

УТВЕРЖДАЮ  
Генеральный директор ООО «ИНЕТ»

\_\_\_\_\_ Докучаев Ю.А.  
« 01 » июня 2013 года

**РЕГЛАМЕНТ**  
работы в Системе юридически значимого электронного документооборота  
DataCrypt

**г. Кемерово 2013 год.**

## 1. Основные понятия, используемые в настоящем Регламенте.

- 1) **владелец сертификата ключа ЭЦП** – уполномоченное лицо налогоплательщика/страхователя, на имя которого выдан сертификат ключа ЭЦП и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- 2) **средства ЭЦП** - аппаратные и программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.
- 3) **закрытый ключ ЭЦП** - уникальная последовательность символов, известная владельцу сертификата ключа электронной подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- 4) **открытый ключ ЭЦП** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю Системы и предназначенная для подтверждения использования средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.
- 5) **сертификат ключа подписи (далее СКП)** - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются удостоверяющим центром участнику информационной системы.
- 6) **подтверждение подлинности ЭЦП в электронном документе** - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа электронной подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.
- 7) **компрометация ключа** – констатация лицом, владеющим закрытым (секретным) ключом ЭЦП, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами.
- 8) **система электронного документооборота (далее СЭД)** – организационно-техническая система, представляющая собой совокупность программного, информационного и аппаратного обеспечения организатора и ее участников, реализующая электронный документооборот; СЭД является корпоративной информационной системой.
- 9) **оператор** - участник СЭД, осуществляющий управление работой СЭД в целом, приём запросов на изготовление СКП от участников СЭД, передачу отчетности участников СЭД в контролирующие органы.
- 10) **система юридически значимого электронного документооборота DataCrypt (далее система)**- юридически значимая СЭД с ограниченным кругом участников, в которой условия работы участников определяются Договором на подключение и абонентское обслуживание с Оператором и данным регламентом.
- 11) **удостоверяющий центр (далее УЦ)** - организация, осуществляющая следующие виды деятельности:
  - регистрация пользователей в реестре удостоверяющего центра и изготовление СКП;
  - создание закрытых ключей ЭЦП по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа ЭЦП;
  - приостановление и возобновление действия СКП, а также их аннулирование;
  - ведение реестра СКП, обеспечивая его актуальность и возможность свободного доступа к нему участников информационных систем;
  - проверка уникальности открытых ключей ЭЦП в реестре и архиве удостоверяющего центра;
  - выдача СКП в форме документов на бумажных носителях и/или в форме электронных документов с информацией о сроках их действия;
  - осуществление подтверждения подлинности ЭЦП в электронном документе по обращениям пользователей удостоверяющего центра.

## 2. Общие положения

- 2.1. Целью настоящего Регламента является определение порядка эксплуатации Системы всеми ее участниками.
- 2.2. В Системе используется только сертифицированные средства ЭЦП.
- 2.3. Система представления отчетов в электронном виде с использованием электронно-цифровой подписи по данному Регламенту является - корпоративной.
- 2.4. Любое заинтересованное лицо может ознакомиться с Регламентом в офисе Оператора по адресу: г. Кемерово, ул. Д.-Бедного, д. 6, оф. 65, а также на сайте Оператора <http://www.kemnet.ru/>.
- 2.5. Присоединение к Регламенту осуществляется путем подписания договора на подключение и абонентское обслуживание в системе юридически значимого электронного документооборота DataCrypt.
- 2.6. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.
- 2.7. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Оператором путем обязательного размещения указанных изменений (дополнений) на сайте - <http://www.kemnet.ru/>.
- 2.8. Все изменения (дополнения), вносимые Оператором в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 14 календарных дней с даты размещения указанных изменений и дополнений на сайте [www.kemnet.ru](http://www.kemnet.ru/)
- 2.9. Все изменения (дополнения), вносимые Оператором в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

### **3. Деятельность Оператора**

ООО «ИНЕТ» действует как Оператор в Системе.

ООО «ИНЕТ» осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

Лицензия УФСБ России по Кемеровской области ЛЗ № 0006123 1040У от 05 ноября 2009г. на осуществление работ по предоставлению услуг в области шифрования информации.

Лицензия УФСБ России по Кемеровской области ЛЗ № 0006122 1039Р от 05 ноября 2009г. на осуществление работ по распространению шифровальных (криптографических) средств.

Лицензия УФСБ России по Кемеровской области ЛЗ № 0006121 1038Х от 05 ноября 2009г. на осуществление работ по техническому обслуживанию шифровальных (криптографических) средств.

Оператор:

- оказывает услуги налогоплательщикам/страхователям по передаче отчетности в контролирующие органы;
- принимает запрос на сертификат ключа ЭЦП налогоплательщика/страхователя и передает его в УЦ;
- обеспечивает актуальность справочника сертификатов ЭЦП участников Системы;
- может предоставлять участникам информационной системы иные, связанные с использованием электронных цифровых подписей услуги;
- осуществляет функции и деятельность удостоверяющего центра в Системе.

### **4. Порядок изготовления сертификатов ключей подписей**

4.1. Изготовление сертификатов ключей подписей осуществляется на основании заявления участника Системы, которое содержит сведения, необходимые для идентификации владельца сертификата ключа подписи.

Содержащиеся в заявлении сведения подтверждаются предъявлением Оператору следующих документов:

4.1.1. Оригинал либо заверенная копия свидетельства о внесении в ЕГРЮЛ (1 стр).

4.1.2. Заверенная копия Приказа о назначении на должность.

4.1.3. Паспорт либо заверенная копия паспорта ответственного лица.

4.2. Предоставление документов на изготовление сертификатов ключей подписей осуществляется не позднее чем за 5 рабочих дней до наступления обстоятельств его выпуска или замены согласно регламента УЦ.

4.3. Сертификаты передаются владельцу в форме бумажного носителя, составленного в двух экземплярах, которые заверяются собственноручными подписями владельца сертификата ключа подписи или его доверенного лица и уполномоченного лица УЦ с печатью УЦ.

4.4. Выпуск, плановая и внеплановая замена сертификатов ключей подписей проводится в соответствии с требованиями нормативных документов и документации на средства криптографической защиты информации и Регламента УЦ.

### **5. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи и печати участников Системы.**

5.1. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи приведены в Федеральном законе РФ от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи», Федеральном законе РФ от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

## **6. Сертификат ключа подписи**

6.1. Сертификат ключа подписи участника Системы содержит следующие сведения:

- серийный номер сертификата (уникальный в рамках выдавшего его УЦ)
- дата начала и дата окончания срока действия СКП, находящегося в реестре УЦ;
- фамилия, имя, отчество, должность владельца СКП;
- страна, область/район, город (населенный пункт) нахождения/регистрации/осуществления деятельности, электронная почта;
- для организации: сокращенное название организации
- для налогоплательщиков: ИНН;
- для страхователей ФСС: код подразделения ФСС, реестровый номер страхователя ФСС;
- наименование и реквизиты УЦ, выдавшего сертификат ключа ЭЦП;
- открытый ключ ЭЦП;
- сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

В случае использования сертификата ключа усиленной квалифицированной подписи сертификат также содержит:

- наименование средств электронной подписи, используемых участником Системы и УЦ, выдавшим СКП;
- ОГРН или ОГРНИП участника Системы;
- СНИЛС владельца СКП;
- наименование и место нахождения аккредитованного УЦ, который выдал квалифицированный сертификат;
- ограничения использования квалифицированного сертификата (если такие ограничения установлены).

6.2. Сертификат ключа подписи должен быть внесен Оператором в справочник сертификатов ключей подписей Системы не позднее даты выдачи сертификата участнику Системы в форме на бумажном носителе.

6.3. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке УЦ и заверяется собственноручной подписью уполномоченного лица УЦ и печатью УЦ, а также собственноручной подписью владельца сертификата или его доверенного лица.

6.4. Сроки и порядок хранения сертификата ключа подписи определяются согласно Регламента УЦ.

6.5. Оператор принимает на себя обязательства по передаче запроса на сертификат ключа подписи в УЦ.

6.6. Приостановление действия сертификата ключа подписи, а так же аннулирование сертификата ключа подписи производится на основании предоставленного Оператору заявления со стороны участника Системы и согласно Регламента УЦ.

6.7. В случае компрометации криптографических ключей владелец скомпрометированных ключей обязан незамедлительно уведомить Оператора о компрометации. В случае получения уведомления о компрометации криптографических ключей, датой и временем компрометации считаются дата и время, указанные в уведомлении о компрометации. Оператор принимает на себя обязательства по передаче данного уведомления в УЦ.

## **7. Обязательства владельца сертификата ключа подписи**

7.1. Владелец сертификата ключа подписи обязан:

- не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются другим лицом или использовались ранее;
- хранить в тайне закрытый ключ электронной цифровой подписи;
- немедленно требовать приостановления действия сертификата ключа подписи и информировать об этом участников системы при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.
- своевременно сообщать Оператору об изменении информации об участнике Системы, включая, но не ограничиваясь информацией о реквизитах, местонахождении, ответственном лице участника Системы, а также любых реквизитов, указанных в сертификатах ключей подписи. Информация об изменениях должна быть предоставлена не позднее 5 (пяти) календарных дней с момента таких вступления в силу таких изменений.

7.2. При несоблюдении требований, изложенных в п.7.1., возмещение причиненных вследствие этого убытков возлагается на участника Системы.

## **8. Электронный документооборот в системе**

8.1. Обмен между участниками Системы осуществляется по правилам и формату определенному Оператором и законом об ЭЦП.

8.2 Представление отчетов в электронном виде с использованием ЭЦП через Систему осуществляется участниками, являющимися налогоплательщиками/страхователями, в контролирующие органы в соответствии со стандартами и форматами, определяемыми контролирующими органами.

8.2. Описание стандартов и форматов отчетности в электронном виде, опубликованы на сайтах ФНС России, ПФР, РосСтат, ФСС и других органов государственной власти, являющихся получателями отчетности.

8.3. В случае невозможности отправки отчетов в электронном виде участники Системы принимают все меры для своевременной сдачи отчетности иным путем.

8.4. До начала пользования услугой по организации обмена электронными документами в ЭДО ПФР по ТКС, заключить соглашение об обмене электронными документами в системе ЭДО ПФР по ТКС с отделением ПФР по месту регистрации.

8.5. Участники Системы безусловно обязуются выполнять требования определяемые «Регламентом работы в Системе юридически значимого документооборота DataCrypt».

## **9. Порядок представления отчетности в электронном виде по телекоммуникационным каналам связи**

9.1. Порядок предоставления отчетности с помощью Системы DataCrypt разработан в соответствии с действующим законодательством:

- Приказами МНС России №НБГ-3-32/169, БГ-3-32/705, Приказом ФНС России № ММВ-7-6/535@ от 09.11.2010, приказом ФНС России № ММ-7-6/353@ от 2 июля 2009 г.,

- Регламентом обмена документами индивидуального (персонифицированного) учета страховых взносов по телекоммуникационным каналам связи в системе электронного документооборота Пенсионного фонда Российской Федерации с внешними организациями» утвержденным распоряжением Правления ПФР от 11.10.2007г. №190,

- Приказом Фонда социального страхования РФ от 12 февраля 2010 г. N 19"О внедрении защищенного обмена документами в электронном виде с применением электронной цифровой подписи для целей обязательно социального страхования",

- ФЗ РФ от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи",

- ФЗ РФ от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

9.2. Настоящий "Порядок представления отчетности в электронном виде по телекоммуникационным каналам связи" (далее - Порядок) определяет общие принципы организации информационного обмена при представлении участниками Системы, которые являются налогоплательщиками/страхователями, отчетов в электронном виде по телекоммуникационным каналам связи (далее - представление отчетов в электронном виде).

9.3. Участниками информационного обмена при представлении отчетов в электронном виде являются: налогоплательщики/страхователи или их представители, являющиеся участниками Системы; контролирующие органы; Оператор в роли специализированного оператора связи, осуществляющий передачу данных в электронном виде принятых от налогоплательщиков/страхователей или их представителей в контролирующие органы.

9.4. Отношения между участниками информационного обмена при представлении отчетов в электронном виде регулируются: Гражданским кодексом Российской Федерации ("Собрание законодательства РФ", 03.12.2001, N 49, ст. 4552); Налоговым кодексом Российской Федерации ("Собрание законодательства РФ", 03.08.1998, N 31, ст. 3824; 07.08.2000, N 32, ст. 3340); Федеральным законом "О бухгалтерском учете" ("Собрание законодательства РФ", 25.11.1996, N 48, ст. 5369); Федеральным законом "Об электронной цифровой подписи" ("Собрание законодательства РФ", 14.01.2002, N 2, ст. 127); Федеральным законом "Об информации, информатизации и защите информации" ("Собрание законодательства РФ", 20.02.1995, N 8, ст. 609); Федеральным законом "О связи" ("Собрание законодательства РФ", 20.02.1995, N 8, ст. 600), другими федеральными законами, иными нормативными правовыми актами, а также настоящим Порядком.

9.5. Представление отчетов в электронном виде осуществляется по инициативе налогоплательщика/страхователя и при наличии у него и контролирующих органов совместимых технических средств и возможностей для их приема и обработки в соответствии со стандартами, форматами и процедурами, утвержденными соответствующими нормативными документами данных структур.

9.6. Представление отчетов в электронном виде осуществляется через специализированного Оператора связи, оказывающего услуги налогоплательщику/страхователю.

9.7. При представлении налоговой декларации в электронном виде в соответствии с Порядком налогоплательщик/страхователь не обязан представлять ее в контролирующий орган на бумажном носителе.

9.8. При представлении отчетности в электронном виде в соответствии с Порядком налогоплательщик/страхователь и контролирующий орган обеспечивают хранение ее в электронном виде в установленном порядке.

9.9. Представление отчетности в электронном виде допускается при обязательном использовании сертифицированных ФСБ средств ЭЦП, позволяющих идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, содержащейся в отчетности в электронном виде.

9.10. Использование, учет, распространение и техническое обслуживание СКЗИ и средств ЭЦП при представлении отчетов в электронном виде осуществляется в соответствии с требованиями законодательства Российской Федерации и иными нормативными правовыми актами.

9.11. При представлении налогоплательщиком/страхователем отчетности в электронном виде контролирующий орган обязан принять отчетность и передать налогоплательщику/страхователю квитанцию о ее приеме, представляющую собой электронный документ с описью полученных файлов, подписанную ЭЦП уполномоченного лица налогоплательщика, заверенную ЭЦП уполномоченного лица налогового органа.

## **10. Регламент взаимодействия участников информационного обмена при представлении отчетности в электронном виде**

10.1. Налогоплательщик/страхователь представляет отчетность в электронном виде в контролирурующий орган, в котором он состоит на учете, посредством Оператора.

10.2. Представление отчетности в электронном виде по телекоммуникационным каналам связи возможно при подключении налогоплательщика/страхователя к Системе DataCrypt, наличии необходимых аппаратных средств, а также соответствующего программного обеспечения, необходимого для работы с Системой DataCrypt. Список требуемого ПО опубликован на сайте <http://www.kemnet.ru/>.

10.3. Оператор предоставляет налогоплательщику/страхователю возможность выполнять с использованием Системы и при условии соблюдения действующего законодательства РФ и настоящего Регламента следующие действия:

10.3.1. Производить передачу отчетности в контролирующие органы;

10.3.2. Передавать в контролирующие органы прочие данные, используя неформализованный документооборот;

10.3.3. Обращаться в ИФНС с запросом на получение информационной выписки (справки об исполнении обязанности по уплате налогов, сборов, страховых взносов, пеней и налоговых санкций; акта сверки расчетов налогоплательщика по налогам, сборам и взносам; перечня бухгалтерской и налоговой отчетности, представленной в отчетном году; выписки операций из карточки «Расчёты с бюджетом»; справки о состоянии расчетов с бюджетом). Обращаться в ПФР с запросом на получение информации по уточнению платежей на интересующую дату.

10.3. При представлении отчетности в электронном виде налогоплательщик/страхователь соблюдает следующий порядок электронного документооборота:

10.3.1. При отправке в органы ИФНС:

- после подготовки отчета, содержащего данные налоговой декларации или бухгалтерской отчетности, налогоплательщик подписывает их ЭЦП уполномоченного лица налогоплательщика и отправляет в зашифрованном виде в адрес ИФНС по месту учета с использованием Системы. Произведенная отправка отображается в личном кабинете абонента Системы с указанием даты и времени отправки. Дата отправки, указанная в личном кабинете, является датой подачи отчета (аналогично почтовому штемпелю в бумажном документообороте);

- в соответствии с Приказом ФНС России № ММ-7-6/534@ от 02.11.2009 не позднее следующего рабочего дня после отправки налоговой декларации (бухгалтерской отчетности) налогоплательщик последовательно получает следующие документы от налоговой инспекции:

- Извещение о получении;
- Квитанция о приеме – документ, который свидетельствует, что отчет прошел форматно-логическую проверку. Квитанция подтверждает факт исполнения налогоплательщиком своей обязанности по представлению отчетности, но не является подтверждением того, что отчет сдан. Если представленный отчет не прошел проверку на соответствие формату, то вместо квитанции о приеме, налогоплательщик получает Уведомление об отказе с указанием причин отказа. Это означает, что отчет не принят. Необходимо исправить ошибки и повторить отправку отчета.
- Извещение о вводе – документ, подтверждающий факт переноса данных отчета в информационные ресурсы налогового органа. Именно этот документ означает то, что ваш отчет принят. Если в отчете содержатся ошибки, то налоговая инспекция высылает в адрес налогоплательщика Уведомление об уточнении, в котором указываются ошибки и содержится сообщение о необходимости представления пояснений или внесения соответствующих исправлений. Это означает, что отчет принят, но требуются уточнения. Необходимо сформировать и отправить корректирующий отчет с необходимыми уточнениями в установленные законом сроки.

10.3.2. При отправке в органы ПФР:

- после подготовки отчета ПФР, страхователь подписывает его ЭЦП уполномоченного лица страхователя и отправляет в зашифрованном виде в адрес ПФР по месту учета с использованием Системы. Произведенная отправка отображается в личном кабинете абонента Системы с указанием даты и време-

ни отправки. Дата отправки, указанная в личном кабинете, является датой подачи отчета (аналогично почтовому штемпелю в бумажном документообороте);

- согласно Информации Пенсионного фонда России от 20 мая 2011 г. «Изменения в порядке представления страхователями отчетности по персонализированному учету и страховым взносам в органы ПФР в 2011 году в электронном виде», Пенсионный фонд в течение 4 рабочих дней отправляет страхователю квитанцию о получении файла (отчета). Наличие квитанции свидетельствует о том, что отчет был получен Пенсионным фондом, но еще не проверен;

- далее, Пенсионный фонд, проверив файл с отчетом, в течение еще 6-ти рабочих дней формирует протокол проверки;

- Положительный протокол свидетельствует об успешной сдаче отчетности. При этом отправленная отчетность считается представленной своевременно, если дата ее отправки в территориальный орган ПФР не позднее срока, установленного действующим законодательством Российской Федерации.
- Отрицательный протокол говорит о том, что при проверке были найдены ошибки. Электронная отчетность не представлена. В случае получения отрицательного протокола необходимо исправить ошибки и повторно отправить сведения.

Таким образом, суммарно весь цикл может занять 10 рабочих дней.

10.3.3. При отправке в органы РосСтат:

- в соответствии с приказом Росстата №370 от 27 октября 2010 г., в течение 1-го рабочего дня с момента отправки отчета, абоненту высылаются:

- Квитанция (извещение) о получении первичных статистических данных, формируемое Территориальным Органом Государственной Статистики (ТОГС).
- Затем, в течение 2-х рабочих дней с момента получения отчета, ТОГС проверяет полученные от абонента данные и формирует один из документов:
  - Положительный протокол (уведомление о приеме в обработку) - подтверждает факт представления отчетности. Отчет принят.
  - Отрицательный протокол (уведомление об ошибке, о несоответствии формату) - содержит описание причин, по которым статистические данные не были приняты. В этом случае следует сформировать отчет, содержащий исправленные данные, и повторно выслать его в адрес ТОГС.

10.3.4. При отправке в органы ФСС:

- В соответствии с приказом ФСС РФ от 12.02.2010 г. № 19, зашифрованный и подписанный с помощью Системы отчет передается страхователем на шлюз ФСС [f4.fss.ru](http://f4.fss.ru), а затем он обрабатывается в течение 24 часов с момента получения.

- После обработки страхователь имеет возможность скачать квитанцию либо протокол проверки на шлюзе ФСС [f4.fss.ru](http://f4.fss.ru) и расшифровать в Системе.

- Квитанция свидетельствует о том, что контроль на шлюзе успешно пройден, расчет считается представленным.
- Протокол проверки свидетельствует о том, что отчет не прошел первичный контроль на соответствие файла электронному формату и корректность ЭЦП. Расчет считается не представленным. Необходимо исправить ошибки и выслать расчет заново. При этом датой представления расчета будет считаться дата получения Фондом уже исправленного расчета, успешно прошедшего этапы контроля.

## 11. Порядок работы при предоставлении информационных услуг

11.1. Для получения информационных услуг налогоплательщик/страхователь подготавливает с помощью Системы запрос на предоставление информации, подписывает документ ЭЦП уполномоченного лица, и отправляет в адрес контролирующего органа по месту своего учета. Запрос должен быть сформирован в соответствии с форматом, утвержденным контролирующими органами.

11.2. Контролирующий орган, получив от налогоплательщика/страхователя запрос, фиксирует дату и время его получения, формирует извещение о получении, подписывает его ЭЦП контролирующего органа и отправляет налогоплательщику/страхователю-отправителю.

- Согласно Информации Пенсионного фонда России от 20 мая 2011 г. «Изменения в порядке представления страхователями отчетности по персонализированному учету и страховым взносам в органы ПФР в 2011 году в электронном виде», Пенсионный фонд в течение 4 рабочих дней отправляет страхователю квитанцию о получении файла запроса. В течение 5 рабочих дней с момента получения запроса, территориальный орган ПФР отправляет формализованный ответ на запрос страхователя;

- В соответствии с Приказом ФНС России № ММ-7-6/381@ от 22.07.2011г. не позднее следующего рабочего дня после отправки запроса налогоплательщик последовательно получает следующие документы от налоговой инспекции:

- Извещение о получении;

- Квитанция о приеме – документ, который свидетельствует, что запрос прошел форматно-логическую проверку. Если представленный запрос не прошел проверку на соответствие формату, то вместо квитанции о приеме, налогоплательщик получает Уведомление об отказе с указанием причин отказа. Это означает, что запрос не принят к обработке. Необходимо исправить ошибки и повторить отправку запроса.
- Формализованный ответ.

11.3. Налогоплательщик/страхователь, получив файл ответа на запрос, с помощью Системы формирует извещение о получении ответа в адрес контролирующего органа, расшифровывает ответ и при необходимости распечатывает его.