

Приложение №9

(утверждено Приказом от 27 июня 2014 г. №387)
к Правилам «Электронного документооборота с использованием системы «iBank 2» в Акционерном коммерческом ипотечном банке «АКИБАНК» (публичное акционерное общество)»

РЕКОМЕНДАЦИИ КЛИЕНТУ О ДЕЙСТВИЯХ В СЛУЧАЕ ПОПЫТКИ ИЛИ НЕСАНКЦИОНИРОВАННОГО СПИСАНИЯ ДЕНЕЖНЫХ СРЕДСТВ С ЕГО РАСЧЕТНОГО СЧЕТА

Клиенту в случае попытки несанкционированного списания денежных средств с расчетного счета Клиента необходимо руководствоваться пунктами 1-5, 15 настоящих рекомендаций, в случае хищения денежных средств с расчетного счета Клиента – пунктами 1-15 рекомендаций:

1. Немедленно прекратить любые действия с электронными устройствами (далее - ЭУ): персональный компьютер, ноутбук, планшетный компьютер и т.п., подключенным к Системе «iBank 2», обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.), отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим). При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2. Отозвать перевод денежных средств, обратившись немедленно к специалисту отдела операционного обслуживания в ПАО «АКИБАНК» по телефону с требованием о блокировке доступа Клиента к системе «iBank 2», приостановке исполнения платежа или на номер Службы поддержки клиентов ПАО «АКИБАНК» **8-800-100-25-42**.

3. Проинформировать все банки, с которыми Клиент имеет договорные отношения, предусматривающие использование дистанционного банковского обслуживания (далее - ДБО), о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

4. Дополнительно обратиться в ПАО «АКИБАНК» с письменным заявлением об отзыве платежа, приостановлении платежа, блокировании доступа к системе «iBank 2» ([Приложение 9.1](#)), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк в течение одного рабочего дня.

5. Направить в ПАО «АКИБАНК» Справки по факту инцидента информационной безопасности в системе «iBank 2» ([Приложение 9.2](#)), а также подтверждающие документы при их наличии ([Приложение 9.3](#)) в срок не позже следующего рабочего дня после фиксирования инцидента.

6. В целях сохранения доказательной базы 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.

7. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ) ([Приложение 9.4](#)). Копию заявления предоставить в отдел операционного обслуживания Банка в срок не более 2 рабочих дней со дня выявления факта хищения денежных средств.

8. 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,

содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме, а также документы подтверждающие неправомерность списания денежных средств с расчетного счета. Обращаем внимание на то, что ходатайство необходимо направлять в суд по почте либо нарочно (отправка ходатайства через сервис «Мой арбитр» недопустима).

9. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи ([Приложение 9.5](#)) для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

10. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), 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 заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

11. 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 (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

12. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы «iBank 2», систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через систему «iBank 2» Банка, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

13. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе «iBank 2», предшествовавшие факту хищения денежных средств, подготовить объяснения Клиента (работников Клиента) об использовании ЭУ в целях, отличных от осуществления операций в системе «iBank 2», посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

14. Все действия, указанные в пп. 1, 10, 11, 12, 13 настоящих рекомендаций, производить с привлечением специалистов соответствующих служб Клиента, протоколировать и документировать, в т.ч. с использованием фотосъемки.

15. После окончания процедуры смены ключей не возобновлять деятельность на данной рабочей станции без проведения соответствующих технических мер, которые гарантируют полное уничтожение вирусных объектов. Если средствами антивирусных программ они не обнаружены, рекомендуется провести переустановку операционной системы с полным форматированием жесткого диска, но только в том случае, когда уже не требуется сохранение доказательной базы в целях проведения расследования инцидента правоохранительными органами и рассмотрения судебного иска. В случае необходимости сохранения персонального компьютера в текущем состоянии, использовать в работе другой компьютер с установленным лицензионным программным обеспечением (операционные системы, офисные пакеты и пр.) и его автоматическим обновлением. Рекомендуемые для проверки, а в дальнейшем и еженедельные, следующие средства: <http://www.kaspersky.ru/virusscanner>, <http://freedrweb.com>

Приложение № 9.1.

к Приложению № 9 «Рекомендации клиенту в случае попытки или несанкционированного списания денежных средств с его расчетного счета» к Правилам электронного документооборота с использованием системы "iBank 2" в ПАО «АКИБАНК», утвержденным приказом от 27 июня 2014 г. №387.

**ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА В БАНК ПЛАТЕЛЬЩИКА
ОБ ОТЗЫВЕ ПЛАТЕЖА, БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ "iBank 2"**

_____ (должность руководителя)

_____ (наименование банка)

_____ (Фамилия И.О.)

Уважаемый(ая) _____
(имя, отчество руководителя)

“ ____ ” _____ 201__ года с нашего банковского счета, открытого в Вашем банке, по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации, были переведены со следующими реквизитами платежа:

Дата платежа: _____

Номер распоряжения: _____

Наименование банка плательщика: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____

Прошу Вас заблокировать нашу учетную запись в системе "iBank 2", провести процедуру компрометации всех ключей ЭП и оказать содействие в приостановлении прохождения платежа и отзыве платежа.

Должность руководителя

подпись

Ф.И.О.

Исп.

Тел.

Приложение № 9.2.

к Приложению № 9 «Рекомендации клиенту в случае попытки или несанкционированного списания денежных средств с его расчетного счета» к Правилам электронного документооборота с использованием системы «iBank 2» в ПАО «АКИБАНК», утвержденным приказом от 27 июня 2014 г. №387.

**ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ «iBank 2»**

« _____ » _____ 20 _____ неустановленным лицом через систему «iBank 2» была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____

Номер распоряжения: _____

Наименование банка плательщика: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____

Дополнительно сообщая:

Количество ЭУ, настроенных для доступа в систему «iBank 2»: _____

Для доступа в системы «iBank 2» хотя бы раз использовались

- корпоративные ЭУ
- личные ЭУ
- ЭУ, находящиеся в общественном пользовании

Периодичность смены пароля системы «iBank 2»: _____

Применяемые элементы безопасности ЭУ включают:

- соблюден порядок подготовки ЭУ к установке системы «iBank 2»
- используется только программное обеспечение для работы системы «iBank 2»
- Замечали ли перебои в работе компьютера, системы
- Получали ли предупреждения о наличии вредоносных программ
- USB-токен вынимается из компьютера после работы в АРМ - клиента
- используется только лицензионное программное обеспечение
- операционная система и приложения обновляются в автоматическом режиме
- используется антивирусное программное обеспечение: _____
- антивирусное программное обеспечение обновляется ежедневно
- из числа съемных носителей информации на ЭУ используются только ключевые носители

- передача файлов и обмен сообщениями электронной почты на ЭУ ограничены
- целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью _____

- используются средства сетевой защиты: _____
- на ЭУ запрещены входящие соединения из сети Интернет
- с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____

- обеспечивается возможность доступа к ЭУ только уполномоченных лиц
- обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: _____

(подпись плательщика)

- Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

Заявление в правоохранительные органы принято в ОВД _____

(район, округ, город, субъект федерации и иные идентифицирующие ОВД данные)

и зарегистрировано за № _____ в КУСП

- Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелегального и контрафактного программного обеспечения в соответствии со статьей 146 Уголовного кодекса Российской Федерации предупрежден.

Заявитель: _____ / _____ /

Дата: _____ /Телефон: _____

Приложение № 9.3.

к Приложению № 9 «Рекомендации клиенту в случае попытки или несанкционированного списания денежных средств с его расчетного счета» к Правилам электронного документооборота с использованием системы "iBank 2" в ПАО «АКИБАНК», утвержденным приказом от 27 июня 2014 г. №387.

**ПЕРЕЧЕНЬ
ДОКУМЕНТОВ, КОТОРЫЕ НЕОБХОДИМО ПРЕДОСТАВИТЬ ПЛАТЕЛЬЩИКОМ
БАНКУ В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ.**

1. Копия лицензии на операционную систему ПК.
2. Копия чека на приобретение операционной системы ПК.
3. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).
4. Копия договора на оказание телематических услуг информационно-телекоммуникационной сети Интернет.
5. Описание организации доступа в сеть Интернет на рабочем месте.
6. Копия чека на оказание доступа в сеть Интернет на повременной основе.
7. Копия заявления в правоохранительные органы.
8. Копия лицензии на антивирусное ПО.
9. Копия чека на антивирусное ПО.
10. Описание по антивирусной защите рабочего места (наличие установленного на жестком диске автоматизированного рабочего места клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на автоматизированном рабочем месте клиента вредоносных программ).
11. Описание системы защиты информации (наличие или отсутствие персонального межсетевое экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности - интернет-серфинга, сведения о порядке хранения и использования ключевых носителей).

Приложение № 9.4.

к Приложению № 9 «Рекомендации клиенту в случае попытки или несанкционированного списания денежных средств с его расчетного счета» к Правилам электронного документооборота с использованием системы "iBank 2" в ПАО «АКИБАНК», утвержденным приказом от 27 июня 2014 г. №387.

**РЕКОМЕНДУЕМАЯ ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО)
В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО ФАКТУ
ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ**

Начальнику ОВД по _____
(наименование ОВД)
от _____
(должность, Ф.И.О. 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/Ф.И.О. потерпевшего)

денежными средствами (кражи) с использованием системы дистанционного банковского обслуживания "iBank 2" (далее – ДБО) “ _____ ”
(наименование банка)

_____ 201__ г. неизвестными лицами по системе ДБО 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 получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____

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 был осуществлен не уполномоченными лицами.

Факт появления этого перевода был установлен “ ____ ” _____ 201__ г.

(Ф.И.О. лица, установившего факт несанкционированного перевода, должность, наименование организации)

при _____ .

(обстоятельства обнаружения факта несанкционированного перевода)

Электронное устройство, с которого осуществляется подключение к системе ДБО, 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 (нужное подчеркнуть) ввод, удаление, блокирование, модификацию компьютерной информации, 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 систему ДБО)
2. _____ ;
(наблюдавшиеся сбои, нехарактерное поведение системы ДБО и рабочего места системы ДБО)
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)

Об уголовной ответственности за заведомо ложный донос по ст. 306 УК РФ предупрежден.

(подпись)

(_____)
(расшифровка подписи)

Приложение № 9.5.

к Приложению № 9 «Рекомендации клиенту в случае попытки или несанкционированного списания денежных средств с его расчетного счета» к Правилам электронного документооборота с использованием системы "iBank 2" в ПАО «АКИБАНК», утвержденным приказом от 27 июня 2014 г. №387.

**РЕКОМЕНДУЕМАЯ ФОРМА ПИСЬМА ИНТЕРНЕТ-ПРОВАЙДЕРУ
О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)**

_____ (должность руководителя)

_____ (наименование организации)

_____ (Ф.И.О.)

от _____ (должность, Ф.И.О. 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 московскому времени со счета

по системе дистанционного банковского обслуживания (ДБО) был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого осуществляется подключение к системе ДБО, 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 ДБО.

“ ____ ” _____ 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 руководителя
Исп. тел.

подпись

Ф.И.О.