технологическим ключам и ключам ЭЦП должен быть строго ограничен. Компрометация (утеря; ознакомление посторонних лиц; бесконтрольный доступ сотрудников организации, не связанных с использованием системы ДБО) указанных данных может привести к утечке конфиденциальной информации о деятельности организации Клиента, а также к хищению денежных средств. Рекомендуется располагать ключевую информацию на съёмном носителе.

4. Рабочее место пользователя (РМП) системы ДБО должно быть обеспечено надежной парольной защитой для запуска операционной системы (ОС). Пароль рекомендуется использовать длиной не менее 8 символов, с использованием букв в верхнем и нижнем регистре, цифр, а также специальных символов (!, @ и т.д.). Должна быть настроена блокировка экрана с запросом пароля (при времени простоя более 20 минут).

5. На РМП должно быть установлено только необходимое лицензионное ПО. Нелицензионное ПО может содержать программные закладки, вирусы или вредоносный код, о которых конечный пользователь может не иметь представления и не замечать во время работы в системе, однако все его действия могут фиксироваться и передаваться злоумышленнику. Следует устанавливать все доступные обновления для используемого ПО.

6. На РПМ должно быть установлено лицензионное антивирусное ПО, настроенное на автоматическое обновление антивирусных баз и программных модулей. Обязателен постоянно работающий модуль контроля работающих и запускаемых программ. Перед установкой новых программ следует производить проверку инсталляционных пакетов антивирусным средством. Следует использовать функцию фильтрации трафика Интернет-соединений. При наличии встроенного брандмауэра – ограничить количество разрешенных портов ОС для работы в локальной сети и сети Интернет.

7. На РМП должен вестись контроль учетных записей, обладающих правами «Администратора» в ОС. Количество таких учетных записей должно быть сведено к минимуму. Учетная запись пользователя системы ДБО должна обладать лишь необходимым уровнем прав для нормальной работы в ОС.

8. Перегенерация ключа ЭЦП должна производиться лично пользователем системы ДБО, либо при консультировании сотрудником отдела поддержки системы ДБО Банка. Ознакомление с процедурой перегенерации посторонних лиц должно быть исключено.

9. Доступ в помещение, в котором установлено РМП с системой ДБО, должен быть ограничен. Помещение в ночное время должно ставится под охрану.

10. Не допускается:

- снимать несанкционированные копии с ключа ЭЦП;

- знакомить с логином/паролем лиц, не допущенных к работе со счетом организации;

- записывать на съёмный носитель, содержащий ключевую информацию, посторонние данные;

- оставлять съёмный носитель в РМП при завершении работы в системе ДБО;

- оставлять систему ДБО без внимания при удачном входе.

11. При компрометации (или подозрении на компрометацию) следует незамедлительно обратиться в Банк, предпринять все необходимые меры по прекращению любых операций с использованием скомпрометированного ключа ЭЦП.

12. При увольнении или переводе на другую должность сотрудника, ответственного за работу в системе ДБО, следует произвести внеплановую смену ключа ЭЦП.