

**ВРЕМЕННЫЙ РЕГЛАМЕНТ
ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ С ЭЦП
ПО ТЕЛЕКОММУНИКАЦИОННЫМ КАНАЛАМ СВЯЗИ В УНИФИЦИРОВАННОЙ
СИСТЕМЕ ПРИЕМА, ХРАНЕНИЯ И ПЕРВИЧНОЙ ОБРАБОТКИ НАЛОГОВЫХ
ДЕКЛАРАЦИЙ И БУХГАЛТЕРСКОЙ ОТЧЕТНОСТИ**

1. Введение

Настоящий Регламент разработан на основании действующего законодательства Российской Федерации и определяет:

- порядок подключения Пользователей к системе информационного обмена электронными документами с ЭЦП по телекоммуникационным каналам связи (далее - Система);
- порядок обмена информацией между Участниками Системы;
- порядок организации защиты информации в Системе при обмене электронными документами.

2. Термины, используемые в Регламенте

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Доверенный удостоверяющий центр - действующий удостоверяющий центр (УЦ), прошедший аккредитацию в сети доверенных УЦ в соответствии с Приказом ФНС России от 13.06.2006 N САЭ-3-27/346@ "Об организации сети доверенных удостоверяющих центров". Список Доверенных УЦ публикуется на Интернет-сайте ФГУП ГНИВЦ ФНС России (www.gnivc.ru).

Заявка - заявка Пользователя на подключение к унифицированной системе приема, хранения и первичной обработки налоговых деклараций и бухгалтерской отчетности.

Заявление - заявление Пользователя о присоединении к Системе.

Закрытый (секретный) ключ ЭЦП - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания (с использованием средств ЭЦП) в электронных документах электронной цифровой подписи. Закрытые ключи хранятся Пользователями Системы в тайне. Закрытые ключи применяются Пользователем для формирования ЭЦП в электронных документах и шифрования информации.

Квитанция о приемке налоговой декларации (формы бухгалтерской отчетности) - электронный документ, формируемый налоговым органом и содержащий налоговую декларацию (форму бухгалтерской отчетности) в электронном виде, подписанную ЭЦП налогоплательщика и заверенную ЭЦП налогового органа.

Ключевой носитель - отчуждаемый носитель (дискета, eToken, и т.п.), содержащий один или несколько ключей ЭЦП.

Компрометация ключа ЭЦП - утрата доверия к тому, что используемые закрытые ключи ЭЦП недоступны посторонним лицам.

Конфиденциальная информация - требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации, а также настоящим Регламентом.

Конфликтная ситуация - ситуация, при которой у Участников Системы возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

Некорректный электронный документ - электронный документ, не прошедший процедуры проверки ЭЦП, имеющий искажения в тексте сообщения, не позволяющие понять его смысл, или содержащий реквизиты отправителя, не соответствующие реквизитам, закрепленным за владельцем СКП, подписью которого заверен документ.

Несанкционированный доступ (НСД) к информации - доступ к информации, нарушающий установленные правила разграничения доступа.

Неформализованное сообщение - сообщение в виде электронного документа, для которого не существует утвержденного электронного формата представления.

Открытый ключ ЭЦП - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому Участнику информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе. Открытый ключ Пользователя является действующим на момент подписания, если он зарегистрирован (сертифицирован), введен в действие и не включен в список отозванных сертификатов (СОС).

Подтверждение отправки - содержащий ЭЦП электронный документ от налогового органа или специализированного оператора связи, в котором зафиксирована дата и время отправки налогоплательщиком налоговой декларации (бухгалтерской отчетности) в электронном виде по телекоммуникационным каналам связи.

Пользователь - налоговый орган или налогоплательщик (хозяйствующий субъект, в т.ч. кредитная организация), осуществляющий информационный обмен в рамках Системы и признающий данный Регламент.

Протокол входного контроля налоговой декларации (формы бухгалтерской отчетности) - электронный документ, формируемый налоговым органом и подписанный ЭЦП налогового органа, содержащий результаты проверки налоговой декларации (формы бухгалтерской отчетности) на соответствие требованиям утвержденного формата представления налоговой и бухгалтерской отчетности в электронном виде и правилам ее заполнения;

Сертификат ключа подписи (СКП) - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного должностного лица удостоверяющего центра, включающий в себя открытый ключ ЭЦП и/или шифрования, которые выдаются удостоверяющим центром участнику информационного обмена электронными документами для подтверждения подлинности ЭЦП, идентификации владельца сертификата ключа подписи и/или обеспечения защиты от искажения информации в электронном документе.

Система информационного обмена электронными документами с ЭЦП по телекоммуникационным каналам связи (далее - Система) - совокупность программных и аппаратных средств, обеспечивающих представление налоговой и бухгалтерской отчетности и информационных услуг в электронном виде по телекоммуникационным каналам связи, принадлежащая Участникам Системы, а также совокупность нормативных и организационно-методических документов, регламентирующих взаимоотношения Участников Системы.

СОС (список отозванных сертификатов - certificate revocation list, CRL) - список отозванных сертификатов ключей подписи. СОС публикуется на Интернет-сайте ФГУП ГНИВЦ ФНС России (www.gnivc.ru).

Средства криптографической защиты информации (СКЗИ) - сертифицированные в порядке, установленном законодательством Российской Федерации, аппаратные и (или) программные средства, обеспечивающие шифрование, контроль целостности и применение ЭЦП при обмене электронными документами в Системе и совместимые с СКЗИ, используемыми в системе ФНС России.

Средства ЭЦП - сертифицированные в порядке, установленном законодательством Российской Федерации, аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП;
- подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе;
- создание закрытых и открытых ключей ЭЦП.

Управление ключами - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также выдача и отзыв сертификатов ключей подписи в соответствии с регламентом удостоверяющего центра.

Участники Системы - налоговые органы и налогоплательщики (хозяйствующие субъекты, в т.ч. кредитные организации), осуществляющие обмен электронными документами с ЭЦП в Системе, а также организации, предоставляющие услуги по обеспечению и обслуживанию осуществляемого обмена.

Формат представления электронных документов - формализованное описание состава, структуры, а также требований к формированию представляемых в электронном виде показателей налоговых деклараций, бухгалтерской отчетности и документов, определенных ФНС России для обеспечения информационного обслуживания налогоплательщиков.

Электронный документ (ЭД) с ЭЦП - документ, в котором информация представлена в электронно-цифровой форме и содержащий ЭЦП.

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

ЭЦП налогоплательщика - ЭЦП, владельцем сертификата ключа которой является должностное лицо налогоплательщика (хозяйствующего субъекта), использующее средства ЭЦП в рамках Системы.

ЭЦП налогового органа - ЭЦП, владельцем сертификата ключа которой является должностное лицо налогового органа, использующее средства ЭЦП в рамках Системы.

3. Общие положения

Регламент - публичный, общедоступный документ, обязательный для исполнения всеми участниками Системы. Регламент содержит процедурные вопросы и правила работы в Системе, определяет порядок защиты информации и разбора конфликтных ситуаций при обмене электронными документами, содержит образцы документов, необходимых для подключения и работы в Системе.

Регламент начинает действовать между Пользователем и налоговым органом с момента подписания Заявления о присоединении к Системе (Приложение 1). При обмене электронными документами в Системе Пользователи должны руководствоваться положениями настоящего Регламента.

Пользователи должны применять для защиты информации средства ЭЦП и СКЗИ, сертифицированные в порядке, установленном законодательством Российской Федерации.

Доверенный удостоверяющий центр осуществляет работы по управлению ключами на основании Заявки Пользователя на подключение к Системе (Приложение 2) и договора с УЦ.

Используемые во взаимоотношениях между Пользователями электронные документы, заверенные ЭЦП, являются оригиналами, имеют юридическую силу, в соответствии с требованиями законодательства Российской Федерации подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

Пользователи признают, что применение в Системе сертифицированных средств ЭЦП и СКЗИ, которые реализуют ЭЦП и шифрование, достаточно для обеспечения конфиденциальности информационного взаимодействия, а также подтверждения того, что электронный документ:

- исходит от Пользователя (подтверждение авторства документа);

- не претерпел изменений при информационном взаимодействии Пользователей в рамках Системы (подтверждение целостности и подлинности документа).

Пользователи осуществляют обмен электронными документами в соответствии с настоящим Регламентом и только в рамках взаимодействия Участников Системы.

Пользователи соблюдают установленный настоящим Регламентом порядок взаимодействия Участников Системы при обмене электронными документами и проверке их подлинности.

Система строится по общим принципам, единым для всех Пользователей на территории Российской Федерации.

В рамках Системы Пользователи применяют разработанное или сертифицированное ГНИВЦ ФНС России ПО.

Все электронные документы (в т.ч. неформализованные сообщения <*> - файлы, созданные в распространенных форматах, таких как MS Word, MS Excel, RTF (.doc; .xls; .rtf)), квитанции и протоколы, передаваемые в рамках Системы, должны быть заверены ЭЦП отправителя и переданы по телекоммуникационным каналам связи только в зашифрованном виде.

<*> Примечание: При обмене неформализованными сообщениями Пользователь самостоятельно обеспечивает безопасность использования электронных документов средствами антивирусной защиты.

Налоговый орган (или специализированный оператор связи, в случае представления налоговых деклараций (бухгалтерской отчетности) через специализированных операторов) при получении заверенного ЭЦП налогоплательщика электронного документа, содержащего налоговую декларацию (бухгалтерскую отчетность), должен сформировать подтверждение отправки, содержащее дату представления налогоплательщиком данного электронного документа в налоговый орган. Подтверждение отправки, заверенное ЭЦП налогового органа, доставляется отправителю документа.

Пользователи подтверждают получение электронных документов, содержащих ЭЦП, заверяя эти документы ЭЦП и направляя их в адрес отправителя. Электронные документы, содержащие ЭЦП отправителя и получателя (квитанции), сохраняются Пользователями.

В случае, когда для обработки электронного документа налоговым органом требуется соответствие утвержденному ФНС России электронному формату представления документа или другим требованиям, предъявляемым ФНС России, налоговый орган высылает налогоплательщику протокол входного контроля.

Документ, содержащий налоговую декларацию (бухгалтерскую отчетность), считается представленным в электронном виде в налоговый орган с момента получения налогоплательщиком подтверждения отправки.

Представленный налогоплательщиком документ, содержащий налоговую декларацию (бухгалтерскую отчетность) в электронном виде с ЭЦП, считается принятым налоговым органом с момента получения налогоплательщиком из налогового органа:

- протокола входного контроля;
- квитанции о приемке, содержащей заверенный ЭЦП налогового органа представленный налогоплательщиком документ.

Налоговый орган отказывает в приеме представленного налогоплательщиком электронного документа по следующим причинам:

- документ не может быть расшифрован;
- ЭЦП в документе отсутствует или документ подписан ЭЦП лица, не имеющего права подписи данного документа;
- документ представлен в несоответствующем формате.

Обмен неформализованными сообщениями в виде ЭД допускается по запросу налогового органа в случаях, предусмотренных налоговым законодательством с целью повышения качества налогового администрирования.

В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, заверенных ЭЦП, или в иных конфликтных ситуациях, связанных с использованием ЭЦП, Стороны руководствуются Порядком разрешения конфликтных ситуаций, изложенным в главе 11 настоящего Регламента.

4. Общие вопросы организации защиты информации при обмене электронными документами

На основании Заявки Пользователя (Приложение 2) Доверенный удостоверяющий центр изготавливает и передает Пользователю закрытые и соответствующие им открытые ключи ЭЦП на ключевых носителях и сертификаты ключей подписи в электронном виде на магнитных носителях. Одновременно Доверенный удостоверяющий центр оформляет изготовленные СКП в форме документов на бумажных носителях в двух экземплярах, каждый из которых заверяется собственноручной подписью владельца СКП и уполномоченного должностного лица Доверенного удостоверяющего центра. Один экземпляр каждого сертификата ключа подписи на бумажном носителе выдается владельцу сертификата ключа подписи, второй - остается в Доверенном удостоверяющем центре.

Доверенный удостоверяющий центр использует программные и технические средства генерации ключевой информации в неизменном виде по отношению к сертифицированному эталону. Доверенный удостоверяющий центр гарантирует отсутствие привнесенных нерегламентированных процедур скрытого копирования индивидуальной секретной ключевой информации в используемых программных и технических средствах.

Пользователь получает доступ к реестру сертификатов ключей подписи Участников Системы и списку отозванных сертификатов (СОС), публикуемых на Интернет-сайте Доверенного Удостоверяющего центра и на сайте ФГУП ГНИВЦ ФНС России (www.gnivc.ru).

Срок действия ключей ЭЦП Пользователя Системы составляет 1 (один) год. Начало периода действия ключей ЭЦП исчисляется с даты и времени начала действия соответствующих им СКП.

Участники Системы обязаны обеспечить сохранность полученной в рамках Системы конфиденциальной информации в соответствии с действующим законодательством Российской Федерации.

Программное обеспечение, позволяющее производить информационный обмен между Пользователями Системы, должно обеспечивать:

- применение протоколов SMTP/POP3;
- унифицированный формат транспортного сообщения, утвержденный Приказом ФНС России N САЭ 3-13/345@ от 13 июня 2006 года "Об унифицированном формате информационного взаимодействия";
- взаимодействие с СКП Участников Системы;
- возможность проверки статуса СКП Участников Системы.

Для обеспечения проверки статуса СКП Участников Системы Пользователи должны применять:

- действующий СКП Участника Системы;
- СОС Доверенного УЦ, выдавшего Участнику Системы СКП;
- СКП Доверенного УЦ, выдавшего Участнику Системы СКП;
- СКП Участников Системы, с которыми взаимодействует Пользователь;
- СОС УЦ, выдавших СКП Участникам Системы, с которыми взаимодействует Пользователь;
- СКП УЦ, выдавших СКП Участникам Системы, с которыми взаимодействует Пользователь.

Распространение и обслуживание соответствующего ПО может осуществляться Доверенными УЦ или третьими лицами.

5. Порядок взаимодействия Участников Системы

Любая операция, выполняемая Участниками в рамках Системы, относится в целом к процессу обмена электронными документами между налоговыми органами и налогоплательщиками.

Форматы представления налоговой и бухгалтерской отчетности в электронном виде утверждаются и вводятся в действие в порядке, определенном Министерством финансов Российской Федерации или приказом ФНС России.

Электронный вид представляемых форм налоговых деклараций (бухгалтерской отчетности) разрабатывается и сопровождается в соответствии с утвержденными и опубликованными ФНС России форматами.

Налоговые органы обеспечивают доступ всех заинтересованных лиц к описанию форматов, публикуя их на Интернет-сайтах ФНС России (www.nalog.ru) и Управлений ФНС России субъектов Российской Федерации, в официальных периодических изданиях, а также предоставляют консультации по вопросам применения форматов.

Начиная со дня ввода в действие формата электронного представления форм налоговых деклараций (бухгалтерской отчетности), налогоплательщик, представляющий отчетность в электронном виде, должен обеспечить соответствие отчетности введенному в действие формату и применив ПО, разработанное или сертифицированное ГНИВЦ ФНС России на соответствие требованиям нормативных документов, регламентирующих процесс представления отчетности в электронном виде (в т.ч. на соответствие требованиям Приказа ФНС России N САЭ-3-13/345@ от 13.06.2006 "Об унифицированном формате информационного взаимодействия"), передать отчетность в налоговый орган по телекоммуникационным каналам связи.

Налогоплательщик подготавливает налоговые декларации (бухгалтерскую отчетность) в соответствии с утвержденными форматами в электронном виде с ЭЦП (набором ЭЦП) и представляет их по телекоммуникационным каналам связи в налоговый орган. При этом в соответствии с настоящим Регламентом информационный обмен между налогоплательщиком и налоговым органом реализуется следующими электронными документами:

- подтверждение отправки, содержащее дату отправки налогоплательщиком налоговой декларации (бухгалтерской отчетности), формируемое в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности);
- протокол входного контроля налоговой декларации (бухгалтерской отчетности), формируемый в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности);
- квитанция о приемке налоговой декларации (бухгалтерской отчетности) в электронном виде, формируемая в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности).

Налогоплательщик, получивший подтверждение отправки, содержащее дату отправки налоговой декларации (бухгалтерской отчетности) в налоговый орган, проверяет подлинность ЭЦП в подтверждении отправки, заверяет подтверждение отправки ЭЦП налогоплательщика и в течение суток (без учета выходных и праздничных дней) высылает в адрес отправителя подтверждения. Налоговая декларация (бухгалтерская отчетность) считается представленной налогоплательщиком в налоговый орган. Подтверждение отправки, содержащее ЭЦП обеих сторон (отправителя и получателя), сохраняется как отправителем, так и получателем в соответствующих хранилищах электронных документов.

Если в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности) налогоплательщик не получил соответствующее подтверждение отправки, он заявляет в налоговый орган (или специализированному оператору связи, в случае представления налоговых деклараций (бухгалтерской отчетности) через специализированных операторов) о данном факте и, при необходимости, повторяет процедуру представления.

Налогоплательщик, получивший протокол входного контроля представленной налоговой декларации (бухгалтерской отчетности), проверяет подлинность содержащейся в протоколе ЭЦП налогового органа, заверяет протокол ЭЦП налогоплательщика и в течение суток (без учета выходных и праздничных дней) высылает в адрес налогового органа. Содержащий ЭЦП налогового органа и налогоплательщика протокол сохраняется в соответствующих хранилищах электронных документов.

Налогоплательщик, получивший квитанцию о приемке - представленную налогоплательщиком налоговую декларацию (бухгалтерскую отчетность), заверенную ЭЦП налогового органа, проверяет подлинность содержащейся в квитанции ЭЦП налогового органа и сохраняет квитанцию в хранилище электронных документов.

Если в протоколе входного контроля содержится информация, что представленная налоговая декларация (бухгалтерская отчетность) содержит ошибки, налогоплательщик в течение пяти суток (без учета выходных и праздничных дней) устраняет указанные налоговым органом ошибки, заново подготавливает налоговую декларацию (бухгалтерскую отчетность) в электронном виде с ЭЦП и отправляет ее в адрес налогового органа, повторяя процедуру представления налоговой декларации (бухгалтерской отчетности).

Если в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности) налогоплательщик не получил из налогового органа протокол входного контроля и/или квитанцию о приемке представленной налоговой декларации (бухгалтерской отчетности), он заявляет в налоговый орган (или специализированному оператору связи, в случае представления налоговых деклараций (бухгалтерской отчетности) через специализированных операторов) о данном факте и, при необходимости, повторяет процедуру представления налоговой декларации (бухгалтерской отчетности).

Налоговая декларация (бухгалтерская отчетность) считается принятой налоговым органом по установленной форме в электронном виде в соответствии с законодательством Российской Федерации в случае, если налогоплательщик получил следующие электронные документы:

- формируемое налоговым органом или специализированным оператором связи подтверждение отправки, содержащее дату отправки налоговой декларации (бухгалтерской отчетности);
- формируемый налоговым органом протокол входного контроля, содержащий результаты проверки налоговой декларации (формы бухгалтерской отчетности) на соответствие требованиям утвержденного формата электронного представления;
- формируемую налоговым органом квитанцию о приемке - представленную налогоплательщиком налоговую декларацию (бухгалтерскую отчетность), заверенную ЭЦП налогового органа.

Неформализованное сообщение в виде электронного документа с ЭЦП Пользователя принято налоговым органом, если Пользователь получил из налогового органа следующие электронные документы:

- подтверждение отправки, содержащее дату отправки неформализованного сообщения;
- квитанцию о приемке - неформализованное сообщение, заверенное ЭЦП налогового органа.

Неформализованное сообщение в виде электронного документа с ЭЦП налогового органа принято Пользователем, если налоговый орган получил сформированное Пользователем подтверждение отправки - электронный документ с ЭЦП, содержащий дату отправки налоговым органом неформализованного сообщения.

6. Порядок подключения Пользователей к Системе

Для осуществления информационного обмена в рамках Системы Пользователю необходимо:

- ознакомиться с настоящим Регламентом;
- подать в налоговый орган Заявление о присоединении к Системе;
- заполнить и заверить печатью налогового органа Заявку <*> на подключение к Системе;

<*> Примечание: Если Пользователь сдает отчетность в нескольких налоговых инспекциях, Заявки необходимо заверить в каждой из них.

- получить СКП в Доверенном УЦ, предоставив:
- заверенную налоговым органом Заявку на подключение к Системе;
- доверенность по специальной форме (Приложение 3) от имени каждого сотрудника организации, которому необходимо изготовить СКП (если СКП получает другое лицо);
- документ, удостоверяющий личность лица, получающего ЭЦП и СКП.

7. Права и обязанности Участников Системы

Налоговый орган обязан:

- использовать программно-аппаратные комплексы в соответствии с эксплуатационной документацией и только в рамках Системы;
- немедленно приостанавливать обмен электронными документами с Пользователем, подписанными ЭЦП Пользователя, при получении сообщения о компрометации этого ключа ЭЦП Пользователя;
- немедленно информировать Доверенный УЦ в случае компрометации ключа ЭЦП;
- своевременно извещать Пользователя об изменениях во взаимодействии налоговых органов и налогоплательщиков в Системе.

Налоговый орган может привлекать Доверенный удостоверяющий центр к работе по разрешению конфликтных ситуаций.

Доверенный УЦ в процессе обеспечения информационного обмена в рамках Системы обязан осуществлять регулирование отношений с Пользователями в соответствии с Федеральными законами и иными нормативными

правовыми актами Российской Федерации и ФНС России (в т.ч. Приказом N САЭ-3-27/346@ от 13.06.2006 "Об организации сети доверенных удостоверяющих центров"), регламентирующими деятельность в области электронного документооборота с использованием ЭЦП, а также настоящим Регламентом.

Пользователь системы обязан:

- соблюдать положения настоящего Регламента;
- немедленно требовать аннулирования СКП в случае компрометации ключей ЭЦП, а также в случае изменений сведений, указанных в СКП, либо в случае прекращения действия документа, на основании которого он оформлен;
- использовать ПО, разработанное или сертифицированное ГНИВЦ ФНС России (информация о сертифицированном ПО публикуется на Интернет-сайте www.gnivc.ru), позволяющее производить информационный обмен между Участниками Системы только в рамках Системы;
- руководствоваться положениями и инструкциями эксплуатационной документации ПО;
- применять СКЗИ в соответствии с требованиями законодательства Российской Федерации и только в рамках Системы;
- хранить в тайне закрытый ключ ЭЦП и принимать меры для предотвращения его компрометации;
- при уничтожении утративших силу ключей ЭЦП обеспечивать расшифровывание зашифрованных этими ключами электронных документов и хранение их в расшифрованном виде в соответствии с требованиями, установленными законодательством Российской Федерации и настоящим Регламентом. Перед уничтожением ключей ЭЦП необходимо расшифровать все ЭД, зашифрованные с их использованием, иначе в дальнейшем прочитать эти документы будет невозможно.

Пользователь имеет право запрашивать подтверждения по полученным электронным документам в случае возникновения сомнений в их подлинности, самостоятельно определять необходимость проверки нахождения СКП отправителя в СОС, а также требовать исполнения обязательств по принятым электронным документам от других Участников Системы.

Участникам Системы запрещается принимать к исполнению электронные документы с ЭЦП в следующих случаях:

- сертификат ключа подписи отправителя утратил силу (не действует, находится в СОС) на момент проверки или на момент создания ЭЦП в документе;
- не подтверждена подлинность ЭЦП в электронном документе;
- использование ЭЦП не соответствует сведениям, указанным в СКП;
- электронный документ с ЭЦП лица, не имеющего права на утверждение данного документа.

8. Действия Участников Системы в случае компрометации ключей ЭЦП

Доверенный УЦ уведомляет Пользователей о ставших ему известных фактах, которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и СКП.

Доверенный УЦ в момент генерации и сертификации ключей ЭЦП передает Пользователю пароль для экстренной связи в случае компрометации закрытых ключей ЭЦП. Пользователь обеспечивает сохранение конфиденциальности пароля.

Пользователь в случае компрометации собственных ключей ЭЦП обязан немедленно по телефонным каналам связи с использованием устного пароля или факсимильным сообщением, заверенным подписью и печатью Пользователя, информировать Доверенный УЦ о наступлении события, трактуемого как компрометация.

При компрометации ключа ЭЦП Пользователь должен прекратить обмен электронными документами с Участниками Системы.

Доверенный УЦ, получивший сообщение о компрометации ключей Пользователя, должен убедиться в достоверности сообщения о компрометации (запросить пароль или факсимильное сообщение, заверенное подписью и печатью Пользователя) и после этого обязан немедленно аннулировать скомпрометированные ключи ЭЦП (занести в СОС соответствующие СКП).

Пользователь, объявивший о компрометации собственных криптографических ключей, в течение одного рабочего дня документально оформляет уведомление и направляет его в Доверенный УЦ.

Пользователь, допустивший компрометацию собственных криптографических ключей, несет все издержки, связанные с генерацией новых ключей, их сертификацией и вводом в действие.

9. Ответственность Участников Системы

За невыполнение либо ненадлежащее исполнение обязательств виновный Участник Системы несет ответственность в порядке и на основаниях, предусмотренных действующим законодательством Российской Федерации.

Доверенный УЦ не отвечает за последствия компрометации Пользователем используемых закрытых ключей ЭЦП и иных нарушений Регламента, допущенных Пользователем.

Участники Системы освобождаются от ответственности за частичное или полное неисполнение условий Регламента, в случае, если такое неисполнение явилось следствием непреодолимой силы, то есть чрезвычайных и неотвратимых обстоятельств, не зависящих от воли Участников, в том числе: принятия органами государственной власти, ФНС России, УФНС, законодательных и нормативных актов, распоряжений, приказов, препятствующих исполнению условий по настоящему Регламенту.

Участник, ссылающийся на обстоятельства непреодолимой силы, обязан незамедлительно (не позднее чем в 5-дневный срок с момента наступления) известить другую сторону о наступлении этих обстоятельств.

Извещение должно содержать данные о характере обстоятельств и оценку их влияния на возможность исполнения Участником своих обязательств. Несвоевременное извещение Участником о наступлении обстоятельств, освобождающих ее от ответственности, влечет за собой утрату права для этого Участника ссылаться на эти обстоятельства.

Все предоставленные Участникам Системы данные или любые сведения, отнесенные к конфиденциальной информации в соответствии с действующим законодательством Российской Федерации, являются исключительной собственностью Участников и не подлежат разглашению Участниками или передаче третьим лицам ни при каких обстоятельствах, кроме случаев, предусмотренных законодательством Российской Федерации.

Налоговый орган несет ответственность перед Пользователями за своевременность обработки информации, поступающей от Пользователей в электронном виде по телекоммуникационным каналам связи, и предоставление всех необходимых в соответствии с нормативными актами ФНС РФ подтверждений и квитанций в электронном виде.

Налоговый орган несет ответственность за своевременное доведение до сведений Пользователей информации об изменении в представлении отчетности в электронном виде по телекоммуникационным каналам связи, публикуя соответствующую информацию на Интернет-сайте ФНС России и Управлений ФНС России субъектов Российской Федерации <*>.

<*> Ст. 21, 32 НК РФ, Приказ МНС России от 31.12.2002 N БГ-3-06/756 "О порядке ввода в действие новых форм налоговых деклараций". Распоряжение МНС РФ от 13.02.2004 N 44 "Об информационном наполнении Интернет-сайта ФНС России".

Доверенный УЦ не несет ответственности перед владельцами СКП и лицами, использующими СКП для проверки подписи и шифрования сообщений, а также перед третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием СКП, независимо от суммы заключенных с использованием СКП сделок и совершения ими иных действий, за исключением случаев нарушения Доверенным удостоверяющим центром обязательств, предусмотренных настоящим Регламентом и действующим законодательством Российской Федерации.

10. Порядок взаимодействия Участников Системы при нештатных ситуациях, связанных с эксплуатацией СКЗИ

При возникновении нештатных ситуаций, таких, как выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств ЭЦП и др., Пользователь обязан:

- руководствоваться положениями и инструкциями эксплуатационной документации;
- сообщить о возникшей ситуации Доверенному удостоверяющему центру;
- выполнить указания Доверенного удостоверяющего центра, касающиеся выхода из данной нештатной ситуации.

11. Порядок разрешения конфликтных ситуаций, возникающих при информационном обмене в рамках Системы

При возникновении конфликтной ситуации, связанной с тем, что Участники Системы по-разному трактуют содержание одного и того же электронного документа, комиссия, созданная для разрешения спора, на основании архивных копий документа (подписанных ЭЦП с обеих сторон), предъявленных сторонами Участников, организует экспертизу, на основании которой выносится решение о корректности ЭЦП каждой из сторон в данном электронном документе.

При возникновении конфликтной ситуации, связанной с тем, что стороны по-разному трактуют дату поступления Электронного документа от отправителя получателю, решение об истинной дате поступления документа выносится на основании архивных файлов подтверждений отправки, подписанных ЭЦП налогового органа и налогоплательщика.

Разрешая конфликтные ситуации при нарушении процедур криптографической защиты информации и/или установлении авторства и/или подлинности электронных документов, заверенных ЭЦП, Участники Системы исходят из того, что:

- в соответствии с действующим законодательством документ в электронном виде, заверенный ЭЦП, является документом, имеющим юридическую силу, аналогичным бумажному, снабженному подписью и печатью;
- подтверждением даты представления электронного документа является получение отправителем подтверждения отправки электронного документа;
- используемая в соответствии с настоящим Регламентом система защиты информации, которая обеспечивается ЭЦП и шифрованием, достаточна для защиты информации от несанкционированного доступа, подтверждения целостности, подлинности и авторства электронных документов, а также для разрешения конфликтных ситуаций по ним;

- Математические свойства алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р34.10-94 (или ГОСТ Р34.10-2001) и ГОСТ Р34.11-94, свидетельствуют о невозможности подделки значения ЭЦП любым лицом, не обладающим закрытым криптографическим ключом ЭЦП. Участник Системы признает, что разбор конфликтной ситуации в отношении авторства, целостности и подлинности электронного документа заключается в доказательстве подписания конкретного электронного документа на конкретном ключе ЭЦП.

В соответствии с настоящим порядком подлежат разрешению конфликтные ситуации двух типов:

- некорректность входящего электронного документа или ЭЦП (конфликтная ситуация типа А);
- для корректного электронного документа непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности (конфликтная ситуация типа Б).

Порядок разрешения конфликтных ситуаций (тип А)

Действия сторон в данной ситуации заключаются в следующем.

Принимающая сторона по телефону (или иным образом) запрашивает у отправляющей стороны информацию о документе, подлинность которого вызывает сомнения. При получении подтверждения об отправке указанного документа запрашивает повторное оформление и отправку данного документа.

Результатом повторной обработки принимающей стороной полученного документа может быть:

А.1. Проверка ЭЦП в повторно переданном документе дала отрицательный результат.

В этом случае делается вывод о возможном нарушении действующего криптографического ключа либо о неисправности программно-аппаратных средств одной из сторон.

При этом необходимо:

- проверить сертификаты открытых ключей;
- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ. Переустановить его в случае необходимости.

Если положительный результат не достигнут, необходимо обратиться в Доверенный УЦ.

А.2. Повторная проверка дала положительный результат, - электронный документ корректен, ЭЦП верна.

Порядок разрешения конфликтных ситуаций (тип Б)

Если одна из сторон приходит к выводу, что другая сторона ссылается на документ, который не отправлялся и/или на измененный по содержанию документ, эта сторона немедленно извещает Доверенный УЦ о наличии такой конфликтной ситуации.

Доверенный УЦ формирует Экспертную (согласительную) комиссию для разрешения конфликтной ситуации, в состав которой входят представители Доверенного УЦ и Участники, вовлеченные в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные независимые специалисты в области криптографической защиты информации.

В ходе работы Экспертной комиссии рассматриваются все документы и материалы, относящиеся к предмету разногласий, и выполняется процедура проверки ЭЦП документа. Экспертной комиссии должны быть представлены следующие данные:

- электронный документ с ЭЦП, авторство которого оспаривается;
- архивные копии этого электронного документа с ЭЦП, переданные Участниками, вовлеченными в конфликтную ситуацию;
- сертификаты ключей подписи;
- дистрибутивы СКЗИ;
- ключевые носители.

При необходимости Экспертная комиссия имеет право провести экспертизу ПЭВМ Участников, вовлеченных в конфликтную ситуацию.

Экспертиза проводится на Автоматизированном рабочем месте Доверенного УЦ.

Экспертная комиссия подтверждает или опровергает авторство Участника для документа, вызвавшего данную конфликтную ситуацию. Решение Экспертной комиссии оформляется в виде Протокола.

12. Прочие условия

Изменения и дополнения в настоящий Регламент вносятся приказом ФНС России.

Все приложения являются неотъемлемой частью настоящего Регламента:

Приложение 1. Форма Заявления о присоединении к Системе.

Приложение 2. Форма Заявки Пользователя на подключение к Системе.

Приложение 3. Образец доверенности.

Приложение 1

Заявление N _____

о присоединении к Системе информационного обмена электронными документами с ЭЦП по телекоммуникационным каналам связи

наименование организации, включая организационно-правовую форму
в лице _____

должность

Фамилия, Имя, Отчество

с Регламентом обмена электронными документами с ЭЦП по телекоммуникационным каналам связи в унифицированной системе приема, хранения и первичной обработки налоговых деклараций и

Подпись лица, получившего доверенность _____
(подпись) (Фамилия И.О.)

Подпись лица, выдавшего доверенность _____
(подпись) (Фамилия И.О.)

УДОСТОВЕРЯЮ

(Должность руководителя, название
организации) (подпись) (Фамилия И.О.)

М.П.

"__" _____ 200_ г.