БАНК САНКТ-ПЕТЕРБУРГ

Требования по информационной безопасности при установке и эксплуатации системы ДБО

Уважаемый Клиент!

Обязанность по обеспечению защиты от несанкционированного доступа к установленному в Вашей организации программному обеспечению Системы «Интернет-банк i2B» и к ключам ЭП 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. Требуется обеспечить конфиденциальность паролей, используемых для доступа в Систему «Интернет-банк i2B». Используйте сложные пароли, осуществляйте их периодическую смену. Если возникло подозрение, что пароли стали известны неуполномоченному лицу, незамедлительно смените пароль.
2. Вход с систему необходимо осуществлять только с сайтов https://www.bspb.ru/ или https://i.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 аутентификационных данных на любых других сайтах.
3. При компрометации/подозрениях на компрометацию пароля/логина, ключей электронной (цифровой) подписи необходимо самостоятельно произвести смену пароля/логина, выполнить процедуру перегенерации ключей в Системе «Интернет-банке i2B» и обратиться в Службу технической поддержки или в подразделение Банка, по месту ведения счета, с соответствующим заявлением и заблокировать доступ к Интернет-банку i2B.
4. Для доступа в Систему «Интернет-банк i2B» рекомендуется использовать персональный компьютер только с лицензионным программным обеспечением.
5. На устройство (компьютер, ноутбук, планшет, смартфон и пр.), с которого осуществляется доступ в Систему «Интернет-банк i2B», должно быть установлено и регулярно обновляться антивирусное программное обеспечение.
6. Рекомендуется включить в браузере настройку проверки сертификата посещаемого сайта. При предупреждении браузера о недоверенном ресурсе не вводите свои аутентификационные данные (Логин, Пароль, Код), этот ресурс может контролироваться злоумышленниками.
7. Не рекомендуется использовать устройство, с которого осуществляется доступ в Систему «Интернет-банк i2B», для обычной работы в интернет.
8. В случае заражения вирусами или нарушения работоспособности компьютера, с которой осуществляется доступ в Систему «Интернет-Банк i2B», необходимо связаться со Службой технической поддержки и обратиться в обслуживающее подразделение для подачи заявления о приостановлении обслуживания по Системе «Интернет-Банк i2B».

   После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей доступа в Систему «Интернет-банк i2B» и произвести внеплановую смену ключей ЭП Уполномоченных лиц.Контакты Службы технической поддержки: e-mail: sbk@bspb.ru, телефоны: Санкт-Петербург: (812) 329 59 39, с 8-00 до 20-00 по рабочим дням, время работы московское.
9. Не рекомендуется использовать для доступа в Систему «Интернет-банк i2B» компьютеры в интернет-кафе и т.п.
10. Ежедневно проверяйте выписку по счетам организации.
11. Уполномоченному лицу не следует передавать мобильный телефон, используемый для получения Кодов, сторонним лицам. В случае утраты телефона необходимо немедленно заблокировать доступ к Системе «Интернет-банк i2B» путем обращения в Службу технической поддержки банка или в обслуживающее подразделение Банка.

12. Поддерживайте актуальность номеров телефонов Уполномоченных лиц для получения SMS-кодов. При изменении номеров телефонов предоставьте в Банк дополнительное Заявление по форме Приложения 1 к Правилам i2B.
13. Не следует сообщать Логин, Пароль, одноразовые коды третьим лицам, в том числе и работникам Банка. Работники Банка не вправе запрашивать подобную информацию. Если такие запросы приходят по электронной почте или SMS, это – мошенники.
14. Если на мобильный телефон Уполномоченного лица начали поступать сообщения от Банка с четырехзначными SMS-кодами для входа в Систему «Интернет-банк i2B» или осуществления операций в Системе «Интернет-банк i2B», не инициированные данным пользователем, необходимо немедленно сообщить об этом в Службу технической поддержки банка и произвести смену Идентификатора (логина) и Пароля для входа в Систему «Интернет-банк i2B».
15. При внезапном нарушении работоспособности компьютера, с которого осуществляется доступ в Интернет-Банк i2B, необходимо немедленно сообщить об этом в Службу технической поддержки банка и проверить санкционированность последних проведенных в Системе «Интернет-банк i2B» платежей.
16. Персонифицированные ключи ЭП должны формироваться Уполномоченными лицами организации самостоятельно. USB-токен с ключами ЭП необходимо подключать к компьютеру только на время работы в Системе «Интернет-банк i2B».
17. Покидая рабочее место, обязательно блокируйте компьютер и извлекайте USB-токен с ключами. в нерабочее время он должен храниться способом, исключающим несанкционированный доступ к нему.
18. Необходимо выключать компьютер, с которого осуществляется доступ в Интернет-Банк i2B, по окончании рабочего дня.
19. В случае изменения состава должностных лиц, обладающих правом электронной подписи (или увольнении ответственных исполнителей, имевших доступ к Системе «Интернет-Банк i2B» и ключам ЭП), необходимо в кратчайшие сроки подать в банк заявление на прекращение доступа к Системе «Интернет-Банк i2B» и действия ключей ЭП, принадлежащих данным лицам.

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