Утверждено
Решением Правления
АО «Таганрогбанк»

(протокол № 47 от 20.09.2021 г.)

ИНСТРУКЦИЯ
клиентам АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

Введено с 20.09.2021 года
приказом № 190 от 20.09.2021 г.

Таганрог
2021

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СКОРАЩЕНИЯ

1.1. **Банковский технологический процесс** - технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг.
1.2. **Банк** – Акционерное общество «Акционерный городской банк «Таганрогбанк».
1.3. **Закрытый ключ** - криптографический ключ (уникальная последовательность символов), известный только владельцу ключа (клиенту или Банку соответственно) и хранимый владельцем в тайне.
1.4. **Клиент -** клиент АО «Таганрогбанк», с которым заключен соответствующий договор о порядке обмена документами в электронном виде с использованием системы «Интернет-банк «iBank 2».
1.5. **Компрометация ключа -** утрата доверия к тому, что используемые ключи обеспечивают возможность установления авторства и неизменности содержания электронного документа.
1.6. **Криптографический ключ -** конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всех возможных для данного алгоритма преобразований.
1.7. **Несанкционированный доступ -** доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системой.
1.8. **Носитель ключевой информации -** аппаратное USB-устройство генерации и хранения ключей электронной подписи (USB-токен Рутокен ЭЦП 2.0).
1.9. **Электронная подпись -** реквизит электронного документа, полученный в результате криптографического преобразования информации, который позволяет получателю электронного документа удостовериться в его авторстве и неизменности его содержания, в том числе в отсутствии подделки или искажения со стороны получателя или третьих лиц.
1.10. **АРМ -** устройство Клиента, используемое в качестве удаленного рабочего места для целей управления денежными средствами клиента в системе дистанционного банковского обслуживания.
1.11. **ДБО –** дистанционное банковское обслуживание.
1.12. **ИБ –** информационная безопасность.
1.13. **ИТ –** информационные технологии.
1.14. **НСД –** несанкционированный доступ.
1.15. **Система ДБО –** система дистанционного банковского обслуживания «Интернет-Банк «iBank 2».
1.16. **СКЗИ –** средство криптографической защиты информации.
1.17. **ЭП –** электронная подпись.
1.18. **КУСП** – книга учета сообщений о правонарушениях. При подаче письменной заявки непосредственно в отделение полиции заявителю выдается талон с номером КУСП, присвоенным его заявлению в КУСП, который должен совпадать с данными корешка талона в полиции.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Использование системы ДБО связано с повышенным риском возможного НСД третьих лиц к защищаемой информации. Последствиями НСД могут быть списание денежных средств со счета Клиента или утечка конфиденциальной информации о совершаемых Клиентом операциях.

2.2. Настоящая Инструкция определяет требования и рекомендации по обеспечению информационной безопасности в процессе эксплуатации системы ДБО, выполнение которых позволит Клиенту Банка снизить возможные риски ИБ, а также порядок действий Клиентов в случае обнаружения инцидентов информационной безопасности, связанных с хищением денежных средств в процессе эксплуатации системы ДБО.

2.3. Данная инструкция разработана на основании:

— Пункта 7 «Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;

— «Методическими рекомендациями по усилению кредитными организациями информационной работы с клиентами в целях противодействия несанкционированным операциям» от 19 февраля 2021г. №3-МР;

— Эксплуатационной и технической документации на систему дистанционного банковского обслуживания «iBank 2» и используемые в процессе осуществления услуг средства защиты информации.

2.4. Рекомендации указанные в настоящей Инструкции не заменяют, а дополняют и расширяют перечень мер по обеспечению информационной безопасности указанные в Приложении №3 к Дополнительному соглашению №1 к форме Договора банковского счета в валюте Российской Федерации между Банком и Клиентом (его представителем).

3. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИБ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ ДБО

3.1. Рекомендации по обеспечению ИБ АРМ:

3.1.1. Информационная безопасность АРМ, с использованием которого осуществляется работа в Системе ДБО, должна обеспечиваться за счет реализации комплекса организационных и технических мер.

3.1.2. В целях работы с Системой ДБО рекомендуется организовать отдельный АРМ. Оборудование АРМ должно размещаться в служебных помещениях, для которых обеспечен режим ограниченного доступа и исключается присутствие посторонних лиц.

3.1.3. Рекомендуется использовать на АРМ исключительно лицензионное программное обеспечение и регулярно его обновлять.

3.1.4. В операционной системе для каждого допущенного к работе в Системе ДБО работника Клиента должна быть заведена уникальная учетная запись с ограниченными правами. Доступ к файловым ресурсам компьютера должен быть ограничен минимально необходимыми правами в соответствии с реализуемыми функциональными обязанностями.

3.1.5. Стандартные учетные записи (Пользователь, Администратор) операционной системы АРМ рекомендуется переименовать, установить пароли для доступа к ним. Административная учетная запись (имеющая права уровня Администратор) должна использоваться исключительно в процессе установки и конфигурирования АРМ. Гостевую учетную запись (Guest) рекомендуется отключить.

3.1.6. Для каждой учетной записи рекомендуется установить пароли длиной не менее 8 символов, содержащие буквы из различных регистров (заглавные и строчные), специальные символы (*, &, л, % и т.п.) и цифры. Пароли рекомендуется изменять с периодичностью не меньшей, чем один раз в три месяца.

3.1.7. Для административных учетных записей (имеющих права Администратор) рекомендуется установить пароли длиной не менее 16 символов, с применением требований к сложности пароля согласно пункту 3.1.6.

3.1.8. Рекомендуется полностью блокировать сетевой доступ к ресурсам АРМ с других рабочих станций. Сетевое оборудование, обеспечивающее доступ организации в

сеть Интернет, должно блокировать любые сетевые пакеты, передаваемые с АРМ на серверы, не относящиеся к Системе ДБО, веб-сайту Банка, службам обновления установленного программного обеспечения и антивирусных баз.

3.1.9. Рекомендуется АРМ для работы с системой ДБО выносить в отдельный VLAN.

3.1.10. Рекомендуется исключить возможность загрузки и использования операционной системы, отличной от установленной на АРМ (например, отключив в BIOS функцию загрузки с CD/DVD приводов, USB- flash дисков и т. п.). Доступ к изменению настроек BIOS АРМ должен быть защищен надежным паролем.

3.1.11. На АРМ должно быть установлено лицензионное средство антивирусной защиты. По возможности на АРМ также рекомендуется установить персональный межсетевой экран.

3.1.12. Рекомендуется использовать на границе периметра локальной вычислительной сети средства межсетевого экранирования, обнаружения/предотвращения вторжений (IDS /IPS) и потокового антивирусного сканирования.

3.1.13. Обновление антивирусных баз следует проводить не реже одного раза в сутки. Полное антивирусное сканирование всех машинных носителей информации следует проводить не реже одного раза в неделю. Все съёмные электронные носители, подключаемые к АРМ (DVD/CD, USB- flash носители и др.) рекомендуется проверять на предмет наличия вирусов.

3.1.14. По возможности следует настроить автоматическое обновление баз сигнатур антивирусных средств.

3.1.15. Обновление сигнатур средств обнаружения/предотвращения вторжений (IDS/IPS) рекомендуется осуществлять не реже одного раза в неделю.

3.2. Защита от НСД путем использования ложных (фальсифицированных) ресурсов сети Интернет:

3.2.1. При осуществлении переводов денежных средств с использованием Системы ДБО существует риск получения несанкционированного доступа к защищаемой информации путем использования ложных ресурсов сети Интернет лицами, не обладающими правом распоряжения этими денежными средствами. Для реализации данного риска злоумышленник может создать копию сайта, с помощью которого осуществляется взаимодействие с Системой ДБО, внешне неотличимую от настоящего ресурса. Информация, вводимая на таком ложном ресурсе, в том числе, логины и пароли для доступа в Систему ДБО, будет отправляться не на сервера Банка, а злоумышленнику. Попадание на такой сайт-копию возможно, например, с различных внешних ссылок, на которых установлена переадресация на сайт злоумышленника, из рассылок электронных писем и пр.

3.2.2. С целью снижения указанного риска Клиентам рекомендуется:

3.2.2.1. Для входа в систему ДБО набирать в адресной строке Интернет-браузера «`https://ibank.tagbank.ru`».

3.2.2.2. Перед вводом логина и пароля для доступа в Систему ДБО проверить подлинность сайта `ibank.tagbank.ru` по данным TLS/SSL-сертификата. В этих целях необходимо просмотреть сведения о сертификате - вкладка Состав. В поле субъект должна быть указана следующая информация:

— Общее имя (CN): «`ibank.tagbank.ru`»;

— Организация (O): «`JSC Taganrogbank`».

3.2.2.3. В качестве удостоверяющего центра, подтверждающего принадлежность сервера «`ibank.tagbank.ru`» Банку, используется центр сертификации компании `DigiCert Inc`. Сведения об издателе должны быть следующие:

КЕМ ВЫДАН:

— Общее имя (CN): «`Thawte EV RSA CA 2018`»;

— Организация (O): «`DigiCert Inc.`».

3.3. Обеспечение ИБ носителей ключевой информации:

3.3.1. Порядок хранения и использования носителей ключевой информации с секретными ключами должен исключать возможность несанкционированного доступа к ним. Для хранения носителей ключевой информации должны устанавливаться металлические сейфы.

3.3.2. Доступ работников Клиента к носителям ключевой информации должен осуществляться на основании приказа или распоряжения руководства Клиента согласно закрепленных за ними функций и полномочий.

3.3.3. Носители ключевой информации должны использоваться только допущенными работниками. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

3.3.4. После окончания рабочего дня, а также вне времени сеансов связи с Банком носители ключевой информации должны быть отключены от АРМ. Неиспользуемые в настоящий момент носители ключевой информации должны храниться в сейфе.

3.3.5. Хранение носителей ключевой информации допускается в одном сейфе с другими документами, если при этом исключается возможность несанкционированного доступа к ним.

3.3.6. Не допускается:

— передача носителей ключевой информации лицам, к ним не допущенным;
— вывод закрытых ключей на дисплей или принтер;
— изготовление копий криптографических ключей без санкции уполномоченных лиц;
— использование носителя ключевой информации на автоматизированных рабочих местах, отличных от АРМ определенного для работы с Системой ДБО.

3.4. Использование дополнительных мер по обеспечению ИБ:

3.4.1. В целях снижения рисков информационной безопасности, возникающих в ходе эксплуатации Системы ДБО, Клиенту Банка рекомендуется:

— использовать для подписания электронных платёжных документов ЭП в соответствии с сочетаниями подписей, указанных в Договоре банковского счета.
— хранить носители ключевой информации в различных местах (сейфах, запираемых шкафах и пр.), что снизит вероятность их одновременной кражи злоумышленниками.

3.4.2. В целях обеспечения информационной безопасности в процессе эксплуатации Системы ДБО Клиенты Банка при необходимости могут попросить подключить дополнительно услугу:

— «IP-фильтрация» - дополнительная услуга, предоставляющая возможность каждому Клиенту осуществлять взаимодействие с системой ДБО только с определенных IP-адресов и IP-подсетей. Использование встроенного в систему ДБО механизма IP - фильтрации ограничивает возможности Клиента работать с системой при подключении к Интернету из произвольного места, но при этом делают задачу хищения средств злоумышленником трудновыполнимой.

3.4.3. Подключение указанной выше услуги, приведённой в пункте 3.4.2, осуществляется на основании Заявления о дополнительной защите, принятого Банком (Приложение 2 к «Правилам дистанционного банковского обслуживания корпоративных клиентов в АО «Таганрогбанк»).

4. ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА В СЛУЧАЕ ВЫЯВЛЕНИЯ ФАКТОВ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

4.1. В случае выявления фактов хищения денежных средств в Системе ДБО необходимо:

4.1.1. Немедленно прекратить любые действия с АРМ, с использованием которого осуществляется подключение к Системе ДБО, обесточить ее (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 к ЛВС, USB, Wi-Fi, 3-G модем и др.) или перевести АРМ в режим гибернации (энергосберегающий режим операционной системы АРМ, позволяющий сохранять содержимое оперативной памяти на энергонезависимое устройство хранения данных (жёсткий диск) перед выключением питания.).

4.1.2. При наличии технической возможности необходимо отозвать перевод с использованием иной АРМ, после чего заблокировать Систему ДБО.

4.1.3. При отсутствии технической возможности отозвать перевод по Системе ДБО необходимо **незамедлительно обратиться в Банк** по телефону с заявлением о приостановке исполнения платежа и возврате денежных средств (контактная информация приведена в Приложении 7 к Инструкции).

4.1.4. Произвести фотофиксацию АРМ и её расположения в помещении. Обеспечить сохранность (целостность) АРМ как возможного средства совершения преступления, поместив ее 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. При необходимости ведения хозяйственной деятельности - задействовать другую АРМ.

4.1.5. Обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к Системе ДБО (Приложение 1 к Инструкции), а также о компрометации ключей незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции. Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть предоставлен в Банк **течение одного дня**.

4.1.6. Проинформировать все банки, с которыми Клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

4.1.7. 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.

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

4.1.9. В течение одного дня обратиться с письменным заявлением к своему Интернет-провайдеру (Приложение 3 к Инструкции) для получения в электронной форме журналов соединений с сетью Интернет с использованием АРМ или из ЛВС Клиента как минимум за три месяца, предшествовавшие факту хищения денежных средств.

4.1.10. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности АРМ, не отправлять АРМ в сервисные службы ИТ (сторонние сервисные организации) для восстановления работоспособности.

4.1.11. Зафиксировать в протокольной форме значимые действия и события, в том числе действия с АРМ, с использованием которого осуществляется подключение к

Системе ДБО, предшествовавшие факту хищения денежных средств; подготовить объяснения работников Клиента об использовании АРМ в целях, отличных от осуществления операций в Системе ДБО, посещаемых сайтах, о странностях при работе с АРМ, перебоях или отказах АРМ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения АРМ и т.д.

4.1.12. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (Приложение 4 к Инструкции).

4.1.13. В установленные законодательством Российской Федерации сроки и порядке 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, содержащую отметку правоохранительного органа о его приеме.

4.1.14. Копии вышеуказанных документов по перечню, в Приложении 6 к Инструкции, направить в Банк с приложением Справки по факту инцидента информационной безопасности в системе ДБО (Приложение 5 к Инструкции).

4.2. Все действия, указанные в пп. 4.1.1, 4.1.4, 4.1.7, 4.1.9, 4.1.11. необходимо производить коллегиально, результаты их проведения должны быть запротоколированы и документированы.

ПРИЛОЖЕНИЕ 1
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В БАНК ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДБО

Председателю Правления АО «Таганрогбанк»
_____

Уважаемая _____, « _____ » _____ 202 __ года с нашего расчетного счета, открытого в Вашем банке, по системе дистанционного банковского обслуживания «Интернет-банк «iBank 2» были похищены денежные средства, которые, по имеющейся информации, были переведены со следующими реквизитами платежа:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: АО «Таганрогбанк» _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____
(для случаев перевода электронных денежных средств - указать реквизиты перевода)

_____ _____
(должность) *(подпись),*

_____
(расшифровка подписи)

Прошу Вас заблокировать нашу учетную запись в системе ДБО, провести процедуру компрометации всех ключей ЭП и оказать содействие в возврате денежных средств.

Исп.:
ФИО
тел.
«___»_____202__г.

ПРИЛОЖЕНИЕ 2
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

_____ _____
(должность руководителя) *(наименование организации)*

_____
(ФИО, полностью)

Уважаемый (ая)

_____
(имя, отчество руководителя)

«___ » _____ _____ 202___ года с нашего расчетного счета были похищены денежные средства, которые, по информации, полученной из АО «Таганрогбанк», были переведены со следующим реквизитам платежа:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: АО «Таганрогбанк»
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя:
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя:_____
Сумма платежа: _____
Назначение платежа: _____
(для случаев перевода электронных денежных средств - указать реквизиты перевода)

_____ _____
(должность) *(подпись),*

_____
(расшифровка подписи)

Прошу Вас оказать содействие в приостановлении прохождения платежа и возврате денежных средств.

Исп.:
ФИО
тел.
«___»_____202__г.

ПРИЛОЖЕНИЕ 3
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

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

_____ _____
(должность руководителя) *(наименование организации)*

_____
(ФИО, полностью)

ОТ _____
(должность, ФИО заявителя)

место работы: _____
(наименование организации)

контактный телефон: _____
(телефон заявителя)

адрес для корреспонденции _____
(почтовый адрес)

Уважаемый (ая) _____ _____ ,
(имя, отчество руководителя)

«___ » _____ 202 _ года в _____ : __ по московскому времени со счета _____ по системе дистанционного банковского обслуживания (ДБО) был осуществлен несанкционированный перевод денежных средств. АРМ (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.

«_____ » _____ 202 __ 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 « _____ » _____ 202____ года по « _____ » _____ 202 ___ года с указанием времени соединения, IP и MAC адресах.

_____ _____
(должность) *(подпись),*

_____
(расшифровка подписи)

Исп.:
ФИО
тел.
«___»_____202__г.

ПРИЛОЖЕНИЕ 4
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

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 дистанционного банковского обслуживания (далее - ДБО) АО «Таганрогбанк».

_____ 202 ___ г. неизвестными лицами по системе ДБО был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: АО «Таганрогбанк» _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____
(для случаев перевода электронных денежных средств - указать реквизиты перевода)

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 « _____ » _____ 202 __ г.
(ФИО лица, установившего факт несанкционированного перевода, должность, наименование организации)
при_____

_____
(обстоятельства обнаружения факта несанкционированного перевода)

АРМ (рабочая станция), с которой осуществляется подключение к системе ДБО, располагается по адресу _____ , доступ к АРМ (рабочей станции) 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 систему ДБО)

2. _____ ;
(наблюдавшиеся сбои, нехарактерное поведение системы ДБО и рабочего места системы ДБО)

3. _____ .
(иное)

_____ _____
(должность) *(подпись),*

_____
(расшифровка подписи)

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.

202 __ г. _____ / _____
(*ФИО*) (*подпись*)

ПРИЛОЖЕНИЕ 5
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

СПРАВКА ПО ФАКТУ ИНЦИДЕНТА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

«_____ » _____ 202 _ неустановленным лицом через систему ДБО была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: АО «Таганрогбанк» _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____
(для случаев перевода электронных денежных средств - указать реквизиты перевода)

Количество АРМ (рабочих станций), настроенных для доступа в систему ДБО: _____ .

1. Для доступа в системы ДБО хотя бы раз использовались:
   - □ корпоративные АРМ;
   - □ личные АРМ;
   - □ АРМ, партнеров и/или сторонних организаций;
   - □ АРМ, находящиеся в общественном пользовании.

   (*установить □ в необходимом пункте*)
2. Периодичность смены пароля системы ДБО: _____
3. Применяемые элементы безопасности АРМ включают:
   - 3.1. Соблюден порядок подготовки АРМ к установке системы ДБО:
     - — используется только программное обеспечение для работы системы ДБО;
     - — используется только лицензионное программное обеспечение;
     - — операционная система и приложения обновляются в автоматическом режиме;
   - 3.2. Используется антивирусное программное обеспечение:
     - — следующих производителей: _____;
     - — антивирусное программное обеспечение обновляется ежедневно.
   - 3.3. Из числа съемных носителей информации на АРМ используются только ключевые носители.
   - 3.4. Передача файлов и обмен сообщениями электронной почты на АРМ ограничены.
   - 3.5. Целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью_____.
   - 3.6. Используются средства сетевой защиты: _____.
   - 3.7. На АРМ запрещены входящие соединения из сети Интернет.
   - 3.8. С АРМ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных ресурсов сети Интернет составляет _____.

3.9. Обеспечивается возможность доступа к АРМ только уполномоченных лиц.
3.10. Обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц.

Иная информация, имеющая отношение к инциденту: _____

Подтверждаю отсутствие у меня претензий к АО «Таганрогбанк».

_____ / _____ /
(подпись клиента) *(расшифровка подписи)*

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. _____ / _____ /
(подпись клиента) *(расшифровка подписи)*

О необходимости предоставления доступа сотрудников правоохранительных органов к АРМ (рабочей станции), об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

Заявитель: _____ / _____ /
(подпись) *(расшифровка подписи)*

Дата: _____ /Телефон: _____

ПРИЛОЖЕНИЕ 6
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, КОТОРЫЕ МОГУТ БЫТЬ ИСТРЕБОВАНЫ У КЛИЕНТА В СЛУЧАЕ ВЫЯВЛЕНИЯ ФАКТОВ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМЕ ДБО

1. Копия лицензии на операционную систему АРМ.
2. Копия чека на приобретение операционной системы АРМ.
3. Описание используемого программного обеспечения (перечень использованного лицензионного программного обеспечения на АРМ (автоматизированном рабочем месте), информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).
4. Копия договора на оказание телематических услуг (услуга удаленного доступ к информации) информационно-телекоммуникационной сети Интернет.
5. Описание организации доступа в сеть Интернет на АРМ (автоматизированном рабочем месте).
6. Копия чека на оказание услуг доступа в информационно-телекоммуникационную сеть Интернет на повременной основе.
7. Копия заявления в правоохранительные органы.
8. Копия лицензии на антивирусное программное обеспечение.
9. Копия чека на антивирусное программное обеспечение.
10. Описание организации антивирусной защиты АРМ (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 межсетевого экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности – применение сети Интернет в иных целях (посещение веб-сайтов не относящихся к выполняемым задачам), сведения о порядке хранения и использования ключевых носителей).

ПРИЛОЖЕНИЕ 7
к «Инструкции клиенту АО «Таганрогбанк» по обеспечению информационной безопасности в процессе эксплуатации системы дистанционного банковского обслуживания «Интернет-банк «iBank 2»

КОНТАКТНАЯ ИНФОРМАЦИЯ

Наименование полное:
Акционерное общество «Акционерный городской банк «Таганрогбанк».

Наименование сокращенное:
АО «Таганрогбанк».

Адрес местонахождения:
Главный офис:
347900, Россия, Ростовская область, г.Таганрог, ул. Греческая, 71.
Контактный телефон: +7 (8634) 310-975.

Дополнительный офис:
344000, Россия, Ростовская область, г. Ростов-на-Дону, пр. Ленина, 107
Контактный телефон: 7+(863) 243-05-41

Электронная почта: admin@tagbank.ru