Приложение 8
к Соглашению о предоставлении
услуг электронного документооборота
в АО "Промэнергобанк"

Памятка
по мерам защиты информации при работе в системе ДБО

В целях минимизации риска несанкционированного доступа к системе ДБО от имени Клиента, несанкционированного списания средств с расчетных счетов Клиента рекомендуется применение следующих организационных мер и технических средств защиты информации:

1. Для АРМ Клиента, на котором установлена клиентская программа системы ДБО или производится работа с системой ДБО через веб-браузер:

- На компьютере должно быть установлено и включено антивирусное ПО, база сигнатур которого должна регулярно (не реже раза в неделю) обновляться; рекомендуется также регулярная (раз в неделю) полная проверка компьютера на наличие вредоносного кода (вирусов, троянских программ, и т.д.).
- На компьютере должен быть включен брандмауэр Windows (если не используются другие средства защиты подключения к сети как, например, межсетевой экран антивирусного ПО Kaspersky Internet Security).
- На компьютер не следует устанавливать средства удаленного управления (RAdmin, VNC, и прочие), средство «Удаленный рабочий стол» Windows должно быть отключено.
- Не следует устанавливать на компьютер программное обеспечение, не требуемое для работы, особенно загруженное из Интернет.
- Все учетные записи пользователей должны иметь пароль, рекомендуемая длина пароля – не менее 6 символов.
- Если компьютер находится в локальной сети - не рекомендуется разрешать общий доступ к локальным дискам компьютера, также желательно запретить входящие подключения из Интернет к этому компьютеру средствами используемого маршрутизатора/межсетевого экрана.
- Рекомендуется ограничить исходящие подключения к Интернет только необходимыми адресами (адресами проверенных сайтов, серверов банков, с которыми ведется работа).

2. При работе с системой ДБО:

- При подключении к специализированному сайту банка для работы в системе ДБО онлайн убедиться, что соединение установлено по протоколу https: и защищено действующим сертификатом. Сертификат должен быть выдан на имя JSC Promenergobank и для сайта ibank.promenergobank.ru. Если сертификат недействителен, или не соответствует названию сайта, - веб-браузер выдаст предупреждение об этом при подключении. В этом случае необходимо немедленно прекратить подключение к системе ДБО, и обратиться в службу поддержки Банка.
- Вставлять дискету (подключать flash-накопитель, токен) с ключевой информацией только на время работы с Системой.
- Хранить носители ключей ЭП в недоступном для посторонних лиц месте (сейфе, запираемом ящике).
- Если Клиент имеет более одного ключа ЭП (например, 1-я и 2-я подпись) – не объединять ключевую информацию на одном носителе.
- В случае компрометации ключей (наличие подозрений или конкретных фактов получения доступа посторонних лиц) необходимо незамедлительно сообщить об этом в Банк любым доступным способом.
- При подозрительной и нестандартной работе компьютера, на котором используется система ДБО (например, невозможность запуска или непонятные ошибки в работе ПО, отсутствие связи с банком) рекомендуется сообщить об этом в службу поддержки Банка.

Служба поддержки банка – тел. (8172) 59-74-55