Требования и рекомендации
по обеспечению информационной безопасности при обмене ЭД

1. Следует исключить доступ лиц, не уполномоченных для работы с Системой ДБО, к компьютеру, предназначенному для работы по ее использованию.
2. Доступ неуполномоченных лиц к компьютеру, предназначенному для работы с Системой ДБО, должен быть исключен как путем физической изоляции компьютера, так и использованием программной (аппаратно-программной) системы разграничения доступа. При использовании Системы ДБО разграничения доступа должен исключаться доступ неавторизованного пользователя, как к компонентам Системы, так и к компонентам и разделам операционной системы компьютера, а также любого другого программного обеспечения.
3. Следует исключить доступ неуполномоченных лиц к ключевой информации (паролям, ключам шифрования, ключам ЭП), используемой для обеспечения функционирования Системы ДБО. Порядок хранения и использования носителей ключевой информации должен исключать возможность доступа к ним без гарантированного обнаружения факта несанкционированного доступа. Носитель ключевой информации должен быть доступен для программного обеспечения компьютера, предназначенного для работы с Системой ДБО, только в момент работы с данной Системой.
4. При использовании Системы ДБО следует запретить доступ к внешним Интернет-ресурсам (сайтам), непосредственно не связанным с работой Системы. Необходимо оснастить компьютер актуальной системой обнаружения и блокирования попыток несанкционированного сетевого доступа к ресурсам компьютера (персональный межсетевой экран и антивирусное программное обеспечение).
5. Запрещается генерировать или выполнять любые действия над ключами ЭП или их носителями на любых компьютерах, за исключением компьютера Клиента – владельца ЭП, предназначенного для работы с Системой ДБО.
6. Запрещается передавать ключи ЭП сотрудникам Банка, под каким бы то ни было предлогом. О любых подобных попытках следует немедленно извещать Банк. Если же вследствие существенных обстоятельств (тестирование, выявление причин некорректного функционирования Системы ДБО) такая необходимость все же возникнет, то необходимо сгенерировать новую пару ключей и при регистрации сделать соответствующую запись в обоих экземплярах Сертификата ключа проверки ЭП и максимально ограничить срок его использования и перечень полномочий. Действующие ключи ЭП не могут быть переданы ни при каких условиях.
7. При наступлении следующих событий:
- утеря носителя ключевой информации с последующим обнаружением или без;
- обнаружение факта несанкционированного доступа к носителю ключевой информации;
- увольнение сотрудников, имевших доступ к носителям ключевой информации;
Ключи ЭП клиента считаются скомпрометированными и подлежат немедленному выводу из обращения.
8. Следующие события рассматриваются как предпосылки к возможному доступу неуполномоченных лиц к ключевой информации:
- нарушение правил хранения и использования носителей с ключами ЭП;
- возникновение каких-либо подозрений на утечку информации;
- обнаружение нарушения целостности программного обеспечения на компьютере, используемом в Системе ДБО;
- обнаружение вредоносного программного обеспечения на компьютере, используемом в Системе ДБО;
- обнаружение нарушения целостности топологии локальной сети клиента, временное или постоянное;
- обнаружение попыток сетевых атак на компьютер, предназначенный для работы с Системой ДБО.

В данном случае также рекомендуется произвести смену ключей ЭП и другой ключевой информации.

Следование вышеизложенным правилам полностью находится под ответственностью Клиента. Если при расследовании спорных инцидентов будет установлено их нарушение Клиентом, Банк оставляет за собой право безусловно возложить на Клиента ответственность за возникновение инцидента и соответствующий ущерб.