БАНК САНКТ-ПЕТЕРБУРГ

Требования по информационной безопасности при установке и эксплуатации системы ДБО

Уважаемый Клиент!

В последнее время по данным МВД участились случаи несанкционированного списания средств с расчетных счетов организаций путем получения злоумышленниками доступа к программному обеспечению и ключам электронной подписи (ЭП) систем дистанционного банковского обслуживания, в том числе через сеть Интернет.

Обязанность по обеспечению защиты от несанкционированного доступа к ключам ЭП и к установленному в Вашей организации программному обеспечению Системы, в соответствии с Договором возлагается на Вас.

Выполнение настоящих требований по информационной безопасности позволит обеспечить защиту информационного обмена Вашей организации с Банком и минимизировать риски возможных финансовых потерь.

1. Рабочие ключи ЭП должны формироваться Уполномоченными лицами организации самостоятельно. Файлы с ключами ЭП необходимо хранить на внешних носителях (токен, флешка, компакт-диск и т.п.), и подключать носитель к компьютеру только на время работы с Системой. Самым безопасным ключевым носителем из перечисленных является токен с неизвлекаемыми ключами ЭП, информацию с которого нельзя скопировать.

2. Носители с ключами ЭП должны храниться исключительно у лиц, имеющих право подписи документов, и использоваться ими только при подписании электронных документов в Системе. В нерабочее время носители с ключами ЭП необходимо хранить в сейфе или ином месте, исключающем несанкционированный доступ к ним.

3. Необходимо ограничить доступ в помещение, в котором установлен компьютер с Системой, и доступ к самому компьютеру. Покидая рабочее место, обязательно блокируйте компьютер и извлекайте внешний носитель с ключами.

4. Требуется обеспечить конфиденциальность паролей, используемых для доступа в Систему. Используйте сложные пароли, осуществляйте их периодическую смену. Если возникло подозрение, что пароли стали известны неуполномоченному лицу, незамедлительно смените пароль.

5. В случае изменения состава должностных лиц, обладающих правом электронной подписи (или увольнении ответственных исполнителей, имевших доступ к ключам ЭП), необходимо в кратчайшие сроки подать в банк заявление на прекращение действия ключей ЭП, принадлежащих данным лицам. Необходимо также произвести смену паролей для доступа в Систему, которые были известны этим лицам.

6. Рекомендуем ограничить доступ в сеть Интернет с компьютера, который используется для работы в Системе, оставив возможность подключения только к серверам банка. Доступ ко всем другим сайтам с рабочего компьютера должен быть закрыт. Доступ к данному компьютеру из сети Интернет также должен быть закрыт.

7. На компьютере, используемом для работы в Системе, должно быть установлено и регулярно обновляться антивирусное программное обеспечение.

8. В случае заражения вирусами или нарушения работоспособности компьютера, на котором установлена Система, необходимо связаться со службой технической поддержки и обратиться в обслуживающее подразделение для подачи заявления о приостановлении обслуживания по Системе.
Контакты службы технической поддержки: e-mail: sbk@bspb.ru, телефоны: Санкт-Петербург: (812) 329 5939, для регионов 8 800 500 5939 (по России звонок бесплатный) с 8-00 до 20-00 по рабочим дням, время работы московское.

После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей доступа в Систему и произвести внеплановую смену ключей ЭП Уполномоченных лиц.

9. Немедленно информируйте Банк при выявлении несанкционированного доступа к Системе или несанкционированных платежей, отправленных по Системе, и инициируйте временную приостановку обслуживания по Системе.

10. Поддерживайте актуальность номеров телефонов для SMS-авторизации. При изменении номеров телефонов предоставьте в Банк дополнительное Заявление по форме Приложения 1 к Правилам.

11. В случае утраты телефона, на который приходят SMS-сообщения с одноразовыми паролями, обеспечьте немедленную блокировку номера телефона у оператора сотовой связи и обратитесь в обслуживающее подразделение с просьбой временно приостановить возможность работы в Системе.

12. При поступлении на телефон Уполномоченного лица SMS-сообщений, свидетельствующих о попытке входа в Систему или подтверждения отправки документов, которых данное лицо не совершало, немедленно обратитесь в Банк и инициируйте временную приостановку работы по Системе.

13. Будьте внимательны и не поддавайтесь на обманные действия злоумышленников по хищению паролей: не сообщайте запрашиваемые по телефону, электронной почте Идентификатор (логин) и пароль/SMS-код, сотрудники Банка не имеют права запрашивать данную информацию.

14. Для подсистемы «Интернет – Клиент»:
- Вход с систему осуществляется только с сайта https://sbk.bspb.ru. Обращайте внимание, что в адресной строке браузера присутствует именно этот адрес, остерегайтесь похожих названий: dsbp.ru, bcpb.ru и т.д. Не вводите данных (Идентификатор, Пароль, SMS-код) на любых других сайтах.
- Настоятельно рекомендуется включить в браузере каждого Уполномоченного лица настройку проверки сертификата посещаемого сайта. При предупреждении браузера о недоверенном ресурсе не вводите Идентификатор и Пароль, этот ресурс может контролироваться злоумышленниками.
- Все объявления о проведении технических работ публикуются Банком на странице сайта до входа в Систему. Будьте внимательны, если после ввода Идентификатора, Пароля и SMS-кода и входа в систему вместо главного экрана Системы появляется сообщение о проведении технических работ, возможно, данное подключение перехвачено злоумышленниками, немедленно обратитесь в Банк и инициируйте временную приостановку работы по Системе.

Выполнение данных правил позволит минимизировать риски несанкционированного доступа к информации по счетам.