ООО «Инбанк» версия от 01.07.2012

ПАМЯТКА
по обеспечению безопасности использования электронной подписи

1. В настоящем документе используются термины, определения и сокращения, применяемые в «Договоре об обмене документами с клиентом - физическим лицом в электронном виде с использованием электронной подписи».
2. Порядок использования электронных подписей устанавливается «Договором об обмене документами с клиентом - физическим лицом в электронном виде с использованием электронной подписи», заключаемом между Клиентом и Банком.
3. Для предотвращения риска искажения передаваемой в Банк по системе ДБО информации, а также рисков несанкционированного использования электронной подписи Клиента, Банком рекомендуется:

3.1. На рабочие места для доступа к системе ДБО должны быть установлены специализированные программные средства безопасности: персональные межсетевые экраны, антивирусное программное обеспечение и т.п.

3.2. Исключить доступ третьих лиц к информации, позволяющей получить несанкционированный доступ к использованию электронной подписи Клиента.

3.3. Хранить пароль для доступа в систему ДБО, пароль для доступа к ключу электронной подписи, ключ электронной подписи, а также коды и пароли, используемые в качестве простой электронной подписи, в недоступном для третьих лиц месте.

3.4. Не передавать третьим лицам пароль для доступа в систему ДБО, пароль для доступа к ключу электронной подписи, ключ электронной подписи или коды и пароли, используемые в качестве простой электронной подписи. При необходимости проверки работы системы ДБО, изменении настроек пользователя и пр. на рабочем месте Клиента, пароль для доступа в систему ДБО, пароль для доступа к ключу электронной подписи, ключ электронной подписи, а также коды и пароли, используемые в качестве простой электронной подписи, должны применяться только лично их владельцем.

3.5. Немедленно обратиться в Банк для блокировки доступа в систему ДБО и для отзыва сертификата ключа проверки подписи, если пароль для доступа к ключу электронной подписи или ключ электронной подписи утрачены или имеется подозрение, что они оказались у посторонних лиц. **Изменение пароля доступа к ключу электронной подписи не защищает от использования злоумышленником ранее похищенного ключа.**

3.6. Использовать для хранения файлов с ключами электронной подписи отчуждаемые носители: дискеты, флеш-диски, токены.

3.7. Отключать, извлекать носители с ключами электронной подписи после завершения работы с системой ДБО.

3.8. Для подключения к системе ДБО с гостевых рабочих мест (интернет-кафе и т.д.), использовать дополнительно сформированный ключ электронной подписи с

установленными лимитами на суммы совершаемых операций и ограниченным доступом к счетам.

3.9. При утрате или хищении телефона, номер которого используется Банком для идентификации Клиента и в качестве контактного номера телефона, самостоятельно заблокировать в системе ДБО возможность взаимодействия с Банком посредством кодов и паролей, используемых в качестве простой электронной подписи.

4. Перечень рекомендаций, приведенных в настоящем документе, не является исчерпывающим. Клиент обязан выполнять иные действия по предотвращению компрометации информации, используемой для идентификации Клиента Банком, в том числе при взаимодействии с осуществляемого с помощью системы ДБО.
5. Игнорирование или неполное следование рекомендациям, указанным в настоящем документе, может привести к хищению и использованию злоумышленниками пароля для доступа в систему ДБО, пароля для доступа к ключу электронной подписи, ключа электронной подписи или кодов и паролей, используемых в качестве простой электронной подписи.