а) банк

банк
александровский

Рекомендации по информационной безопасности для пользователей системы дистанционного банковского обслуживания (ДБО) юридических лиц и индивидуальных предпринимателей

Обеспечение защиты от несанкционированного доступа к системе ДБО и ключам ЭП в вашей организации и соблюдение данных требований по информационной безопасности надежно защитит обмен данными вашей организации с Банком и сведет к минимуму риски финансовых потерь.

Внимание! При работе в системе ДБО существует риск несанкционированного доступа к вашим данным и управления вашим счётом мошенниками. Будьте осторожны и соблюдайте правила безопасности.

Основные угрозы безопасности в системе ДБО

1. Несанкционированный доступ к информации третьими лицами.

2. Вирусные атаки на систему ДБО с целью хищения финансовых средств.

3. Использование вредоносных программ для работы в системе от имени владельца счета.

Что такое электронная подпись (ЭП)?

ЭП — это информация, присоединенная к электронному документу, позволяющая идентифицировать подписавшего и выявлять любые изменения, внесенные в документ после его подписания. Для защиты от копирования используются специальные носители, доступ к которым защищен ПИН-кодом, известным только владельцу.

Основные меры по информационной безопасности

Безопасность при установке и эксплуатации системы ДБО

1. Конфиденциальность паролей:

- Используйте сложные пароли для доступа в систему «Интернет-банк BIFIT» и меняйте их регулярно.
- При подозрении на компрометацию пароля немедленно смените его.

2. Доступ только с доверенных сайтов:

- Входите в систему только с официальных сайтов банка, например, https://abank.ru или https://ibank.alexbank.ru/
- Проверяйте адресную строку браузера и избегайте сайтов с похожими названиями.

3. Меры при компрометации данных:

- В случае компрометации ключей ЭП или утери контроля над устройством с мобильным приложением - обратитесь в Службу технической поддержки для блокировки системы ДБО.

4. Использование лицензионного ПО:

- Доступ к системе ДБО должен осуществляться только с устройства с лицензионным программным обеспечением и регулярно обновляемым антивирусом.

5. Проверка сертификатов сайтов:

/ Используйте обновлённые версии браузеров, не отключайте проверку сертификатов в браузере и не вводите данные на недоверенных ресурсах.

6. Ограничение доступа к интернету:

/ Не используйте устройство для других интернет-активностей, не связанных с работой в системе ДБО.

7. Антивирусная защита:

/ На устройстве для доступа в систему ДБО должен быть установлен и обновляться антивирус.

8. Реагирование при сбоях:

/ В случае вирусного заражения устройства или сбоев в работе системы обратитесь в Службу технической поддержки и приостановите обслуживание в ДБО до устранения угроз.

9. Использование USB-токена с ключами ЭП:

/ Подключайте USB-токен только на время работы в системе. Храните токен в защищённом месте и извлекайте его по окончании работы.

Организационные меры по безопасности

1. Блокировка устройства:

/ При покидании рабочего места блокируйте компьютер и извлекайте носитель с ключами ЭП.

2. Контроль активности:

/ Регулярно проверяйте дату и время последнего входа в систему, выписки по счетам и проводимые операции.

/ При обнаружении в выписке по счету расходных операций, которые не были санкционированы Вами, незамедлительно обратитесь в банк.

3. Безопасность мобильных устройств:

/ Не передавайте мобильный телефон для получения SMS-кодов третьим лицам.

/ При потере телефона немедленно заблокируйте доступ к системе, обратившись в Службу технической поддержки банка.

4. Проверка информации об уполномоченных лицах:

/ Поддерживайте актуальность информации о сотрудниках, имеющих доступ к системе, и номеров телефонов для SMS-кодов.

5. Избегание фишинга:

/ Не сообщайте логин, пароль или коды третьим лицам, включая сотрудников банка, и не вводите данные по ссылкам из подозрительных писем или SMS.

6. Изменение состава ответственных лиц:

/ При изменении сотрудников, имеющих доступ к системе и ключам ЭП, немедленно уведомляйте банк и отзывайте доступы и ключи.

Своевременное выполнение этих мер позволит минимизировать риски несанкционированного доступа и финансовых потерь.