ВАЖНО! **Рекомендации по информационной безопасности**

В настоящее время, кредитные организации и их клиенты все чаще сталкиваются с угрозами при осуществлении переводов денежных средств. Поскольку осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, является основной целью злоумышленников, инциденты данного вида закономерно составляют большую долю всех выявляемых инцидентов.

В этой связи, Банки реализуют комплекс мероприятий организационного и технического характера, направленных на обеспечение защиты информации. Соблюдение правил информационной безопасности (ИБ) призвано обеспечить защищенность интересов кредитной организации и её клиентов в условиях угроз в информационной сфере при оказании услуг дистанционного банковского обслуживания (ДБО).

Задачи ИБ сводятся к минимизации ущерба, а также к прогнозированию и предотвращению случайных или злонамеренных воздействий. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам ИБ уделяется достаточно внимания, как на стороне банка, так и на стороне клиента.

Поскольку основное количество схем хищений направлено на реализацию различных атак на процедуры и технологии расчетов с использованием электронных средств платежа, включая системы ДБО, то и основные мероприятия ориентированы на защиту этих средств.

Для минимизации рисков при использовании дистанционного банковского обслуживании Банк рекомендует Клиентам:

- Использовать в работе только лицензионные версии операционных систем и прикладного программного обеспечения;
- Применять сертифицированные средства криптографической защиты информации (СКЗИ);
- Применять и своевременно обновлять средства антивирусной защиты;
- Своевременно устанавливать обновления безопасности для используемого ПО;
- Определить последовательность необходимых действий, осуществляемых при возникновении внештатной ситуации или при подозрении на неё.
- Разработать Регламент доступа к компьютерам и секретным ключам при использовании систем ДБО, в котором определить перечень событий, наступление которых должно повлечь за собой немедленную замену/изъятие ключей электронной подписи;
- Разработанный Регламент доводить до сведения всех своих сотрудников, работа которых связана с системой ДБО;
- Для снижения риска неправомерного доступа и использования услуг ДБО в результате хищения злоумышленниками идентификаторов доступа (логина, пароля и криптографических ключей) применять современные технические средства такие, как ключевые носители (токены, смарт-карты) с неизвлекаемыми ключами электронной подписи;
- Использовать весь доступный функционал операционной системы, программного обеспечения и системы ДБО, в том числе, включающий в себя ограничения на использование «простых» паролей, минимальную длину и период действия паролей, ограничение разрешенных IP-адресов, с которых допускается работа в системе ДБО.

Противодействие инсайдерам

Наибольшими возможностями для нанесения ущерба при осуществлении дистанционного банковского обслуживания обладает собственный персонал (инсайдеры), а также ненадлежащим образом защищенная (с точки зрения ИБ) территория размещения АРМ ДБО Клиента.
Для обеспечения защиты от атак с участием инсайдеров Банк рекомендует предусмотреть:

- разработку и внедрение строгой политики ролей и прав сотрудников, разграничение доступа к информационным ресурсам;
- использование сетевых брандмауэров (FireWall) для фильтрации и разграничения доступа сотрудников как к внешним, так и к внутренним ресурсам;
- организацию физического доступа в помещения, в которых функционирует система ДБО.

Весь этот комплекс мер — как организационных, так и технических,— позволит Банку и Клиентам обеспечить надлежащий уровень защиты услуг дистанционного банковского обслуживания от внешних и внутренних угроз.