ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 25 мая 2011 г. N 76-Т

ОБ УСЛОВИЯХ
СОГЛАШЕНИЙ, ОПРЕДЕЛЯЮЩИХ ПРАВА И ОБЯЗАННОСТИ БАНКА (ФИЛИАЛА БАНКА) И БАНКА РОССИИ ПРИ НАПРАВЛЕНИИ В БАНК (ФИЛИАЛ БАНКА) ПОРУЧЕНИЙ НАЛОГОВЫХ ОРГАНОВ, РЕШЕНИЙ НАЛОГОВЫХ ОРГАНОВ, А ТАКЖЕ ПРИ НАПРАВЛЕНИИ БАНКОМ (ФИЛИАЛОМ БАНКА) В НАЛОГОВЫЙ ОРГАН СВЕДЕНИЙ ОБ ОСТАТКАХ ДЕНЕЖНЫХ СРЕДСТВ В ЭЛЕКТРОННОМ ВИДЕ ЧЕРЕЗ БАНК РОССИИ

В связи с принятием Положения Банка России от 29.12.2010 N 365-П "О порядке направления в банк поручения налогового органа, решения налогового органа, а также направления банком в налоговый орган сведений об остатках денежных средств в электронном виде" ("Вестник Банка России" от 9 февраля 2011 года N 8) (далее - Положение Банка России N 365-П) в соглашение, заключаемое между банком (в том числе в лице филиала банка) и Банком России (в лице территориального учреждения Банка России) (далее - ТУ Банка России), определяющее особенности (условия) взаимодействия банка (филиала банка) и ТУ Банка России при получении поручений налогового органа на списание и перечисление денежных средств со счетов налогоплательщика (плательщика сборов, налогового агента) - организации, индивидуального предпринимателя в бюджетную систему Российской Федерации (далее - поручение налогового органа), решений налогового органа о приостановлении операций по счетам налогоплательщика-организации в банке или решения об отмене приостановления операций по счетам налогоплательщика-организации в банке (далее - решение налогового органа) в электронном виде через Банк России, а также при приеме в электронном виде от банка (филиала банка) сведений об остатках денежных средств на счетах налогоплательщика-организации в банке, операции по которым приостановлены (далее - сведения об остатках), в электронном виде через Банк России (далее - соглашение), ТУ Банка России рекомендуется включить следующие условия.

1. В качестве предмета соглашения указывается следующее.

Банк России (в лице ТУ Банка России) обязуется предоставлять банку (филиалу банка) возможность получать сообщения, направленные ФНС России в банк (филиал банка) через Банк России, а также направлять в ФНС России сообщения, полученные Банком России (в лице ТУ Банка России) от банка (филиала банка) для отправки в ФНС России (указать не менее одного условия из следующих условий):

предоставлять банку (филиалу банка) возможность получать в электронном виде сообщения, содержащие поручения налогового органа, направленные ФНС России в банк (филиал банка) через Банк России;

предоставлять банку (филиалу банка) возможность получать в электронном виде сообщения, содержащие решения налогового органа, направленные ФНС России в банк (филиал банка) через Банк России;

принимать в электронном виде от банка (филиала банка) сообщения, содержащие сведения об остатках, направленные банком (филиалом банка) в ТУ Банка России.

Банк России (в лице ТУ Банка России) обязуется обмениваться с банком (филиалом банка) иными сообщениями, формируемыми при получении поручения и (или) решения налогового органа и (или) передаче налоговому органу сведений об остатках в соответствии с требованиями, установленными Положением Банка России N 365-П.

2. В качестве условий осуществления обмена сообщениями в соглашении между банком (филиалом банка) и Банком России указывается следующее.

2.1. При обмене сообщениями применяются следующие средства криптографической защиты информации _____ (указать, какие используются средства аутентификации

и средства шифрования).

Порядок применения средств криптографической защиты информации при обмене сообщениями определяется в приложении 1 к соглашению между банком (филиалом банка) и Банком России, которое излагается в редакции приложения 1 к настоящему письму.

Порядок обеспечения информационной безопасности при использовании средств криптографической защиты информации определяется в приложении 2 к соглашению между банком (филиалом банка) и Банком России, которое излагается в редакции приложения 2 к настоящему письму.

2.2. Перечень, форматы сообщений и порядок осуществления контроля сообщений, используемых при получении в электронном виде поручения и (или) решения налогового органа в банке (филиале) и при передаче в налоговый орган сведений об остатках, поступивших из банка (филиала банка) в электронном виде, устанавливаются Банком России и размещаются в сети Интернет (www.cbr.ru).

3. В качестве необходимых условий для осуществления обмена сообщениями в соглашении между банком (филиалом банка) и Банком России указывается, что ТУ Банка России выполняет следующее:

по заявлению банка (филиала банка), представленному в письменном виде в произвольной форме, регистрирует банк (филиал банка) в качестве участника обмена сообщениями, о чем уведомляет банк (филиал банка) в письменном виде в срок не позднее 15 рабочих дней со дня поступления заявления;

регистрирует ключи кода аутентификации (далее - КА) банка (филиала банка);

передает банку (филиалу банка) ключ шифрования;

передает банку (филиалу банка) открытый ключ КА и шифрования Межрегиональной инспекции Федеральной налоговой службы по централизованной обработке данных (далее - МИ ФНС России по ЦОД);

осуществляет с банком (филиалом банка) обмен электронными сообщениями в тестовом режиме и после его успешного завершения письменно сообщает банку (филиалу банка) о дате начала обмена сообщениями.

4. В качестве прав и обязанностей Банка России (в лице ТУ Банка России) указывается следующее.

4.1. При осуществлении обмена сообщениями Банк России (в лице ТУ Банка России) имеет право в одностороннем порядке устанавливать и изменять перечень, форматы (в том числе структуру) сообщений, используемых при получении в электронном виде поручения и (или) решения налогового органа в банке (филиале) и при передаче в налоговый орган сведений об остатках, поступивших от банка (филиала банка) в электронном виде, а также порядок осуществления контроля данных сообщений.

Банк России (в лице ТУ Банка России) имеет право обращаться в банк (филиал банка) с запросами по вопросам, связанным с обменом сообщениями.

Банк России (в лице ТУ Банка России) не несет ответственности за невозможность осуществления обмена сообщениями, вызванную неисправностями используемых банком (филиалом банка) программно-аппаратных средств и каналов связи.

4.2. При осуществлении обмена сообщениями Банк России (в лице ТУ Банка России) обязан:

осуществлять обмен сообщениями в порядке, предусмотренном Положением Банка России N 365-П и настоящим соглашением;

соблюдать график обмена сообщениями в условиях штатного функционирования систем, обеспечивающих обмен сообщениями;

информировать банк (филиал банка) обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену сообщениями, незамедлительно после их возникновения путем _____ (привести сведения о способе информирования);

обеспечивать хранение полученных от банка (филиала банка) сообщений, содержащих подтверждения, уведомления, а также направленных банку (филиалу банка) сообщений, содержащих извещения, не менее 5 лет со дня их получения (направления);

обеспечивать хранение полученных от банка (филиала банка) сообщений, содержащих

сведения об остатках, по которым ТУ Банка России были получены от МИ ФНС России по ЦОД извещения об отрицательных результатах проверки, до выяснения причины отрицательного результата данной проверки;

обеспечивать хранение направленных банку (филиалу банка) сообщений, содержащих поручения налогового органа, решения налогового органа, извещения, по которым от банка (филиала банка) получены подтверждения с отрицательными результатами проверки, до выяснения причины отрицательного результата данной проверки;

уведомлять банк (филиал банка) об изменении перечней, форматов и порядка, указанных в подпункте 4.1 пункта 4 настоящего письма, установленных Банком России и размещенных в сети Интернет в соответствии с пунктом 2.2 настоящего письма, путем _____ (указать способ уведомления - в письменном виде в произвольной форме, в электронном виде по каналам связи, с использованием средств факсимильной связи) не позднее 30 рабочих дней до дня вступления изменений в силу.

5. В качестве прав и обязанностей банка (филиала банка) в соглашении указывается следующее.

5.1. При осуществлении обмена сообщениями банк (филиал банка) имеет следующие права:

осуществлять обмен сообщениями в порядке, предусмотренном Положением Банка России N 365-П и настоящим соглашением;

обращаться в ТУ Банка России с запросами по вопросам, связанным с обменом сообщениями.

5.2. При осуществлении обмена сообщениями банк (филиал банка) обязан:

соблюдать требования, предусмотренные Положением Банка России N 365-П, а также руководствоваться устанавливаемыми Банком России при осуществлении обмена сообщениями перечнями, форматами и порядком;

соблюдать график обмена сообщениями, в том числе осуществлять получение сообщений, содержащих поручения и решения налоговых органов, от ТУ Банка России не реже одного раза в каждый из следующих периодов по местному времени: с 9 часов 00 минут 00 секунд до 13 часов 00 минут 00 секунд, с 13 часов 00 минут 01 секунды до 16 часов 00 минут 00 секунд;

хранить программные средства, предназначенные для создания и проверки КА, а также документацию на эти средства в течение сроков хранения сообщений, но не менее 5 лет после прекращения их использования;

информировать ТУ Банка России обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену сообщениями, незамедлительно после их возникновения путем _____ (привести сведения о способе информирования), по запросам ТУ Банка России письменно подтверждать наличие этих событий с указанием обстоятельств, при которых они возникли;

обеспечивать хранение не менее 5 лет со дня передачи или получения поручений налоговых органов, решений налоговых органов, сведений об остатках, а также сообщений, содержащих извещения, подтверждения, уведомления;

обеспечивать хранение направленных в ТУ Банка России сообщений, содержащих сведения об остатках, по которым от ТУ Банка России получены извещения с отрицательными результатами проверки, до выяснения причины отрицательного результата данной проверки.

6. В качестве условий прекращения действия соглашения указывается следующее.

6.1. Действие соглашения между банком и Банком России прекращается:

по инициативе банка (в том числе в лице филиала банка);

по инициативе Банка России (в лице ТУ Банка России), в том числе в случае нарушения банком (филиалом банка) требований к обеспечению информационной безопасности при обмене сообщениями.

6.2. Для прекращения действия соглашения сторона-инициатор уведомляет другую сторону о дате прекращения действия соглашения путем направления другой стороне соответствующего уведомления не позднее 10 рабочих дней до даты прекращения действия соглашения.

7. В качестве прочих условий в соглашении между банком и Банком России указывается следующее.

7.1. Права и обязанности сторон по соглашению не могут быть уступлены или переданы

третьим лицам.

7.2. По вопросам, не урегулированным соглашением, стороны руководствуются законодательством Российской Федерации.

8. Соглашение между банком (в том числе в лице его филиала) и Банком России (в лице ТУ Банка России) рекомендуется заключать в качестве отдельного (самостоятельного) документа, либо в качестве дополнительных соглашений к договорам, заключаемым между банком (в том числе в лице его филиала) и Банком России (в лице ТУ Банка России) для передачи сообщений по каналам связи, используемым в Банке России для приема-передачи отчетности.

9. В случае если с банком (в том числе в лице его филиала) ранее было заключено соглашение в соответствии с письмом Банка России от 20.11.2008 N 146-Т "Об условиях соглашений, определяющих права и обязанности банков и Банка России при получении решений налоговых органов о приостановлении (об отмене приостановления) операций по счетам налогоплательщика-организации в банке в электронном виде через Банк России", то внесение в него изменений проводится путем внесения дополнений, связанных с получением банком (филиалом банка) поручений налогового органа, с направлением в налоговый орган сведений об остатках, с изменением порядка получения банком (филиалом банка) решений налогового органа, либо путем изложения соглашения в новой редакции. Внесение в соответствии с настоящим письмом изменений в ранее заключенное соглашение, не требует расторжения действующего соглашения и заключения нового соглашения.

10. Доведите содержание настоящего письма до сведения банков (филиалов банков).

Заместитель Председателя
Банка России
Т.Н.ЧУГУНОВА

Приложение 1
к письму Банка России
от 25 мая 2011 года N 76-Т
"Об условиях соглашений, определяющих
права и обязанности банка (филиала
банка) и Банка России при направлении
в банк (филиал банка) поручений
налоговых органов, решений налоговых
органов, а также при направлении
банком (филиалом банка) в налоговый
орган сведений об остатках денежных
средств в электронном виде
через Банк России"

ПОРЯДОК
ПРИМЕНЕНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ОБМЕНЕ СООБЩЕНИЯМИ

1. В настоящем Порядке используются следующие термины.

1.1. Подтверждение подлинности и контроль целостности сообщения - проверка сообщения, направленного в электронном виде, позволяющая получателю установить, что сообщение исходит из указанного источника и не было изменено при его передаче от источника до получателя.

1.2. Ключ КА - уникальные данные, используемые при создании и проверке КА и состоящие из:

секретной части ключа КА (далее - секретный ключ КА), предназначенной для создания КА

сообщения;

публичной части ключа (далее - открытый ключ КА), предназначенной для аутентификации сообщения получателем.

1.3. Ключ шифрования - уникальные данные, используемые при зашифровании и расшифровании сообщения.

1.4. Владелец ключа КА или ключа шифрования - МИ ФНС России по ЦОД, банк (филиал банка), Уполномоченное подразделение Банка России или ТУ Банка России, ключ КА или ключ шифрования которого зарегистрирован в регистрационном центре, функционирующем в Банке России.

1.5. Средства криптографической защиты информации (далее - СКЗИ) - аппаратные и (или) программные средства, обеспечивающие создание и проверку КА, а также реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при ее передаче по каналам связи.

1.6. Компрометация ключа КА или ключа шифрования - событие, определенное владельцем ключа КА или ключа шифрования как ознакомление неуполномоченным лицом (лицами) с его секретным ключом КА или секретным ключом шифрования.

1.7. Пользователь ключа КА или ключа шифрования - лицо, назначенное владельцем ключа КА или ключа шифрования и уполномоченное им использовать ключ КА или ключ шифрования от имени владельца ключа КА или ключа шифрования.

1.8. Регистрационный центр - структурное подразделение Банка России, выполняющее функции регистрации ключей КА и (или) ключей шифрования и управления ключами КА и (или) ключами шифрования МИ ФНС России по ЦОД, банков (филиалов банков), Уполномоченного подразделения Банка России и ТУ Банка России.

1.9. Регистрационная карточка ключа КА - документ, содержащий распечатку открытого ключа КА в шестнадцатеричной системе счисления, наименование владельца ключа КА и иные идентифицирующие владельца ключа КА сведения, подписанный руководителем (или замещающим его лицом) МИ ФНС России по ЦОД, банка (филиала банка), Уполномоченного подразделения Банка России или ТУ Банка России и содержащий оттиск печати владельца ключа (далее - регистрационная карточка).

2. Обмен сообщениями между МИ ФНС России по ЦОД и банками (филиалами банков) осуществляется с применением СКЗИ, принятых к использованию в Банке России. СКЗИ используются для формирования кодов аутентификации и шифрования сообщений.

3. МИ ФНС России по ЦОД, банки (филиалы банков), Банк России могут иметь резервные ключи КА и шифрования.

4. МИ ФНС России по ЦОД, банки (филиалы банков), Банк России изготавливают ключи КА самостоятельно. Ключи КА подлежат регистрации в регистрационном центре. Для этого изготавливается регистрационная карточка в двух экземплярах в соответствии с порядком, определяемым регистрационным центром. Регистрационная карточка содержит:

наименование владельца ключа КА;

наименование применяемого СКЗИ;

информацию, идентифицирующую ключ КА (идентификатор и (или) номер ключа КА, идентификатор и (или) номер серии);

информацию о назначении ключа КА (область применения);

распечатку открытого ключа КА в шестнадцатеричной системе счисления;

дату изготовления ключа КА;

даты начала и окончания действия ключа КА;

подпись руководителя (или замещающего его лица) владельца ключа КА с оттиском печати владельца ключа КА;

подпись администратора регистрационного центра;

иные реквизиты.

Форма регистрационной карточки разрабатывается регистрационным центром в зависимости от функциональных возможностей конкретного СКЗИ. Регистрационная карточка может распечатываться на одном листе или нескольких страницах. При распечатке регистрационной карточки на нескольких страницах каждая страница должна в обязательном

порядке содержать подпись руководителя (или замещающего его лица) владельца ключа КА, заверенную оттиском печати владельца ключа КА.

Один экземпляр оформленной регистрационной карточки хранится в регистрационном центре, другой - у владельца ключа КА. Ключ КА считается зарегистрированным со дня передачи владельцу ключа КА его экземпляра оформленной регистрационной карточки.

5. Ключи шифрования, используемые МИ ФНС России по ЦОД, банком (филиалом банка), ТУ Банка России для обеспечения защиты информации при передаче сообщений по каналам связи, либо предоставляются регистрационным центром с оформлением акта их приема-передачи по форме, определяемой регистрационным центром, либо изготавливаются самостоятельно и регистрируются регистрационным центром (процедура аналогична процедуре регистрации ключей КА, описанной в пункте 4 настоящего Порядка).

6. МИ ФНС России по ЦОД, банки (филиалы банков), Уполномоченное подразделение Банка России и ТУ Банка России обеспечивают сохранность своих секретных ключей КА и ключей шифрования.

7. Порядок обращения с секретными ключами КА и секретными ключами шифрования, обеспечивающий их конфиденциальность, и допуск к ним конкретных пользователей устанавливаются внутренними документами владельца ключа КА или ключа шифрования и Порядком обеспечения информационной безопасности при использовании средств криптографической защиты информации в соответствии с приложением 2 к настоящему соглашению.

8. Управление ключами КА и ключами шифрования осуществляется и регламентируется регистрационным центром в порядке, предусмотренном Банком России.

9. Плановый срок действия ключей КА и ключей шифрования определяется регистрационным центром.

10. Плановая смена ключей КА и ключей шифрования организуется регистрационным центром при соответствующем уведомлении всех владельцев ключей КА или ключей шифрования.

11. Внеплановая смена ключей КА и (или) ключей шифрования может производиться как по инициативе регистрационного центра, так и владельца ключа КА или ключа шифрования в случае компрометации или утраты секретного ключа КА и (или) ключа шифрования.

12. Смена ключей КА или ключей шифрования выполняется в соответствии с требованиями пунктов 4 и 5 настоящего приложения.

13. После ввода в действие новых ключей КА или ключей шифрования прежде действовавшие секретные ключи КА или ключи шифрования уничтожаются в определенные регистрационным центром сроки, а открытые ключи КА хранятся МИ ФНС России по ЦОД, банками (филиалами банков), Банком России в течение всего срока хранения сообщений, для подтверждения подлинности и контроля целостности которых они могут быть использованы.

14. Уничтожение открытых ключей КА после истечения срока их хранения осуществляется МИ ФНС России по ЦОД, банками (филиалами банков), Банком России самостоятельно.

15. Программные средства, предназначенные для создания и проверки КА, а также документация на эти средства хранятся МИ ФНС России по ЦОД, банками (филиалами банков), Банком России в течение всего срока хранения сообщения, для подписания и подтверждения подлинности и контроля целостности которых использовались (могут использоваться) указанные средства.

16. Сведения о ключах КА и ключах шифрования не подлежат передаче третьим лицам, за исключением случаев, установленных законодательством Российской Федерации.

Приложение 2
к письму Банка России
от 25 мая 2011 года N 76-Т

"Об условиях соглашений, определяющих
права и обязанности банка (филиала
банка) и Банка России при направлении
в банк (филиал банка) поручений
налоговых органов, решений налоговых
органов, а также при направлении
банком (филиалом банка) в налоговый
орган сведений об остатках денежных
средств в электронном виде
через Банк России"

ПОРЯДОК
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1. Установка и настройка СКЗИ на автоматизированных рабочих местах (далее - АРМ) пользователей выполняются с учетом требований, изложенных в эксплуатационной документации на СКЗИ, в присутствии Администратора информационной безопасности, назначаемого владельцем ключа КА или ключа шифрования. При каждом запуске АРМ должен быть обеспечен контроль целостности установленного программного обеспечения СКЗИ.

2. МИ ФНС России по ЦОД, банками (филиалами банков) и Банком России определяется и утверждается порядок учета, хранения и использования носителей ключевой информации (ключевых дискет, ключевых идентификаторов Touch Memory, ключевых Smart-карточек и других носителей ключевой информации) с секретными ключами КА и ключами шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.

3. Ответственность за содержание данных, включаемых в сообщение, несет владелец ключа КА, которым снабжено сообщение.

4. Руководство владельца ключа КА или ключа шифрования утверждает список лиц, имеющих доступ к секретным ключам КА и ключам шифрования (с указанием конкретной информации для каждого лица). Доступ лиц, не допущенных к носителям ключевой информации, должен быть исключен.

5. Для хранения носителей ключевой информации с секретными ключами КА и ключами шифрования должны использоваться надежные металлические шкафы (сейфы). Хранение носителей ключевой информации с секретными ключами КА и ключами шифрования допускается в одном металлическом шкафу (сейфе) с другими документами в отдельном контейнере, опечатываемом пользователем ключа КА и (или) ключа шифрования.

6. В течение рабочего дня вне времени составления и передачи и приема сообщения, а также по окончании рабочего дня носители ключевой информации с секретными ключами КА и (или) ключами шифрования помещаются в металлические шкафы (сейфы).

7. Не допускается:

снимать несанкционированные копии с носителей ключевой информации;

знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным;

выводить секретные ключи КА или ключи шифрования на дисплей (монитор) электронно-вычислительной машины (ЭВМ) или принтер;

устанавливать носитель секретных ключей КА или ключей шифрования в считывающее устройство АРМ, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие ЭВМ;

записывать на носители ключевой информации постороннюю информацию.

8. При компрометации секретного ключа КА или ключа шифрования владелец ключа КА или ключа шифрования, допустивший компрометацию, обязан предпринять все меры для прекращения любых операций с использованием этого ключа и немедленно проинформировать о факте компрометации регистрационный центр, который организует внеплановую смену ключей КА или ключей шифрования.

9. По факту компрометации ключа КА или ключа шифрования владелец ключа КА или ключа шифрования, допустивший компрометацию, должен организовать служебное расследование, документально оформленные результаты которого представляются в регистрационный центр.

10. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей работника МИ ФНС России по ЦОД, банка (филиала банка), Уполномоченного подразделения Банка России и ТУ Банка России, имевшего доступ к секретным ключам КА или ключам шифрования, должна быть проведена замена ключей, к которым указанный работник имел доступ.