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 дистанционного банковского обслуживания для физических лиц (далее – Система ДБО) необходимо подготовленное рабочее место, которое рекомендуется использовать только для работы с Системой 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. Запрещается использовать одно и тоже техническое средство для доступа в Систему ДБО и для получения SMS-подтверждений 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» и подобные.
5. Не следует 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 следует посещать сайты, предлагающие быстро и бесплатно скачать различные файлы или программы, поскольку даже вход на такой сайт может угрожать безопасности технического средства.
7. Не сообщайте третьим лицам пароли от 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 совершены несанкционированные платежи, необходимо немедленно связаться с Банком.
9. Внимательно читайте отправляемые из Банка SMS-сообщения о движении средств по счету с целью контроля производимых операций. Сумма, получатель платежа и другие реквизиты, указанные в SMS-сообщении, должны соответствовать реквизитам, введенным в Системе ДБО.
10. Необходимо регулярно просматривать информацию в Системе ДБО для того, чтобы видеть все совершенные операции и все информационные сообщения, присланные по системе.
11. В случае невозможности входа в Системе ДБО и одновременного отсутствия возможности подключения к Веб-сайту Банка сообщите об этом в Банк, поскольку это может свидетельствовать о возможной попытке злоумышленников совершить мошеннические операции.

ВАЖНО: немедленное обращение в Банк значительно повышает вероятность того, что похищенные денежные средства удастся возвратить и предотвратить мошенничество. В случае несвоевременной реакции вероятность быстрого возврата похищенных денежных средств значительно ниже и необходимо будет обращаться в правоохранительные органы.