Приложение № 12
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПОЛОЖЕНИЕ
о порядке действий сторон в случае компрометации средства подтверждения

1. События, которые могут быть расценены как компрометация Средства подтверждения:
   1.1. утрата/хищение Средства подтверждения;
   1.2. несанкционированное копирование ключа ЭП;
   1.3. передача ключа ЭП по открытым каналам связи;
   1.4. случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения (в том числе случаи, когда Средство подтверждения вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника);
   1.5. любые другие признаки осуществления несанкционированных действий в системе «iBank 2».

2. Решение о компрометации Средства подтверждения может быть принято владельцем ключа ЭП или руководителем организации.

3. **В случае компрометации Средства подтверждения и обнаружения факта несанкционированного списания средств КЛИЕНТУ необходимо:**
   3.1. немедленно прекратить любые действия с Рабочим местом Системы «iBank2», обесточить его и отключить от информационных сетей или перевести в режим гибернации;
   3.2. произвести фотосъемку Рабочего места, обеспечить его сохранность, поместив в место с ограниченным доступом и обеспечив при этом защиту от вскрытия. При необходимости ведения хозяйственной деятельности - задействовать другое Рабочее место;
   3.3. обратиться в БАНК с **Уведомлением о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использованием ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям), далее – «Уведомление по форме Приложения № 7», **на бумажном носителе** за подписью руководителя КЛИЕНТА и оттиском печати, не позднее дня, следующего за днем получения от БАНКА уведомления о совершении операции, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подписанных/подтвержденных указанными Средства подтверждения;
   3.4. обратиться в иные банки, которые предоставляют КЛИЕНТУ услуги электронного банкинга, с просьбой о внеплановой замене ключей ЭП в их информационных системах;
   3.5. предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет за максимальный период времени;
   3.6. провести сбор записей с межсетевых экранов и других средств защиты информации, коммуникационного оборудования и устройств, которые могут использоваться для удаленного управления Рабочим местом;
   3.7. обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений Рабочего места или локальной вычислительной сети компании с сетью Интернет;
   3.8. не предпринимать никаких действий для поиска и удаления компьютерных вирусов, восстановления работоспособности Рабочего места, не отправлять Рабочее место в сервисные службы для восстановления работоспособности;
   3.9. зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к Рабочему месту, предпринимаемые действия с Рабочим местом, подготовить объяснения ответственных сотрудников в случае использования Рабочего места в целях, отличных от осуществления операций в системе электронного банкинга, посещаемых сайтах, перебоях в работе или отказах Рабочего места, обращениях в службы сопровождения, в БАНК, о сторонних лицах, побывавших в месте расположения Рабочего места и т.д.
   3.10. все действия с Рабочим местом производить коллегиально, протоколировать и документировать, в том числе с использованием фотосъемки.

4. **В случае компрометации Средства подтверждения, если факт несанкционированного списания средств не обнаружен, КЛИЕНТУ необходимо:**
Обратиться в БАНК с **Уведомлением по форме Приложения № 7 на бумажном носителе** не позднее дня, следующего за днем обнаружения факта компрометации, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подтвержденных указанными Средствами подтверждения.

5. **О компрометации ключа ЭП КЛИЕНТ уведомляет БАНК следующими способами:**
5.1. **по телефону БАНКА 8(495)933-46-00** (Управление информационных технологий Банка), назвав Кодовое слово, с последующим предоставлением **Уведомлением по форме Приложения № 7 на бумажном носителе,** в срок, предусмотренный п. 3.3. настоящего Приложения.
5.2. направить **Уведомление по форме Приложения № 7** в виде скан-копии на электронную почту БАНКА ibank@russitabank.ru, с последующим предоставлением **Уведомлением по форме Приложения № 7 на бумажном носителе,** в срок, предусмотренный п. 4. настоящего Приложения.
5.3. предоставить **Уведомление по форме Приложения № 7** на бумажном носителе в БАНК. Указанное Уведомление предоставляется руководителем КЛИЕНТА или лицом, имеющим соответствующую доверенность на подачу в БАНК вышеуказанного Уведомления.
Уведомление по форме Приложения № 7 на бумажном носителе, предусмотренное настоящий пунктом должно быть подписано руководителем КЛИЕНТА с проставлением оттиском печати и предоставлено в БАНК руководителем КЛИЕНТА или лицом, имеющим соответствующую доверенность на подачу в БАНК вышеуказанного Уведомления.
Уведомление по форме Приложения № 7 на бумажном носителе от КЛИЕНТА считается принятым БАНКОМ с момента проставления уполномоченными лицами Банка соответствующих отметок, подписей и печати на экземпляре КЛИЕНТА указанного Уведомления.

6. БАНК не позднее 1 (Одного) часа с момента получения Уведомления КЛИЕНТА, способами, предусмотренными п. 5 настоящего Приложения, и подтверждения полномочий КЛИЕНТА, останавливает обработку ЭД, подписанных ключами ЭП КЛИЕНТА, и блокирует ключи ЭП КЛИЕНТА.

7. Во всех случаях отключения КЛИЕНТОМ Системы «iBank 2», предусмотренных п. 5 настоящего Приложения, дальнейшее подключение КЛИЕНТОМ Системы «iBank 2» осуществляется заново с предоставлением в БАНК Заявления о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank 2» (Приложение № 5 к настоящим Условиям) и взиманием комиссии согласно Тарифам БАНКА.

8. В случае получения SMS-Сообщения от БАНКА о принятии от КЛИЕНТА по Системе «iBank 2» платежного поручения на расходную операцию и несогласия с указанной операцией КЛИЕНТ обязан незамедлительно с момента поступления указанного SMS-сообщения уведомить БАНК способами, предусмотренными п. 5.1.-5.3. настоящего Приложения, о своем несогласии и обратиться с просьбой предотвратить совершение планируемой расходной операции.
В случае поступления в БАНК от КЛИЕНТА по Системе «iBank 2» платежного поручения на расходную операцию и отсутствия в соответствии с настоящим Приложением Уведомления от КЛИЕНТА свидетельствуют о согласии КЛИЕНТА с расходной операцией по Счету. В указанном случае БАНК не несет ответственности за совершение несанкционированной расходной операции по Счету(-там) КЛИЕНТА.

9. Электронные документы, находящиеся на момент получения/исполнения **Уведомление по форме Приложения № 7** на бумажном в статусе «На обработке»/«На исполнении» отзыву не подлежат. При наличии в вышеуказанном случае технической возможности БАНК вправе остановить обработку и исполнение ЭД.