Рекомендации для клиентов ПАО КБ «УБРиР» при выявлении случаев хищения (попытки хищения) денежных средств в системах удаленного доступа («Интернет-банк», «Банк-клиент»)

1. Настоящий документ (далее – Рекомендации) разработан для клиентов (юридических лиц и индивидуальных предпринимателей) ПАО КБ «УБРиР» (далее – Банк), которые являются пользователями систем удаленного доступа «Интернет-банк» и «Банк-клиент» (далее - СУД) с целью разъяснения действий в случае выявления хищения (попытки хищения) денежных средств в СУД, а также в целях оперативной организации эффективного взаимодействия и принятия процессуальных решений по фактам совершения хищения денежных средств в СУД.

2. Рекомендации опубликованы на официальном сайте банке в разделе http://www.ubrr.ru/msb/ibank/bezopasnos/ в отдельной вкладке «Рекомендации при выявлении хищения (попытки хищения) денежных средств». При обращении уполномоченного лица клиента в точку продаж Банка (дополнительный офис, операционный офис, структурное подразделение филиала, осуществляющие расчетно-кассовое обслуживание клиентов), в целях непосредственного ознакомления с Рекомендациями, данный документ распечатывается и предоставляется для ознакомления на бумажном носителе.

3. Действия клиента Банка при выявлении хищения денежных средств в СУД.

3.1. Немедленно прекратить любые действия с электронным устройством (далее –ЭУ), подключенным к системе СУД, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.).

3.2. Незамедлительно проинформировать Банк о произошедшей ситуации установленным образом, обратившись к менеджеру услуги по телефону (343) 264-55-19 (круглосуточно) или к менеджеру счета по телефону, указанному в договоре на обслуживание в СУД.

3.3. Незамедлительно, но не позднее, чем в течение трех рабочих дней с момента выявления хищения денежных средств, направить уведомление о возникновении конфликтной ситуации в Банк с письменным заявлением о разъяснении произошедшей ситуации, в связи с хищением денежных средств через СУД (см. Порядок проведения экспертизы при возникновении конфликтных ситуаций (разногласий)).

3.4. Проинформировать другие банки, с которыми клиент имеет договорные отношения, предусматривающие использование систем удаленного доступа, о факте хищения денежных средств и обратиться с просьбой о блокировании доступа и внеплановой замене ключевой информации.

3.5. Произвести фотосъёмку рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину. При необходимости ведения хозяйственной деятельности – задействовать другое ЭУ.

3.6. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видео-наблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

3.7. Провести сбор записей с межсетевых экранов, серверов баз данных и иных компонент клиентского приложения СУД, систем авторизации пользователей (AD, NDS и т.д.), ЭУ, используемых для управления денежными средствами через СУД, устройств, которые могут использоваться для удалённого управления указанными ЭУ.

3.8. В течение одного рабочего дня с момента выявления хищения денежных средств обратиться с письменным заявлением к своему Интернет-провайдеру (Приложение № 1 к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

3.9. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

3.10. Зафиксировать в протокольной форме значимые действия и события, в том числе действия с ЭУ, подключенным к СУД, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании ЭУ в целях, отличных от осуществления операций в СУД, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

3.11. Все действия, указанные в пп. 3.1, 3.2, 3.4, 3.5, 3.7, 3.10 настоящего раздела, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъёмки.

3.12. В течение одного рабочего дня с момента выявления хищения денежных средств обратиться с заявлением в правоохранительные органы по месту регистрации клиента о возбуждении уголовного дела по факту хищения денежных средств (Приложение № 2 к настоящим Рекомендациям).

3.13. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона КУСП (Книга учета сообщений о происшествиях), содержащую отметку правоохранительного органа о его приеме.

4. Действия клиента при выявлении попытки хищения денежных средств в СУД.

4.1. Незамедлительно проинформировать Банк о произошедшей ситуации установленным образом, обратившись к менеджеру услуги по телефону (343) 264-55-19 (круглосуточно) или к менеджеру счета по телефону, указанному в договоре на обслуживание в СУД,

4.2. Незамедлительно, но не позднее, чем в течение трех рабочих дней с момента выявления попытки хищения денежных средств, направить уведомление о возникновении конфликтной ситуации в Банк с письменным заявлением о разъяснении произошедшей ситуации, в связи с выявлением попытки хищения денежных средств через СУД (см. Порядок проведения экспертизы при возникновении конфликтных ситуаций (разногласий)).

4.3. По возможности выполнить действия в пп. 3.1, 3.4, 3.5, 3.7, 3.10 с учетом рекомендации п. 3.11, с целью сохранения каких либо доказательств неправомерного доступа к компьютерной информации.

4.4. В течение одного рабочего дня с момента выявления попытки хищения денежных средств дня обратиться с письменным заявлением к своему Интернет-провайдеру (Приложение № 1 к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

4.5. Обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту неправомерного доступа к компьютерной информации (Приложение № 3 к настоящим Рекомендациям).

Начальник управления
безопасности информационных систем А.Н. Падерин

В.С. Середницкий
(343)228-17-59

Приложение № 1
к Рекомендациям для клиентов ПАО КБ «УБРиР» при выявлении случаев хищения (попытки хищения) денежных средств в системах удаленного доступа («Интернет-банк», «Банк-клиент»)

РЕКОМЕНДУЕМАЯ ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

_____
должность руководителя

_____
наименование организации

_____
ФИО

от _____
должность, ФИО заявителя

проживающего: _____

_____
адрес места жительства

паспорт: _____

_____
номер паспорта, дата выдачи, кем и когда выдан

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____

_____

_____
почтовый адрес

Уважаемый (ая) _____
имя, отчество руководителя

«____» _____ 20___ года в ___:___ по местному времени со счета _____ по системе удаленного доступа _____ (указать тип системы) был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого осуществляется подключение к системе удаленного доступа, располагается по адресу _____ и использует IP-адрес ___.___.___.___.

Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением, кража логина, пароля и секретных ключей системы удаленного доступа.

«____» _____ 20__ года между _____ и вами был заключен договор № _____ об оказании _____ услуг.

Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «____» _____ 20___ года по «____» _____ 20___ года с указанием времени соединения, IP и MAC адресов.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 2
к Рекомендациям для клиентов ПАО КБ «УБРиР» при выявлении случаев хищения (попытки хищения) денежных средств в системах удаленного доступа («Интернет-банк», «Банк-клиент»)

РЕКОМЕНДУЕМАЯ ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Начальнику ОВД по _____
наименование ОВД

от _____
должность, ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: _____
номер паспорта, дата выдачи, кем и когда выдан

место работы _____
наименование организации

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими «_____»
наименование организации

денежными средствами (кражи) с использованием системы удаленного доступа (далее – СУД) «_____» (указать тип системы) ПАО КБ «УБРиР».

_____ 201__ г. неизвестными лицами в СУД был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа: _____

Номер платежного поручения: _____

Наименование банка плательщика: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____[1].

Оснований для данного денежного перевода нет: с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним; перевод расцениваю как хищение денежных средств.

Признаком хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт появления этого перевода был установлен «____» _____ 201__ г.

[1] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

_____

ФИО лица, установившего факт несанкционированного перевода, должность, наименование организации

при _____.

обстоятельства обнаружения факта несанкционированного перевода

Электронное устройство, с которого осуществляется подключение к СУД, располагается по адресу _____, доступ к электронному устройству ограничен, прямая кража реквизитов доступа (учетной записи, пароля и секретных ключей) маловероятна.

Вероятной причиной этого несанкционированного перевода считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в СУД

2. _____.
наблюдавшиеся сбои, нехарактерное поведение СУД и рабочего места СУД

3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__ г.

«___» _____ 20__г. _____ / /

подпись

Приложение № 3
к Рекомендациям для клиентов ПАО КБ «УБРиР» при выявлении случаев хищения (попытки хищения) денежных средств в системах удаленного доступа («Интернет-банк», «Банк-клиент»)

РЕКОМЕНДУЕМАЯ ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО ФАКТУ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Начальнику ОВД по _____
наименование ОВД

от _____
должность, ФИО заявителя

проживающего: _____
дрес места жительства

паспорт: _____
номер паспорта, дата выдачи, кем и когда выдан

место работы _____
наименование организации

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту неправомерного доступа к компьютерной информации (ключевая информация для работы с системой удаленного доступа (далее – СУД), сведения о банковских операция в СУД), принадлежащими «_____»
наименование организации

_____ 201__ г. неизвестными лицами в СУД _____ (указать тип системы) была осуществлена попытка несанкционированного перевода денежных средств со следующими реквизитами:

Дата платежа: _____

Номер платежного поручения: _____

Наименование банка плательщика: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____[2].

Оснований для данного денежного перевода нет: с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним; попытку перевода расцениваю как неправомерный доступ к компьютерной информации, который мог повлечь финансовый ущерб.

Признаком попытки хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт появления этого перевода был установлен «____» _____ 201__ г. _____

[2] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

ФИО лица, установившего факт наличия несанкционированного перевода, должность, наименование организации

при _____.

обстоятельства обнаружения факта наличия несанкционированного перевода

Электронное устройство, с которого осуществляется подключение к СУД, располагается по адресу _____, доступ к электронному устройству ограничен, прямая кража реквизитов доступа (учетной записи, пароля и секретных ключей) маловероятна.

Вероятной причиной осуществления попытки этого несанкционированного перевода считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в СУД

2. _____.
наблюдавшиеся сбои, нехарактерное поведение СУД и рабочего места СУД

3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__ г.

«___» _____ 20__г. _____ / /

подпись