ОАО «ЧЕЛЯБИНВЕСТБАНК»

Рекомендации по снижению рисков несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств в системах дистанционного банковского обслуживания (ДБО).

1. Исключите доступ ключам ЭЦП посторонних лиц. Ключи ЭЦП рекомендуется хранить специальных носителях (USB –токенах) защищённых pin-кодом. Избегайте создания резервных копий ключей ЭЦП (при утрате ключей всегда можно сгенерировать и зарегистрировать новый ключ ЭЦП), а созданные копии храните в сейфе.
2. Подключайте носитель с ключами ЭЦП к компьютеру с системой ДБО исключительно на время работы с системой ДБО. В прочее время носитель должен быть отключен от компьютера.
3. Исключите доступ к компьютеру с системой ДБО посторонних лиц.
4. Используйте лицензионное программное обеспечение со свежими обновлениями, устраняющими уязвимости.
5. Используйте антивирусное программное обеспечение со свежими обновлениями (однако помните, что 100% защиты не обеспечивает ни один антивирус).
6. На межсетевом экране предприятия необходимо настроить запрет на взаимодействие компьютера с неизвестными интернет ресурсами (так называемый «белый список»).
7. Не используйте компьютер с системой ДБО для работы с интернетом и электронной почтой.
8. Внимательно относитесь к подозрительной активности компьютера (в частности, неожиданным «зависаниям», перезагрузкам, сетевой активности), сообщайте системному администратору предприятия о странном поведении компьютера и воздержитесь от использования системы ДБО до устранения неполадок.
9. Подключите СМС-уведомления о платежах.
10. Используйте регулярное резервное копирование.
11. В случае обнаружения попытки/факта кражи – немедленно выключите компьютер, сообщите в банк и обратитесь в правоохранительные органы.