КРЕДИТ УРАЛ БАНК
ГРУППА ГАЗПРОМБАНКА

ПАМЯТКА ДЛЯ КЛИЕНТОВ

О действиях в случае обнаружения попытки или несанкционированного списания денежных средств в системе дистанционного банковского обслуживания (ДБО).

В случае обнаружения несанкционированного доступа к счету и/или несанкционированного списания денежных средств со счета Банк рекомендует Клиенту осуществить следующие действия:

1. Немедленно обратиться к обслуживающему Вас специалисту клиентской службы или главному специалисту клиентской службы по телефону **248-935** с требованием о блокировке доступа Клиента к системе ДБО, приостановке исполнения платежа и/или просьбой оказания содействия в возврате несанкционированно списанных денежных средств или на номера Контакт - центра Банка «КУБ» (АО): **248-933, 544-544**.
2. Не позднее рабочего дня, следующего за днем устного обращения представить в Банк письменное заявление, заверенное печатью и подписью руководителя о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой оказания содействия в возврате несанкционированно списанных денежных средств.
3. Немедленно прекратить любые действия с электронными устройствами: персональный компьютер, ноутбук, планшетный компьютер и т.п., подключенным к системе ДБО, отключить его от сети и обесточить. Эти действия позволят предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.
4. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств. Копию заявления и талона - уведомления о его приеме предоставить в отдел обслуживания корпоративных клиентов в срок не позднее 1 рабочего дня со дня выявления факта хищения денежных средств.
5. Произвести смену ключей электронной подписи , используемых для работы с системой ДБО в соответствии с действующим Дополнительным соглашением по автоматизированному обслуживанию Клиента. **До момента смены ключей участие Клиента в обмене электронными документами прекращается в связи с компрометацией действующих средств доступа.**
6. После окончания процедуры смены ключей не возобновлять деятельность на данной рабочей станции без проведения соответствующих технических мер, которые гарантируют полное уничтожение вирусных объектов, но только в том случае, когда уже не требуется сохранение доказательной базы в целях проведения расследования инцидента правоохранительными органами. В случае необходимости сохранения персонального компьютера в текущем состоянии, использовать в работе другой компьютер.