РЕКОМЕНДАЦИИ
по обеспечению безопасности при работе в системе дистанционного банковского обслуживания «ДБО BS-Client»

Москва
2021

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. По информации Банка России, ежегодно возрастает количество попыток неправомерного доступа злоумышленников к системам дистанционного банковского обслуживания, целью которых является хищение денежных средств клиентов банков.

1.2. Настоящие Рекомендации ООО «Чайна Констракшн Банк» (далее – Банк) предназначены для клиентов Банка (далее – Клиентов), использующих систему дистанционного банковского обслуживания «ДБО BS-Client» (далее – Систему ДБО) на основании договора о дистанционном банковском обслуживании (далее – Договора ДБО), в целях повышения уровня безопасности при дистанционном банковском обслуживании посредством сети Интернет.

1.3. Рекомендации составлены на базе Положения Центрального банка РФ от 09 июня 2012 г. №382-П, Письма Центрального банка РФ от 5 августа 2013 г. № 146-Т.

1.4. В целях снижения рисков информационной безопасности Банк использует совокупность организационных мер защиты информации, программного и аппаратного обеспечения и технологий, способных предотвратить или затруднить совершение несанкционированных операций, а также связанных с обеспечением защиты информации сервисов, предоставляемых Клиентам: резервирование каналов доступа Клиентов к Системе ДБО Банка, многофакторную аутентификацию, подтверждение операций с помощью одноразовых паролей (кодов подтверждения), ограничение каналов взаимодействия Клиентов с Банком, ограничения по операциям Клиентов, процедуры фрод-мониторинга проводимых Клиентами операций, анализ системного окружения клиентской части Системы ДБО Банка и др.

1.5. Меры защиты информации, необходимость применения которых установлена Банком, содержатся в Договоре ДБО, Правилах ДБО и Приложении №2 к Договору ДБО и являются обязательными к использованию Клиентами. Состав применяемых мер защиты позволяет обеспечить необходимый уровень безопасности при работе Клиентов с Системой ДБО Банка.

1.6. Дополнительные меры по обеспечению безопасности при работе в Системе ДБО Банка приведены в настоящих Рекомендациях.

2. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

2.1. Никогда не передавайте третьим лицам информацию, которую они могут использовать для несанкционированного доступа к Системе ДБО. К такой информации относятся сведения об:

- адресах расположения ресурсов Системы ДБО Банка в сети Интернет,
- используемых Банком мерах и способах защиты информации,

- принятых в Вашей организации процедурах подключения к Системе ДБО Банка, хранения, использования Носителей ключа электронной подписи и т.п.

2.2. Не храните Реквизиты доступа к Системе ДБО Банка в файлах на компьютере, не используйте функцию «Запомнить пароль» при работе с системой ДБО.

2.3. Вставляйте Носитель ключа ЭП в компьютер непосредственно перед началом работы в системе ДБО. Обязательно извлекайте из компьютера Носитель ключа ЭП сразу после завершения работы с Системой ДБО Банка. Не оставляйте Носитель ключа ЭП в компьютере, если Вы не работаете с системой ДБО в настоящее время.

2.4. Осуществляйте информационное взаимодействие с Банком только с использованием тех средств связи, реквизиты которых оговорены в документах, получаемых непосредственно от Банка.

2.5. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Банк для получения инструкций по смене пароля.

2.6. Незамедлительно информируйте Банк при получении информации (sms, электронных писем, телефонных звонков от имени Банка), которую Вы не ожидаете получить.

2.7. Сотрудники Банка никогда не попросят у Вас Реквизиты доступа к системе ДБО. Если Вам поступил звонок, в котором Ваш собеседник представился сотрудником Банка и просит у Вас реквизиты доступа к системе ДБО – следует прервать разговор, перезвонить в Банк самостоятельно и сообщить об этом событии.

2.8. На компьютерах, работающих с Системой ДБО Банка, используйте в дополнение к стандартному специализированное программное обеспечение для защиты информации:

- ПО для межсетевого экранирования,
- ПО для предотвращения/обнаружения вторжений,
- иное аналогичное ПО.

2.9. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

2.10. На компьютерах, предназначенных для работы с Системой ДБО Банка, не загружайте файлы и не устанавливайте ПО, полученные из ненадежных источников: загруженные с недоверенных сайтов, полученные по недоверенным веб-ссылкам, принятые от недоверенных лиц по электронной почте.

2.11. Обращайте внимание на расширение файла. Файлы, содержащие вредоносный код, часто маскируются под обычные графические, аудио- видео- и т.п. файлы. С целью маскировки, вредоносный код устанавливает расширение исполняемых

файлов (exe, com, bat, js, и т.п.) после расширения обычных файлов (например - file.txt.exe, video.mkv.com и т.п.) Для того, чтобы видеть настоящее расширение файла, обязательно включите в операционной системе компьютера, предназначенного для работы с Системой ДБО Банка, режим отображения расширений файлов. В целях обеспечения безопасности, подозрительные файлы рекомендуется немедленно удалять.

2.12. В случае подозрения на заражение вирусами компьютера, предназначенного для работы с Системой ДБО Банка (установлено ПО, которое вы не ожидаете увидеть, особенно ПО для удаленного доступа, самопроизвольное переключение окон, отказ компьютерной периферии, массовые срабатывания антивирусного ПО) следует подозревать компрометацию реквизитов доступа к системе ДБО. Сообщайте о таких случаях в Банк и предпринимайте действия по перевыпуску ключа ЭП.

2.13. Мошеннические веб-сайты – это сайты, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти веб-сайты являются почти точной копией сайтов известных компаний, которым Вы доверяете, например - Банка. Они не оказывают реальных услуг и предназначены исключительно для сбора конфиденциальной информации обманным путем. Их доменные имена и стили оформления могут имитировать сайт Банка, но содержать ложные банковские реквизиты и контактную информацию. Ввод реквизитов доступа на таких сайтах приводит к получению этих данных злоумышленниками. В случае обнаружения мошеннического веб-сайта, копирующего дизайн официального сайта Банка или Системы ДБО Банка, пожалуйста, незамедлительно сообщите об этом в Банк.

2.14. Привлекайте специалистов по информационной безопасности высокой квалификации для настройки компьютеров, предназначенных для работы с Системой ДБО Банка, установки и настройки ПО защиты информации.

2.15. При плановом длительном отсутствии необходимости работы с Системой ДБО Банка блокируйте работу компьютера, предназначенного для работы с ней.

2.16. Самостоятельно принимайте меры по исключению доступа в помещения, в которых размещены компьютеры, предназначенные для работы с Системой ДБО Банка, посторонних лиц.

3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

3.1. Заверяем Вас, что Банк очень серьезно относится к обеспечению безопасности работы своих Клиентов с Системой ДБО Банка.

3.2. Деятельность Банка при оказании услуг ДБО регулируется Федеральными законами, Постановлениями Правительства, нормативными документами Банка России, Приказами уполномоченных органов федеральной власти по

соответствующим направлениям. Банк обладает необходимой для оказания услуг ДБО Лицензией ФСБ.

3.3. Банк находится в постоянном взаимодействии с разработчиком Системы «ДБО BS-Client», поставщиками сопутствующего программного обеспечения.

3.4. Соблюдение Вами требований Договора ДБО, в т.ч. Правил ДБО, а также настоящих Рекомендаций, позволит обеспечить высокий уровень безопасности при работе с системой дистанционного банковского обслуживания «ДБО BS-Client» Банка.

3.5. Настоящие Рекомендации не следует рассматривать как исчерпывающий перечень мер защиты информации, исполнение которых позволит полностью исключить риск инцидентов информационной безопасности.