*Редакция – 002
действует с 09.01.2025
до даты ввода новой редакции*

Приложение № 5

к Общим условиям использования

электронных документов

**Рекомендации по безопасному использованию Системы ДБО[[1]](#footnote-2)**

**I. Рекомендации по обеспечению информационной безопасности при работе в Системе ДБО.**

**1. Размещение персонального компьютера (далее - ПК).**

1.1. Размещение ПК, специальное оборудование, охрана и организация режима помещений, в которых хранятся Персональные аппаратные криптопровайдеры (далее - ключевые носители) и расположен ПК, должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

1.2. Помещения, предназначенные для размещения ПК и хранения, должны быть оборудованы прочными дверями, замками и сигнализацией. Окна помещений, расположенных на первых или последних этажах зданий, а также находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних, должны быть оборудованы решетками или сигнализацией.

**2. Защита ПК.**

2.1. Клиент, эксплуатирующий ПК, должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства на ПК, изменение их состава, появление на ПК и в Системе ДБО компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения Системы ДБО, ЭД, либо на перехват паролей, ключей ЭП и другой конфиденциальной информации, а также программ, которые могут использоваться для удаленного управления ПК.

2.2. Перед началом работы в Системе ДБО обязательно провести сканирование ПК на отсутствие вредоносного программного обеспечения (далее – ПО).

2.3. Выполнять полную проверку ПК альтернативными антивирусными средствами 1 раз в 1 месяц.

2.4. При работе в ДБО не допускается работа под учетной записью с правами администратора.

2.5. Обязательное использование межсетевого экрана (кроме штатного Windows) с настройками, обеспечивающими:

□ на ПК запрещены входящие соединения из сети Интернет;

□ с ПК разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет.

 Интернет для проведения обновлений программного обеспечения.

2.6. Не запускать ДБО до установки актуальных обновлений безопасности для операционной системы (далее -ОС) и ПО.

2.7. Подключать Персональный аппаратный криптопровайдер к ПК только на период работы и подписания документов.

2.8. Раз в день проверять остаток денежных средств на Счете.

**3. Правила хранения персональных аппаратных криптопровайдеров.**

3.1. Для хранения ключевых носителей, а также эксплуатационной и технической документации, носителей информации с дистрибутивами средств криптографической защиты информации необходимо использовать надежные металлические хранилища, оборудованные внутренними замками.

3.2. Хранение ключевых носителей допускается в хранилище с ограниченным доступом, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца ключевых носителей и исключающей возможность негласного доступа к ним посторонних лиц.

3.3. Запрещается:

* копировать ключи ЭП на носители информации, которые не зарегистрированы в качестве ключевых носителей;
* передавать ключевые носители другим лицам;
* выводить ключи ЭП на дисплей или принтер;
* оставлять ключевые носители без присмотра;
* записывать на ключевой носитель постороннюю информацию.

**4. Требования к персоналу, работающему на ПК.**

4.1. Непосредственная работа на ПК возможна только после прохождения обучения и проверки знания ими правил эксплуатации ПК.

4.2. Каждый Пользователь системы ДБО, имеющий доступ к ключам ЭП, паролям и другой конфиденциальной информации, должен быть проинформирован об ответственности за разглашение конфиденциальной информации и подписать соглашение, устанавливающее соответствующие обязательства.

**II. Методические рекомендации о порядке действий Клиента в случае выявления хищения денежных средств в Системе ДБО, с использованием ПК Клиента.**

1. В случае выявления хищения денежных средств в Системе ДБО немедленно прекратить любые действия с ПК, подключенным к Системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и 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 ПК, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2. При наличии технической возможности отозвать подозрительный перевод денежных средств с использованием иного ПК, после чего принять меры к блокировке Системы ДБО.

3. При отсутствии технической возможности отозвать перевод денежных средств по Системе ДБО, незамедлительно обратившись в Банк по по электронной почте mw@rosbank.ru, связавшись с Банком, с заявлением о блокировке Системы ДБО, приостановке исполнения подозрительного платежа и возврате денежных средств по данному платежу, используя Блокировочное слово.

4. Произвести фотосъемку ПК (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ПК 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 ПК, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другой ПК.

5. Дополнительно обратиться в Банк с письменным заявлением об отзыве подозрительного платежа, возврате денежных средств и блокировании доступа к Системе ДБО ([Приложение №1](#Par129) к Рекомендациям), а также о Компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в Банк незамедлительно по электронной почте (скан-копия) Financedealer@rosbank.ru. Оригинал заявления должен быть доставлен в Банк не позднее дня, следующего за днем направления копии Заявления.

6. Проинформировать все банки, с которыми Клиент имеет договорные отношения и чьи системы ДБО установлены на ПК, о факте несанкционированного Клиентом доступе к ПК и обратиться с просьбой о внеплановой замене ключевой информации.

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.

8. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения Системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ПК, используемых для управления денежными средствами через Систему ДБО, которые могут использоваться для удаленного управления указанными ПК.

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

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

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

12. Все действия производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки. При невозможности осуществления коллегиальных действий отдельно зафиксировать данный факт.

13 Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

14. 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, 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.

15. Копии вышеуказанных документов, направить в Банк с приложением Справки по факту инцидента информационной безопасности в Системе ДБО ([Приложение №2](#Par417) к Рекомендациям), а также подтверждающих документов ([Приложение №3](#Par545) к Рекомендациям ).

**III. Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций.**

В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки электронных подписей Клиента под электронным документом.

Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ, на основании которого Банк выполнил операции по Счёту Клиента.

Банк обязан в течение 5 (пяти) рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию (далее – Комиссия) для рассмотрения заявления.

В состав Комиссии включаются:

* представители Клиента;
* представители Банка;
* при необходимости представители компании-разработчика Системы ДБО или независимые эксперты.

Выбор членов Комиссии осуществляется по согласованию со всеми участниками.

Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы ДБО, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны, участвующей в Договоре об использовании электронных документов (далее – Договор).

Стороны обязуются способствовать работе Комиссии и не допускать отказа от предоставления необходимых документов.

Стороны обязуются предоставить Комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в Системе ДБО.

В ходе работы Комиссии каждая Сторона обязана доказать, что она исполнила обязательства по Договору надлежащим образом.

Результатом рассмотрения спорной ситуации Комиссией является определение стороны, несущей ответственность согласно выводу о подлинности электронных подписей Клиента под приложенным документом.

Комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

Разрешительная комиссия проводит техническую экспертизу:

* ключа (ключей) проверки ЭП Клиента с использованием штатного программного обеспечения (ПО) Системы ДБО выполняется распечатка Сертификата ключа проверки ЭП Клиента. Результат сверяется с Сертификатом ключа проверки ЭП, заверенным подписью уполномоченного лица Клиента. Сверяются ID ключа и его шестнадцатеричный дамп. При обнаружении расхождений ситуация далее не рассматривается как не соответствующая заявленной;
	+ электронного документа на наличие необходимого количества (согласно Заявлению о присоединении к Общим условиям использования электронных документов, Заявлению на изменение в настройках пользователей системы ДБО и перечне электронных документов) электронных подписей Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия с его счетом;
* корректности электронных подписей Клиента в электронном документе, с использованием штатного ПО Системы ДБО выбирается документ и выполняется операция «Проверить ЭП».

При невозможности получить доступ к документу с помощью штатного ПО Системы ДБО, может использоваться специализированные утилиты от разработчика для выгрузки документа из базы данных системы и автономной проверки.

На основании данных технической экспертизы Комиссия составляет Акт произвольной формы, содержащий следующие данные:

* + фактические обстоятельства, послужившие основанием возникновения разногласий;
	+ порядок работы членов Комиссии;
	+ вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого электронного документа и его обоснование.

Акт составляется в 2 (двух) экземплярах, подписываемых представителями Банка и Клиента, принимающих участие в работе Комиссии, или в 3 (трех) экземплярах, если в состав Комиссии включаются представители компании разработчика ДБО или независимые эксперты, подписываемых представителями Банка, Клиента и представителем компании разработчика ДБО или независимого эксперты принимающих участие в работе Комиссии. Один из экземпляров акта вручается уполномоченному представителю Клиента или направляется в адрес Клиента почтой в срок не позднее 30 (тридцати)календарных дней с даты поступления в Банк претензии Клиента; указанный срок может быть продлен до 60 (шестидесяти) календарных дней в случае, если предметом рассмотрения Комиссии является претензия о ненадлежащем осуществлении трансграничного перевода, т.е. перевода денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.

Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одна из следующих ситуаций:

* + Банк не предъявляет электронный документ, переданный Клиентом, на основании которого Банк выполнил операции по Счёту Клиента;
	+ хотя бы одна ЭП Клиента в исполненном электронном документе оказалась некорректной;
	+ Клиент предоставляет заявление об отмене действия ключа ЭП и соответствующего ему ключа проверки ЭП Клиента (см. Приложение №7 к Общим условиям), подписанное должностными лицами Банка и имеющим оттиск печати Банка. При этом Администратором СКЗИ проставлены в уведомлении Клиента дата и время блокировки в Системе ДБО Пары ключей ЭП Клиента раньше даты и времени, указанных в рассматриваемом электронном документе.

В случае, когда Банк предъявляет электронный документ, в котором корректность электронных подписей Клиента признана Комиссией и принадлежность Клиенту ключей проверки ЭП Клиента подтверждена, Банк перед Клиентом по выполненным операциям со Счётом Клиента ответственности не несёт. Отказ Клиента от подписания акта, при наличии перечисленных в настоящем пункте Положения обстоятельств, не является основанием для признания обоснованности претензии Клиента и не влечет ответственности Банка.

Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими ЭП, Комиссия может вынести определение о Компрометации ключа (ключей) ЭП Клиента, что не снимает ответственности с Клиента за данный документ.

Приложение №1 к Рекомендациям

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность руководителя

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование Банка

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

Уважаемый(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 имя, отчество руководителя Банка

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_ года со счета №…., принадлежащего \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(наименование клиента), открытого в Росбанк филиал АВТО АО «ТБанк», по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации, были переведены по следующим реквизитам:

Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер документа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_

Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

БИК Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Корреспондентский счет Банка получателя\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 должность подпись расшифровка подписи

М.П. (при наличии)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

Исп. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Фамилия И.О.

Приложение №2 к Рекомендациям

**СПРАВКА КЛИЕНТА**

**В БАНК ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО**

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. неустановленным лицом через Систему ДБО была совершена несанкционированная операция по переводу денежных средств со счета № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, принадлежащего \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(наименование Клиента) по следующим реквизитам:

Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер распоряжения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

БИК Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Корреспондентский счет Банка получателя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнительно сообщаю:

Количество ПК, настроенных для доступа в Систему ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Для доступа в Систему ДБО хотя бы раз использовались:

* корпоративные ПК
* личные ПК
* ПК, находящиеся в общественном пользовании

Периодичность смены пароля Системы ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Применяемые элементы безопасности ПК включают:

* соблюден порядок подготовки ПК 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
* используется антивирусное программное обеспечение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* антивирусное программное обеспечение обновляется ежедневно
* из числа съемных носителей информации на ПК используются только ключевые носители
* передача файлов и обмен сообщениями электронной почты на ПК ограничены
* целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* используются средства сетевой защиты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* на ПК запрещены входящие соединения из сети Интернет
* с ПК разрешены исходящие соединения с Банком и ограниченным числом сайтов сети

 Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* обеспечивается возможность доступа к ПК только уполномоченных лиц
* обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 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 нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 Уголовного Кодекса Российской Федерации предупрежден.

ФИО/Должность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/ Дата: \_\_\_\_\_\_\_\_\_\_/ Номер телефона:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Печать Клиента М.П. (при наличии)

Приложение №3 к Рекомендациям

**ПЕРЕЧЕНЬ**

**ДОКУМЕНТОВ, ПРЕДОСТАВЛЯЕМЫХ КЛИЕНТОМ В БАНК,**

**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 межсетевого 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).

1. Если иное прямо не указано в настоящем Приложении № 5 к Общим условиям использования электронных документов, то все термины, используемые по тексту настоящего документа, имеют значения, указанные в Общих условиях использования электронных документов. [↑](#footnote-ref-2)