ДЕРЖАВА БАНК

Приложение №1
к Правилам использования системы дистанционного банковского обслуживания для физических лиц

Рекомендации по безопасности работы в Системе ДБО.

Для снижения рисков убытков в результате неправомерного использования Системы ДБО необходимо выполнять следующие рекомендации:

1. Обеспечить хранение информации о Пароле способом, делающим Пароль недоступным третьим лицам, в том числе Клиенту запрещается в ответ на телефонные звонки, SMS или e-mail сообщения, поступившие от любых лиц, в том числе представившихся сотрудниками Банка, сообщать Логин и (или) Пароль, выполнять рекомендации, связанные с вводом каких-либо данных на любых страницах, открытых браузером, или с повторным входом в Систему ДБО, а также незамедлительно уведомлять Банк о Компрометации Пароля в порядке, предусмотренном п. 8.2 Правил. Несоблюдение вышеуказанных требований безопасности является нарушением порядка использования Системы ДБО.

2. Ограничивать доступ третьих лиц к информации об SMS-коде в период соединения с Системой ДБО.

3. Обязательно проверять текст SMS-сообщений/Push-уведомлений, содержащих SMS-код с деталями выполняемой операции. Если в SMS-сообщении/Push-уведомлении указан код для операции, которую не совершал Клиент или Клиенту предлагается его ввести/назвать, чтобы отменить якобы ошибочно проведенную по счету Клиента операцию, ни в коем случае нельзя вводить данный код в Системе ДБО и не называть его, в том числе сотрудникам Банка.

4. Заблокировать (заменить) SIM-карту, в случае утери мобильного телефона, на который приходят SMS-сообщения/Push-уведомления с SMS-кодом.

5. Прекратить работу в Системе ДБО в случае поступления нестандартных запросов.

6. Для использования системы «Мобильный банк» осуществлять скачивание и установку приложения только через официальные репозитории (Android: Google Play https://play.google.com, Apple: AppStore https://appstore.com). Перед установкой приложения убедиться, что их разработчиком является Center of Financial Technologies.

7. Запрещается скачивать и устанавливать приложения из отличных от указанных выше мест. При этом Банк уведомляет, что распространение мошенниками неофициальных приложений, к которым Банк не имеет никакого отношения, возможны путем появления в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых Банком систем ДБО, и (или) использующих зарегистрированные товарные знаки и наименование Банка. Будьте внимательны, при обнаружении подобных ресурсов и приложений следует незамедлительно обратиться в Банк.

8. Запрещается использовать приложения, скачиваемые из отличных от п. 6 источников. В случае такой установки Клиент несет все риски использования системы ДБО, связанные с возможным нарушением безопасности и возможным получением несанкционированного доступа к защищаемой информации.

9. Использовать лицензионное программное обеспечение (операционную систему, приложения), в том числе на мобильном телефоне, полученное из проверенных и

надежных источников, своевременно устанавливать все обновления программного обеспечения, повышающие его безопасность.

10. Своевременно устанавливать обновления операционной системы и прикладных программ, рекомендуемых разработчиком программного обеспечения. Копируйте обновления только с официальных сайтов разработчиков программного обеспечения.

11. Использовать лицензионную антивирусную программу, в том числе на мобильном телефоне, своевременно обновлять антивирусные базы данных, проводить периодическое сканирование своего компьютера.

12. Установить и настроить персональный брандмауэр (firewall) на компьютере, в случае если компьютер работает в сети.

13. Помнить, что при вводе личной информации любой веб-адрес в адресной строке Системы ДБО должен начинаться с «https». Если в адресе не указано «https», это значит, что Клиент находится на незащищенном веб-сайте, и вводить данные нельзя, так как они будут переданы в открытом (незашифрованном) виде и могут быть перехвачены.

14. Отключить функцию автозаполнения в установках браузера.

15. Использовать систему фильтрации ложных web-узлов (антифишинг).

16. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.

17. Запретить в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешить соединение SMTP только с конкретными почтовыми серверами, на которых зарегистрированы электронные почтовые ящики Клиента.

18. Не открывать электронные почтовые сообщения и сообщения систем мгновенного обмена сообщениями, в том числе вложенные в них файлы, поступающие от неизвестных отправителей.

19. Не оставлять без присмотра свой компьютер, мобильный телефон в период соединения с Системой ДБО.

20. Использовать кнопку «Выход» после окончания работы в Системе ДБО.

21. Выполнять условия Правил, в том числе действия, указанные в п. 3.2.13. Правил.