Приложение 6
к Правилам предоставления и использования
системы дистанционного банковского обслуживания для
физических лиц
КБ «Новый век» (ООО)

ПОРЯДОК
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

1. Для работы с Системой ДБО для физических лиц (далее – Система ДБО) при использовании web-версии ДБО, необходимо подготовленное рабочее место, которое рекомендуется использовать только для работы в Системе ДБО, и на котором установлено современное антивирусное программное обеспечение и персональный межсетевой экран. Антивирусное программное обеспечение необходимо регулярно обновлять и проводить сканирование компьютера для защиты от новых вирусов и вредоносных программ. Персональный межсетевой экран позволяет предотвратить несанкционированный доступ к вашему компьютеру из сети Интернет или из локальной сети.
2. Рекомендуется использовать разные технические средства для доступа в Систему ДБО и для получения СМС-подтверждений, push-уведомлений для осуществления операций по счету.
3. Рекомендуется использовать только лицензионное программное обеспечение — это защитит от программных «закладок», оставленных злоумышленниками в нелицензионном и «взломанном» программном обеспечении. Обязательно производить регулярную установку обновлений программного обеспечения по мере их выпуска производителем, для этого рекомендуется настроить автоматическое обновление.
4. Запрещается устанавливать и использовать на техническом средстве, используемом для отправки ЭД в Банк, средства удаленного управления компьютером, такие как «TeamViewer», «RAdmin», «AnyDesk» и подобные.
5. Не рекомендуется открывать подозрительные файлы и ссылки на неизвестные сайты, даже если они получены с известного адреса, и тем более, если они получены от неизвестных отправителей.
6. Не рекомендуется посещать сайты, предлагающие быстро и бесплатно скачать различные файлы или программы, поскольку даже вход на такой сайт может угрожать безопасности технического средства.
7. Запрещается сообщть третьим лицам пароли доступа к Системе ДБО.
8. В случае утери (хищения) устройства, используемого для доступа в Систему ДБО, а также при возникновении подозрений, что доступ к Системе ДБО могли получить неуполномоченные лица или могли быть совершены несанкционированные платежи, необходимо незамедлительно связаться с Банком.
9. Рекомендуется внимательно читать получаемые из Банка СМС- и push- сообщения о движении средств по счету с целью контроля производимых операций. Сумма, получатель платежа и другие реквизиты, указанные в СМС- или push- сообщении, должны соответствовать реквизитам, введенным в Системе ДБО.
10. Рекомендуется регулярно мониторить информацию в Системе ДБО для поддержания актуальности осведомленности о совершённых операциях и информационных сообщениях от банка.
11. В случае невозможности входа в Систему ДБО и одновременного отсутствия возможности подключения к web-сайту Банка, рекомендуется сообщить об этом в Банк, поскольку это может свидетельствовать о возможной попытке злоумышленников совершить мошеннические операции.

ВАЖНО: своевременное обращение в банк значительно повышает вероятность того, что похищенные денежные средства удастся возвратить и предотвратить мошенничество. В случае несвоевременной реакции, вероятность возврата похищенных денежных средств значительно ниже и с большой вероятностью потребует обращения в правоохранительные органы.