Комплекс мер по предупреждению хищений денежных средств с расчетных счетов юридических лиц, путем несанкционированного удаленного доступа к компьютерам, использующим программное обеспечение дистанционного банковского обслуживания

1. Запретить клиентам устанавливать на служебные компьютеры, на которых инсталлированы программы дистанционного банковского обслуживания, использование сторонних приложений, позволяющих осуществление удаленного доступа к этому компьютеру (таких, как «Team Viewer», «Радмин» и т.п.).
2. Использовать подключение к сети Интернет на служебных компьютерах, на которых инсталлированы программы дистанционного банковского обслуживания исключительно для работы с указанным программным обеспечением. Категорически запретить доступ к социальным сетям, развлекательным и иным ресурсам сети Интернет.
3. Установить на все служебные компьютеры, с которых осуществляется работа с программным обеспечением дистанционного банковского обслуживания лицензионное антивирусное программное обеспечение, позволяющее блокирование несанкционированного удаленного доступа к компьютеру по сети Интернет. Постоянно следить за наличием актуальных обновлением и своевременно инсталлировать их.
4. Ни при каких обстоятельствах не копировать данные электронного ключа на жесткий диск компьютера, с которого осуществляется работа с программным обеспечением дистанционного банковского обслуживания. После завершения работы с указанной программой, извлекать электронный ключ и хранить его в недоступном посторонним лицам месте.
5. В случае выявления на экране компьютера вредоносного программного обеспечения, незамедлительно извлечь ключ электронной подписи, выключит компьютер и связаться со службой технической поддержки.

МВД по Республике Татарстан