БАНК НОВЫЙ ВЕК
г. Москва, ул. Щипок, д. 4, стр. 1
тел.: +7 (495) 223-00-63
www.newbank.ru

ПАМЯТКА КЛИЕНТА ПО РАБОТЕ В СИСТЕМЕ «IBANK 2»

Уважаемые клиенты Банка!

КБ «Новый век» (ООО) настоятельно просит Вас соблюдать правила информационной безопасности при работе с использованием Системы «iBank 2», а именно:

1. При работе через Систему «iBank 2» подключите через уполномоченное подразделение Банка функцию фильтра по IP-адресам/диапазоны IP-адресов, реализованную в Системе «iBank 2». Использование этой функции позволит Вам снизить риски несанкционированного доступа к Вашему лицевому счету, доступ к которому в рамках использования Системы будет осуществляться только с IP-адресов/диапазонов IP-адресов, указанных Вами. Для подключения функции фильтрации в рамках работы через Систему Вам следует направить надлежащим образом оформленное Заявление (Приложение №4 к типовой форме договора) в адрес Банка с заявкой активации вышеуказанного фильтра, указанием перечня IP-адресов/диапазона IP-адресов, необходимых Вам для работы.
2. Храните в режиме строгой конфиденциальности секретные ключи ЭЦП, используемые Вами при работе в Системе «iBank 2». КБ «Новый век» (ООО) настоятельно рекомендует Клиентам персональные аппаратные криптопровайдеры (услуга по защите секретного ключа ЭЦП), а также хранить носители ключевой информации в местах, к которым исключен несанкционированный доступ третьих лиц. Строжайше предостерегаем Вас от хранения ключей ЭЦП непосредственно на жестком диске компьютера. Недопустимо оставлять носители ключевой информации без присмотра, а также в местах, доступ к которым легко получить третьим лицам (ящики столов и т.п.), а равно подключенными к ПЭВМ вне процесса работы в Системе «iBank 2».
3. Используйте возможности сервиса расширенной многофакторной аутентификации с помощью OTP-токенов при входе в систему и/или подтверждения платежных документов, направляемых в Банк.
4. Немедленно обращайтесь в Банк в случаях компрометации секретных ключей ЭЦП либо подозрения на их компрометацию (хранение ЭЦП в местах, доступных третьим лицам, случаи несанкционированного доступа к ключам ЭЦП третьих лиц, случаи несанкционированного доступа к лицевому счету через Систему, случаи пропажи носителей ключевой информации, в том числе кратковременной, и т.п.). В случаях увольнения или смены лиц, допущенных к ключам ЭЦП и соответственно носителям ключевой информации, незамедлительно обращайтесь в Банк для блокировки и исключения соответствующих ключей ЭЦП. Для блокировки/исключения ключей ЭЦП необходимо направить в Банк письменное заявление, с указанием владельца и/или ID ключа, который необходимо заблокировать. Для срочного блокирования ключа ЭЦП пользуетесь возможностью блокировки по телефону с помощью блокировочного слова, оформляемого при подключении к Системе «iBank 2».
5. Банк рекомендует использовать для работы в Системе «iBank 2» отдельно выделенный компьютер, с которого не осуществляется иная текущая работа. Не рекомендуется использовать для взаимодействия с Банком через Систему «iBank 2» общедоступный компьютер, с которого осуществляется публичный доступ сотрудников Вашей организации в сеть Интернет, так как публичный доступ в сеть Интернет несет за собой большие риски проникновения на компьютер вредоносного и шпионского программного обеспечения вне зависимости от характера и направленности установленных средств защиты.
6. Обращаем Ваше внимание на **необходимость** использования персональных средств защиты (средства антивирусной защиты, наличие межсетевого экрана и т.д.) на компьютере, с которого осуществляется взаимодействие с Банком через Систему «iBank 2», а также на необходимость периодического и своевременного обновления компонент данных средств защиты и иного программного обеспечения, установленного на Вашем компьютере (операционная система, web-браузеры, офисные приложения и т.д.).
7. Настоятельно не рекомендуется осуществлять взаимодействие с Банком через Систему «iBank 2» с компьютеров, расположенных в общественных местах (интернет-кафе, компьютеры третьих лиц и т.д.), так как на данных компьютерах невозможно гарантировать соблюдения режима информационной безопасности (наличие антивирусных средств, отсутствие вредоносного и шпионского программного обеспечения, отсутствие программ теневого копирования и т.д.), что существенно увеличивает риск хищения и дальнейшего использования Вашего ключа ЭЦП и другой аутентификационной информации.

В случаях возникновения вопросов и/или получения дополнительной информации по вопросам информационной безопасности при дистанционном банковском обслуживании Вы можете обращаться к сотрудникам Отдела автоматизации КБ «Новый век» (ООО) по телефону (495) 223-00-70.

Помните, что соблюдение режима защиты информации, рекомендаций Банка по использованию дополнительных сервисов Системы «iBank 2», а также осуществление мероприятий по своевременной блокировке скомпрометированных ключей ЭЦП позволит Вам минимизировать риски несанкционированного доступа в Систему «iBank 2», а в случаях, когда подобный доступ имел место, оперативно устранить его последствия.

Спасибо за понимание!