РЕКОМЕНДАЦИИ ПО ПРЕДУПРЕЖДЕНИЮ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Уважаемые клиенты!

Для снижения рисков хищения денежных средств путем несанкционированного доступа к вычислительным средствам, на которых установлены компоненты для доступа в систему дистанционного банковского обслуживания (далее – ДБО), рекомендуем придерживаться следующих правил:

1. Не устанавливайте на средства вычислительной техники, предназначенной для работы с системами ДБО, средства удаленного доступа, такие как «Team Viewer», «Remote Administrator» и другие.
2. Ограничьте доступ к сети интернет. Используйте доступ в сеть Интернет исключительно для работы в системе ДБО. Воздержитесь от доступа к социальным сетям и другим развлекательным ресурсам.
3. Установите на все средства вычислительной техники, с которых осуществляется работа в системе ДБО лицензионные антивирусные средства. Следите за своевременным обновлением антивирусных баз.
4. Сертификат ключа проверки электронной подписи (далее – Сертификат) рекомендуем хранить на смарт-ключе полученном при подключении к системе ДБО. Воздержитесь копирования и хранения Сертификата на других электронных носителях информации.
5. Подключайте смарт-ключ к средствам вычислительной техники исключительно на время работы в системах ДБО. По завершении работы в системе ДБО отключите смарт-ключ и храните его в месте недоступном для посторонних лиц.
6. В случае выявления на средствах вычислительной техники, используемых для работы с системами ДБО, вредоносного программного обеспечения, незамедлительно отключите смарт-ключ и свяжитесь со службой технической поддержки РНКО «Р-ИНКАС» (ООО) по телефону: +7(495)393-48-98