**Памятка по информационной безопасности при работе**

**в системе «iBank 2»**

Настоящей памяткой Банк в целях повышения безопасности работы в системе «iBank 2» обращает Ваше внимание на необходимость соблюдения следующих мер предосторожности:

1. Никогда не открывать сайт системы «iBank 2» по ссылкам (полученным через электронную почту или баннерным сайтам), поскольку существует множество способов фальсифицировать адрес. Необходимо использовать адрес сайта, предоставленный Банком или полученный через корпоративный сайт Банка.
2. Не отвечать на подозрительные письма с просьбой выслать секретный ключ ЭП, пароль и другие конфиденциальные данные. Банк никогда не запрашивает у Клиента конфиденциальную информацию по электронной почте или посредством телефонных звонков, это действия злоумышленников.
3. Программное обеспечение системы «iBank 2» никогда не выводит на экраны компьютера сообщение о временной неработоспособности системы. Сообщения типа: *«На сервере банка ведутся профилактические работы»,*свидетельствуют о том, что Ваш компьютер заражен вредоносным ПО. При возникновении любых подозрений на наличие в компьютере вредоносных программ немедленно позвоните в Банк и заблокируйте ключи, прекратите использование данного компьютера для работы в системе «iBank 2» до ликвидации вирусного заражения.
4. Рекомендуется использовать отдельный компьютер для работы в системе «iBank 2» и исключить посещение Интернет-сайтов сомнительного содержания, открытие подозрительных файлов, работу с непроверенными носителями информации и так далее с этого компьютера.
5. Ограничить физический доступ к компьютеру, используемого для работы в системе «iBank 2». Соблюдайте бдительность при работе ИТ-специалистов, в случае их вызова.
6. Использовать на рабочих местах современные лицензионные операционные системы (ОС) являющиеся более защищенными, в отличие от более старых версий. Обеспечить регулярное обновление операционной системы.
7. Использовать и оперативно обновлять специализированное ПО для защиты информации – антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и т.п. На регулярной основе проводить полное сканирование компьютера на наличие вирусов.
8. Не устанавливать на компьютере, используемом для работы в системе, средства удаленного управления компьютером.
9. При каждом входе в систему проверять предыдущие сеансы работы.
10. Ключи ЭП подключать к компьютеру только на время работы с системой «iBank 2», после окончания работы сеанса работы ЭП необходимо изъять и хранить в недоступном третьим лицам месте.
11. Для защиты ключей ЭП клиента от хищения вредоносными программами рекомендуется использовать USB-токен. Пароль на доступ к ключам ЭП должен быть известен только владельцу (доверенному лицу). Ключи первой и второй подписи необходимо хранить на разных USB-токенах и при формировании платежных поручений использовать их последовательно.
12. При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно заблокируйте ключи проверки ЭП и сгенерируйте новые.
13. При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк и заблокировать ключи ЭП.