Приложение № 1
к Правилам дистанционного банковского обслуживания
с использованием Системы «Клиент-Банк»

РЕКОМЕНДАЦИИ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С СИСТЕМОЙ «КЛИЕНТ-БАНК»

Во исполнение пункта 3 статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк информирует Клиента о мерах безопасного использования Системы:

1. Назначать сотрудников, ответственных за использование Системы;

2. Обеспечить надежное хранение и защиту от компрометации носителя Ключа ЭП (MAC-токен BIFIT, USB–токен «MS_KEY K» – «АНГАРА» Исп.8.1.1, Рутокен ЭЦП 3.0). Размещение ключевой информации на жестком диске компьютера, на котором установлена Система запрещается;

3. Не передавать посторонним лицам данные об использовании Системы: адрес (IP-адрес) Web-сервера, особенности входа в Систему и использования ключа электронной подписи и т.п.;

4. Не оставлять без присмотра рабочие места с загруженной Системой. Ключевые носители информации, извлекать из USB разъема компьютера по завершении работы;

5. Заменять Ключи ЭП в случаях их компрометации или подозрения на компрометацию. Кроме того, рекомендуется заменять ключи электронной подписи при увольнении/прекращении полномочий сотрудников/представителей Клиентов, имевших доступ к ключам ЭП, а также руководителей, которые подписывали Сертификат ключа проверки электронной подписи;

6. Обратить внимание на увеличение риска хищения и дальнейшего неправомерного использования Ключа ЭП и другой аутентификационной информации при доступе к Системе с гостевых рабочих мест (интернет-кафе, гостиницы, офисные центры и т.д.);

7. Использовать на компьютерах, где установлена Система:

– лицензионное антивирусное программное обеспечение с регулярным его обновлением (желательно в автоматическом режиме);

– операционная система компьютера и мобильного телефона должна быть современной, лицензионной и обновляемой, поддерживаемая разработчиком;

– установленный и настроенный Интернет–браузер актуальной версии;

8. Не вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы (логотип другого банка, другие надписи, шрифт и тому подобное), или отображается не так как всегда (нарушен порядок работы в системе), или получили SMS с паролем на вход в систему, в то время как такой доступ не осуществлялся, или нарушена нумерация платежных поручений и т.д. Необходимо обратиться в службу технической поддержки Банка при нетипичной работе Системы;

9. Периодически (не реже одного раза в год) менять пароль для входа в Систему и не создавать простых и легких паролей (например, 111111, 12345 и т.п.). Не указывать в качестве пароля дату рождения, номера телефонов и иные данные, которые легко можно узнать третьим лицам;

10. Не отвечать на подозрительные письма с просьбой выслать Ключ ЭП, пароль и иные конфиденциальные данные, либо с Вами связались по телефону от имени Банка, с просьбой установить какое-либо программное обеспечение, необходимо связаться со службой технической поддержки Банка и уточнить ситуацию. Банк никогда не осуществляет рассылку электронных писем с просьбой предоставить конфиденциальную информацию (ключи, пароли и т.п.);

11. Всегда используйте контактную информацию службы поддержки Банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в письме или полученную в ходе телефонного разговора;

12. В случае, если не удается в штатном режиме войти в Систему или по невыясненным причинам компьютер, с которого осуществляется работа в Системе, перестал загружаться, некорректно реагирует на команды в обычном режиме (самопроизвольное перемещение курсора, открытие и закрытие окон, набор текста), внезапно прекратил работать – рекомендуется **незамедлительно** обратиться в Службу технической поддержки Банка, проинформировать Банк о сложившейся ситуации;

13. Ограничить доступ (физический и/или удаленный) к компьютеру третьих лиц, не имеющих полномочий для работы с Системой.

14. При работе с почтой не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять. В случае необходимости загрузки файла, убедиться, что он проверен антивирусом.

15. Рекомендуется использовать отдельный компьютер исключительно для работы с Системой. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.

15. Контролировать адресную строку браузера, адрес должен начинаться с https://ibank.nipbank.ru. При появлении сообщения о несоответствии сертификата имени узла прекратить работу с Системой и сообщить в службу технической поддержки Банка;

16. Использовать дополнительные средства безопасности – SMS-сервис с получением разовых паролей (Приложение № 8 к Правилам ДБО), MAC-токены (Приложение № 9 к Правилам ДБО), проверку IP-адресов, с которых осуществляется работа с Системой (Приложение № 6 к Правилам ДБО).

17. В случае передачи (списания, утилизации и т.п.) сторонним лицам компьютера, на котором ранее была установлена Система, необходимо удалить с него всю информацию, использование которой третьими лицами может нанести вред Вашей организации.