Важнейшим фактором, способствующим обеспечению безопасности, является личная заинтересованность Клиента. В системе дистанционного банковского обслуживания (далее – система ДБО) используются современные средства обеспечения информационной безопасности, направленные на то, чтобы сделать работу с системой максимально удобной при поддержании высокого уровня безопасности. Банк считает необходимым соблюдение Клиентами следующего комплекса мер по защите информации:

1. Осуществлять вход в Систему только через корпоративный сайт АО УКБ «Белгородсоцбанк» (https://bsbank.ru) или через сайт системы ДБО (https://ibank.belsocbank.ru).
2. Не осуществлять вход в систему в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, Интернет-кафе или общественный транспорт.
3. Права пользователя, работающего с системой ДБО, на данном компьютере должны быть минимально необходимыми (наличие прав администратора нежелательно).
4. Ни в коем случае не отвечать на письма, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену belsocbank.ru, прислать секретный ключ и пароль доступа к нему, или логин и пароль к нему, а немедленно сообщить о подобном факте в контакт-центр по информационной безопасности Банка в рабочие часы Банка по телефону: 8(4722)23-17-18. Банк напоминает, что ни при каких обстоятельствах не требует прислать секретный ключ электронной подписи (далее – ЭП) или пароль.
5. До входа в систему ДБО убедиться в том, что устройство (компьютер, смартфон, планшет), с которого осуществляется работа с системой, не заражен вирусами/вредоносным программным обеспечением (далее – ПО), установлено и работоспособно лицензионное антивирусное программное обеспечение, регулярно и своевременно обновляются антивирусные базы.
6. Не оставлять без присмотра систему в активном состоянии, не осуществив выход из системы специальной кнопкой «Выход». В случае бездействия Пользователя в течение 15 минут, в целях безопасности Банк автоматически завершит сеанс использования системы ДБО. Извлекать из компьютера съемный носитель, содержащий секретный ключ, сразу после завершения работы с системой ДБО.
7. Не записывать на носитель, содержащий секретный ключ, какую-либо другую информацию или секретные ключи от других систем.
8. Не пытаться создавать дубликат секретного ключа.
9. Обеспечить использование секретного ключа только Владельцем ключа ЭП.
10. Никогда не передавать носители ключей ЭП сотрудникам Банка для проверки работы системы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично Владелец ключа ЭП должен подключить съемный носитель с ключами к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского рабочего места системы ДБО и лично ввести пароль.
11. Хранить устройство, содержащее секретный ключ, в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя. Банк напоминает, что

Клиент несет ответственность за конфиденциальность секретных ключей ЭП для работы с системой ДБО.

12. Исключить доступ к устройствам, используемым для работы с системой ДБО, посторонним лицам и персоналу, не уполномоченному для работы с системой ДБО. Обеспечить контроль над действиями персонала, обслуживающего аппаратные средства для работы с системой ДБО.

13. На устройствах, используемых для работы с системой ДБО, исключить посещение всех Интернет-сайтов, кроме используемых для входа в систему ДБО, а также исключить установку развлекательных и игровых программ.

14. Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить своевременное обновление системного и прикладного ПО.

15. Во избежание несовместимости программного обеспечения на устройствах, используемых для работы с системой ДБО, исключить использование сторонних криптографических средств и устройств.

16. В случае выявления явных или косвенных признаков компрометации ключей ЭП (возникновение подозрений на утечку информации) или вредоносных программ в устройстве, используемом для работы с системой ДБО необходимо прекратить работу, отключить материальный носитель ключей ЭП от устройства и незамедлительно уведомить Банк о необходимости блокировки скомпрометированных секретных ключей ЭП с последующей их заменой.

17. К событиям, связанным с компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- ✓ утеря материального носителя, содержащего секретный ключ, в том числе с последующим обнаружением;
- ✓ Не сохраняйте Ваш логин и пароль в текстовых файлах на компьютере либо на других электронных;
- ✓ носителях информации, т.к. при этом существует риск его кражи и компрометации
- ✓ выход из строя материального носителя, содержащего секретный ключ, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- ✓ обнаружение факта или угрозы использования (копирования) секретного ключа и/или доступа к системе ДБО с использованием секретного ключа неуполномоченными лицами (обнаружение факта совершения операции без согласия Клиента);
- ✓ обнаружение ошибок в работе системы ДБО, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- ✓ увольнение ответственного сотрудника Клиента, имевшего доступ к секретному ключу.

18. Производить смену ключей ЭП как в случае компрометации, так и по требованию Банка.

19. Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

20. Исключайте на устройствах, на которых осуществляется подготовка и отправка документов в Банк, использование систем удаленного управления. Не привлекайте для администрирования и обслуживания данного устройства ИТ-персонал на условиях предоставления ему удаленного доступа.

21. В случае сбоев в работе компьютера или его поломки во время работы в системе ДБО или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т. п.), НЕМЕДЛЕННО извлеките ключи ЭП и выключите компьютер, а также обратитесь в Банк и убедитесь, что от Вашего имени не производились несанкционированные операции (путём сверки операций за день).

22. Рекомендуем осуществлять смену пароля доступа к сервису не реже 1-го раза в 3 месяца.