УТВЕРЖДАЮ

Генеральный директор ООО «ИНЕТ»

_____ Докучаев Ю.А.

« 01 » июля 2013 года

РЕГЛАМЕНТ

работы в Системе юридически значимого электронного документооборота DataCrypt

Редакция №2

г. Кемерово 2013 год.

1. Основные понятия, используемые в настоящем Регламенте.

Для целей настоящего Регламента используются следующие основные понятия:

Аккредитованный удостоверяющий центр – удостоверяющий центр, который прошел процедуру аккредитации в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» порядке.

Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Запрос на сертификат ключа проверки электронной подписи – электронное сообщение определенного формата и синтаксиса, содержащее необходимую информацию для создания сертификата.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам.

Оператор СЭД - юридическое лицо, участник СЭД осуществляющий управление работой СЭД в целом, приём запросов на изготовление сертификатов от участников СЭД, передачу отчетности участников СЭД в контролирующие органы.

Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

Пользователь СЭД **DataCrypt** ***(далее - Пользователь)*** - лицо, пользующееся услугами СЭД **DataCrypt** и признающее настоящий Регламент.

Сертификат ключа проверки электронной подписи (далее – сертификат ЭП) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

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.

Средства криптографической защиты информации (далее - СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографические преобразования информации для обеспечения ее защиты от несанкционированного доступа, от навязывания ложной информации и/или обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи.

Удостоверяющий центр (далее - УЦ) - юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись(далее ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2.Общие положения

2.1. Целью настоящего Регламента является определение порядка эксплуатации системы юридически значимого электронного документооборота DataCrypt всеми ее участниками.

2.2. В Системе используется только сертифицированные средства ЭП.

2.3. Любое заинтересованное лицо может ознакомиться с Регламентом в офисе Оператора по адресу: г. Кемерово, ул. Д.-Бедного, д. 6, оф. 56 А, а также на сайте Оператора http://www.kemnet.ru/.

2.4. Присоединение к Регламенту осуществляется путем подписания договора на подключение и абонентское обслуживание в системе юридически значимого электронного документооборота DataCrypt.

2.5. Участники Системы безусловно обязуются выполнять требования определяемые настоящим Регламентом.

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

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

3.1. ООО «ИНЕТ» действует как Оператор в Системе.

3.2. ООО «ИНЕТ» осуществляет свою деятельность на территории Российской Федерации на основании лицензий размещенных на сайте Оператора http://www.kemnet.ru/.

3.3. Оператор:

- принимает запрос на сертификат ЭП от Пользователя и передает его в УЦ;
- оказывает услуги Пользователям Системы по передаче отчетности в контролирующие органы;
- обеспечивает актуальность справочника сертификатов ЭП участников Системы;
- может предоставлять Пользователям информационной системы иные, связанные с использованием электронной подписи услуги.

4. Электронный документооборот в системе

4.1. Обмен между участниками Системы осуществляется по правилам и формату определенному Оператором и законом об ЭП.

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

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

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

4.5. Пользователь Системы до начала пользования услугой по организации обмена электронными документами в ЭДО ПФР по ТКС, должен заключить соглашение об обмене электронными документами в системе ЭДО ПФР по ТКС с отделением ПФР по месту регистрации.

5. Порядок представления отчетности в электронном виде по телекоммуникационным каналам связи

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

- Приказами МНС России №№БГ-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 обязательного социального страхования",

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

5.2. 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.

5.3. Представление отчетности 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.

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

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

5.6. Налогоплательщик/страхователь самостоятельно отслеживает срок действия собственного сертификата ЭП и следит, что в период осуществления всего цикла одного документооборота сертификат Пользователя действителен.

5.7. При представлении отчетности в ИФНС и Росстат цикл одного документооборота составляет 5 рабочих дней. При представлении отчетности в ПФР цикл одного документооборота составляет 10 рабочих дней. При представлении отчетности в ФСС цикл одного документооборота составляет 1 рабочий день.

5.8. Если в течение цикла одного документооборота срок действия сертификата Пользователя истечет, ответные квитанции и протоколы не смогут быть высланы Пользователю.

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

5.10. Использование, учет, распространение и техническое обслуживание СКЗИ и средств ЭП при представлении отчетов в электронном виде осуществляется в соответствии с требованиями законодательства РФ и иными нормативными правовыми актами.

6. Порядок взаимодействия участников информационного обмена при представлении отчетности в электронном виде

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

6.2. 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/.

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

6.3.1. Производить передачу отчетности в контролирующие органы (ИФНС, ПФР, Росстат, ФСС);

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

6.3.3. 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 дат.

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

6.4.1. При отправке в органы ИФНС:

- после подготовки отчета, содержащего данные налоговой декларации или бухгалтерской отчетности, налогоплательщик подписывает их ЭП 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.

6.4.2. При отправке в органы ПФР:

- после подготовки отчета ПФР, страхователь подписывает его ЭП 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 времени 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 персонифицированному 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.

6.4.3. 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 высылается:

- 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.

6.4.4. 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, 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 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.

7. Порядок работы при предоставлении информационных услуг

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

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

- Согласно Информации Пенсионного фонда России от 20 мая 2011 г. «Изменения в порядке представления страхователями отчетности по персонифицированному 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.

7.3. 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.

8. Порядок использования электронной подписи

8.1. Особенности использования электронной подписи.

8.1.1. Электронная подпись является аналогом собственноручной подписи лица.

8.1.2. Информация в электронной форме, подписанная ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

8.1.3. Электронный документ, подписанный ЭП, признается юридически значимым! Поставив свою ЭП Вы соглашаетесь с тем, что написано в документе. Будьте внимательны при использовании ЭП. Внимательно проверяйте, какие документы Вы подписываете, так же, как Вы проверяете, что подписываете на бумажном носителе.

8.2. Общий порядок организации работ при использовании СКЗИ

8.2.1. К работе с ключами электронной подписи и средствами криптографической защиты информации (СКЗИ) допускаются лица после ознакомления со следующими соответствующими нормативными документами:

- Федеральным законом «Об электронной подписи» №63-ФЗ от 6 апреля 2011 года.
- Федеральным законом «О персональных данных» №152-ФЗ от 27 июля 2006 года.
- Регламентом Удостоверяющего центра, которым был осуществлен выпуск электронной подписи.
- Правилами, инструкциями по обеспечению безопасности, принятыми в организации.

8.2.2. На рабочем месте, на котором производится работа с ключами проверки электронной подписи, должно применяться только лицензионное программное обеспечение.

9. Обязанности Пользователя СЭД DataCrypt как владельца сертификата ключей проверки электронной подписи и пользователя СКЗИ

9.1. Владелец сертификата ЭП обязан применять личный ключ проверки электронной подписи только в соответствии с областями действия, указанными в соответствующем данному ключу проверки ЭП сертификате ЭП.

9.2. Владелец ключей проверки ЭП обязан хранить в тайне личный ключ проверки ЭП, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

9.3. Владелец ключей проверки электронной подписи, пользователь СКЗИ не должен:

- оставлять без контроля ключевые носители, содержащие ключи проверки электронной подписи;

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- передавать ключевые носители, содержащие ключи проверки электронной подписи, лицам, к ним не допущенным;
- изменять настройки, установленные программой установки СКЗИ или администратором;

9.4. Владелец ключей проверки ЭП обязан не применять личный ключ проверки ЭП если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

9.5. Владелец сертификата ЭП обязан немедленно обратиться в УЦ с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения личного ключа проверки электронной подписи (компрометации), а также в случае, если стало известно, что этот ключ используется или использовался ранее другими лицами.

9.6. Владелец сертификата ЭП обязан не использовать личный ключ проверки ЭП, связанный с сертификатом ЭП, который аннулирован (отозван) или действие его приостановлено.

9.7. Владелец сертификата ЭП обязан 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.

9.8. Владелец сертификата ЭП обязан самостоятельно отслеживать срок окончания собственного сертификата ЭП и не позднее чем за 7 рабочих дней обратиться к Оператору системы для планового перевыпуска сертификата ЭП с полным пакетом необходимых документов в соответствии с требованиями Удостоверяющего центра.

9.9. При несоблюдении требований, изложенных в п.5.1.-5.2., возмещение причиненных вследствие этого убытков возлагается на участника Системы

10. Риски, связанные с использованием электронных подписей

10.1. В случае несанкционированного доступа (потере, кражи и т.д.) к ключевому носителю, ключам проверки электронной подписи, злоумышленник может за Вас подписать документ без Вашего ведома.

10.2. Поломка ключевого носителя влечет за собой уничтожение ключей проверки ЭП. Восстановление ключей проверки ЭП невозможно, Удостоверяющий центр не хранит копии ключей проверки электронных подписей владельцев сертификатов ключей подписи!

10.3. Во избежание зависимости от надежности ключевого носителя настоятельно рекомендуется создавать копии ключевых контейнеров.

10.4. При подписании электронного документа электронной подписью, срок действия которой истек, данный документ будет признан недействительным. Отслеживайте сроки действия электронной подписи. Срок действия сертификата Вы можете посмотреть в бумажной версии сертификата ключа проверки электронной подписи или в электронной версии сертификата.