Рекомендации
по предупреждению хищений денежных средств с расчетных счетов, путем несанкционированного удаленного доступа к компьютерам, с которых осуществляется доступ в систему электронного документооборота «iBank 2» ОАО «АКИБАНК»

Уважаемые клиенты!

1. Не устанавливайте в организации на служебные компьютеры, с которых осуществляется доступ в систему электронного документооборота «iBank 2» (далее – система ЭДО) сторонние приложения: «Team Viewer», «Radmin» и другие, позволяющие осуществлять удаленный доступ к компьютерам.

2. Используйте сеть Интернет на служебных компьютерах, с которых осуществляется доступ в систему ЭДО, исключительно для работы в системе ЭДО. Категорически запретите доступ к социальным сетям, развлекательным и иным ресурсам сети Интернет.

3. Установите на все служебные компьютеры, с которых осуществляется работа в системе ЭДО лицензионное антивирусное программное обеспечение. Постоянно следите за наличием актуальных обновлений и своевременно инсталлируйте их.

4. Ни при каких обстоятельствах не копируйте данные электронного ключа на жесткий диск компьютера, с которого осуществляется работа в системе ЭДО. После завершения работы в системе ЭДО, извлекайте электронный ключ и храните его в недоступном посторонним лицам месте.

5. В случае выявления на компьютере вредоносного программного обеспечения, незамедлительно извлеките ключ электронной подписи, выключите компьютер и свяжитесь со службой круглосуточной технической поддержки по единому номеру телефона: **8 800 100 2542** (звонок по РФ бесплатно).

Безопасной Вам работы!

АКИБАНК
АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ ИПОТЕЧНЫЙ БАНК