СОГЛАШЕНИЕ № 78/01

о порядке представления органами ЗАГС Удмуртской Республики сведений о государственной регистрации рождения и смерти в налоговые органы Удмуртской Республики в электронном виде с использованием средств криптографической защиты информации

г. Ижевск «02» мая 2007

Управление Федеральной налоговой службы по Удмуртской Республике (далее – Управление), в лице и.о. руководителя Управления А.А. Лабзина, действующего на основании Положения об Управлении, утвержденного 14.12.2004 и Комитет по делам записи актов гражданского состояния при Правительстве Удмуртской Республики (далее – Комитет ЗАГС), в лице председателя Л.В. Лукинской, действующего на основании Положения о Комитете по делам ЗАГС и Закона Удмуртской Республики от 20.03.2007 г. № 8-РЗ «О наделении органов местного самоуправления в Удмуртской Республике государственными полномочиями на государственную регистрацию актов гражданского состояния», заключили настоящее Соглашение о порядке представления органами ЗАГС Удмуртской Республики сведений о государственной регистрации рождения и смерти в налоговые органы Удмуртской Республики в электронном виде с использованием средств криптографической защиты информации (далее – Соглашение) о нижеследующем

1. Общие положения

1.1. Настоящее соглашение определяет порядок и условия обмена информацией в электронном виде с использованием средств криптографической защиты информации (средств шифрования и электронной цифровой подписи (далее - ЭЦП)), использования, признания ЭЦП электронных документов (далее – ЭД) и защиты информации при обмене ЭД между налоговыми органами Удмуртской Республики (далее – налоговые органы) и органами ЗАГС Удмуртской Республики (далее – органы ЗАГС).

1.2. При обмене информацией налоговые органы и органы ЗАГС руководствуются: Налоговым кодексом РФ, Федеральным законом от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния», Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», приказом ФНС России от 12.04.2006 № САЭ-3-13/224@ «Об утверждении форматов файлов информации, представляемой в налоговые органы от органов, учреждений и организаций, перечисленных в пунктах 1, 2, 3, 8 статьи 85 части первой Налогового кодекса Российской Федерации» и другими нормативно-правовыми актами.

1.3. Налоговые органы и органы ЗАГС осуществляют обмен документированной информацией в электронном виде (электронными документами) в соответствии с Регламентом обмена информацией в электронном виде между налоговыми органами Удмуртской Республики и органами ЗАГС Удмуртской Республики (далее – Регламент обмена, Приложение № 1).

1.4. При обмене ЭД налоговые органы и органы ЗАГС руководствуются Инструкцией по защите информации при обмене электронными документами (далее – Инструкция по защите), (Приложение № 2).

2. Обеспечение электронного документооборота

2.1. В соответствии со статьей 19 Федерального закона от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» налоговые органы и органы ЗАГС на основании данного Соглашения, признают ЭЦП в ЭД равнозначной собственноручной подписи уполномоченных должностных лиц налоговых органов и органов ЗАГС в документе на бумажном носителе, заверенном печатью.

2.2. Налоговые органы и органы ЗАГС используют в качестве органа криптографической защиты информации – Удостоверяющего центра (УЦ) стороннюю организацию.

2.3. Удостоверяющим центром при обмене ЭД налоговые органы и органы ЗАГС признают ООО научно-производственное предприятие «Ижинформпроект», имеющее необходимые лицензии на право работы в области использования средств криптографической защиты информации (далее – СКЗИ).

2.4. Налоговые органы и органы ЗАГС признают УЦ координирующим органом криптографической защиты и используют его указания по обеспечению работы средств криптографической защиты информации, передаче ключей шифрования, ЭЦП открытых и закрытых, сертификатов ключей шифрования и ЭЦП.

3. Условия обмена электронными документами и основания его прекращения

3.1. Управление контролирует использование налоговыми органами Удмуртской Республики комплектов программно-аппаратных средств защиты информации, в том числе СКЗИ, соблюдение технической документации и инструкций пользователей СКЗИ.

3.2. Комитет ЗАГС организует использование органами ЗАГС комплектов программно-аппаратных средств защиты информации, в том числе СКЗИ, соблюдение технической документации и инструкций пользователей СКЗИ.

3.3. Налоговые органы и органы ЗАГС назначают работников - ответственных лиц за осуществление обмена ЭД, в том числе должностных лиц, наделенных правом подписи ЭД (назначаются работники, обладающие правом подписи указанных документов на бумажных носителях).

3.4. Непосредственную эксплуатацию АРМ ЭД, СКЗИ (в том числе в составе АРМ ЭД) организуют и обеспечивают уполномоченные лица налоговых органов и органов ЗАГС.

3.5. Основанием для прекращения (приостановления) обмена ЭД является:

3.5.1. Нарушение требований к обмену ЭД и защите информации при обмене ЭД, предусмотренные нормативными правовыми актами Российской Федерации, регулирующими отношения в сфере информатизации и защиты информации с ограниченным доступом.

3.5.2. Заявление одного из налоговых органов или органов ЗАГС о приостановлении обмена ЭД, направленное в письменной форме не позднее, чем за пять рабочих дней до даты начала приостановления обмена ЭД, указанной в заявлении.

3.5.3. Компрометация ключевой информации одного из налоговых органов или органов ЗАГС.

3.6. Порядок действий при компрометации ключей шифрования и/или закрытых ключей ЭЦП определяется Инструкцией по защите.

3.7. Восстановление обмена производится в соответствии с Инструкцией по защите.

4. Использование средств криптографической защиты информации

4.1. Для обеспечения конфиденциальности и подлинности (подтверждения целостности и авторства) ЭД налоговые органы и органы ЗАГС используют сертифицированные в установленном порядке СКЗИ, обеспечивающие в соответствии с требованиями ФСБ России безопасность конфиденциальной информации, не составляющей государственную тайну. Выбор конкретных видов СКЗИ осуществляется с учетом их совместимости.

4.2. Налоговые органы и органы ЗАГС признают стойкость, используемых СКЗИ достаточной для обеспечения конфиденциальности ЭД и подтверждения подлинности электронной цифровой подписи ЭД при условии соблюдения Инструкции по защите, технической и эксплутационной документации на СКЗИ.

4.3. Управление ключевой системой, используемой при обмене ЭД, осуществляется УЦ.

4.4. УЦ осуществляет деятельность по изготовлению сертификатов ключей подписей уполномоченных лиц налоговых органов и органов ЗАГС, регистрации владельцев сертификатов ключей подписи, управлению сертификатами ключей подписи, а также иные виды деятельности в соответствии с Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

4.5. Налоговые органы и органы ЗАГС своевременно предоставляют в УЦ в установленном порядке информацию, необходимую для изготовления и учета сертификатов ключей ЭЦП.

5. Права и обязанности

5.1. При обмене ЭД налоговые органы и органы ЗАГС вправе:

5.1.1. Отказать в приеме ЭД с указанием причины отказа.

5.1.2. Прекратить обмен ЭД при наличии оснований, предусмотренных п. 3.5 Соглашения.

5.1.3. Запросить, с указанием оснований, заверенные копии ЭД на бумажном носителе.

5.2. При обмене ЭД налоговые органы и органы ЗАГС обязаны:

5.2.1. Соблюдать требования Инструкции по защите.

5.2.2. Вести архивы входящих и исходящих ЭД в соответствии со следующими требованиями:

входящие ЭД, прошедшие проверку подлинности ЭЦП, хранятся совместно с сертификатами ключей подписи, используемыми для подтверждения их подлинности, и служебными уведомлениями о получении ЭД;

все исходящие ЭД хранятся со служебными уведомлениями о получении ЭД, формируемыми принимающей Стороной;

сроки хранения ЭД должны соответствовать срокам хранения, установленным для документов на бумажных носителях.

5.2.3. Обеспечить условия использования, хранения закрытых ключей электронной цифровой подписи и ключей шифрования в соответствии с требованиями Инструкции по защите.

5.2.4. Осуществлять контроль полученных ЭД и сообщать об обнаруженных ошибках.

5.2.5. Проводить мероприятия по приостановке действия или отзыву сертификатов ключей подписи уполномоченных лиц.

5.2.6. Информировать УЦ и участников электронного документооборота о фактах компрометации ключей электронной цифровой подписи и/или ключей шифрования.

5.2.7. Информировать участников электронного документооборота обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену ЭД.

6. Обязательства сторон

6.1. Комитет по делам ЗАГС обязуется довести до органов ЗАГС новый порядок передачи сведений о государственной регистрации рождения и смерти граждан в налоговые органы (настоящее Соглашение).

6.2. Персональную ответственность за полноту, достоверность и своевременность передачи сведений несут руководители органов ЗАГС Удмуртской Республики.

6.3. Управление обязуется довести до налоговых органов Удмуртской Республики настоящее Соглашение.

6.4. Налоговые органы Удмуртской Республики обеспечивают прием сведений о государственной регистрации рождения и смерти граждан, представленных органами ЗАГС.

7. Порядок разрешения разногласий

7.1. Споры и разногласия, возникающие в связи с обменом ЭД, разрешаются в соответствии законодательством Российской Федерации.

8. Срок действия Соглашения и порядок его изменения

8.1. Настоящее Соглашение заключено на неограниченный срок и вступает в силу со дня его подписания Сторонами.

8.2. Все изменения и дополнения к настоящему Соглашению оформляются дополнительными соглашениями, подписанными обеими Сторонами.

И. о. руководителя Управления Федеральной налоговой службы по Удмуртской Республике	Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики
_____ А.А. Лабзин	_____ Л.В. Лукинская

Приложение 1
к Соглашению
о порядке представления органами ЗАГС Удмуртской Республики
сведений о государственной регистрации рождения и смерти
в налоговые органы Удмуртской Республики в электронном виде с
использованием средств криптографической защиты информации

Регламент обмена информацией в электронном виде между налоговыми органами Удмуртской Республики и органами ЗАГС Удмуртской Республики

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок подготовки и оформления электронных документов, предназначенных для обмена между налоговыми органами Удмуртской Республики и органами ЗАГС Удмуртской Республики .

1.2. При взаимодействии налоговые органы Удмуртской Республики и органы ЗАГС Удмуртской Республики обеспечивают передачу и прием информации в электронном виде.

2. Организационная структура

2.1. Прием и отправка электронных документов осуществляется ответственными лицами налоговых органов и органов ЗАГС с использованием СКЗИ.

2.2. Формирование ЭЦП для ЭД производится уполномоченными лицами налоговых органов и органов ЗАГС.

2.3. Проверка подлинности ЭЦП ЭД производится уполномоченными лицами налоговых органов и органов ЗАГС.

3. Структура и формат файлов

3.1. Настоящий Регламент устанавливает порядок оформления документов отправляемых/принимаемых в рамках Соглашения.

3.2. Органы ЗАГС Удмуртской Республики направляют ЭД в следующих форматах и структурах:

3.2.1. Сведения о регистрации актов рождения и смерти физических лиц – в формате txt.

3.2.2. Сопроводительный лист приема/передачи информации (Приложение № 1 к настоящему Регламенту обмена) -

в формате MS Word (Office XP, 2003). Архивирование и сжатие данных осуществляется с использованием архиватора WinRar.

3.3. Налоговые органы направляют ЭД в следующих форматах и структурах:

3.3.1. Протокол приема файла сведений от текущей даты – в формате txt. Архивирование и сжатие данных осуществляется с использованием архиватора WinRar.

4. Порядок оформления документов

4.1. Органы ЗАГС:

4.1.1. Формируют файлы выгрузки сведений по актам гражданского состояния.

4.1.2. Исполнителем готовится Сопроводительный лист приема/передачи информации и его электронный образ. Ответственность за соответствие содержания документа на бумажной основе его электронному образу возлагается на исполнителя.

4.1.3. Сопроводительный лист приема/передачи информации подписывается лицом органа ЗАГС.

4.1.4. Файлы выгрузки и электронный образ Сопроводительного листа приема/передачи информации подписываются ЭЦП ответственного лица органа ЗАГС.

4.2. После подписания и формирования ЭЦП внесение изменений в документ и его электронный образ не допускается.

4.3. Налоговые органы:

4.3.1. Принимают файлы – сведения по актам гражданского состояния. Формируют отметку о поступлении сведений.

4.3.2. Производят загрузку сведений в Систему ЭОД. По результатам загрузки формируется Протокол приема файла сведений от текущей даты.

4.3.3. Электронный образ Протокола приема файла сведений от текущей даты подписывается ЭЦП ответственного лица налогового органа и отправляется не позднее следующего рабочего дня в органы ЗАГС.

5. Порядок электронного документооборота

5.1. Налоговые органы и органы ЗАГС при осуществлении электронного документооборота выполняют следующие действия при отправке ЭД:

средствами электронной почты формируется почтовое сообщение, сформированное почтовое сообщение направляется адресату по каналам связи (по электронной почте) с использованием средств криптографической защиты информации.

5.2. Достоверность сведений подтверждается электронной цифровой подписью. В случае отсутствия возможности применения электронной цифровой подписи, отправитель должен направить адресату подписанное уполномоченным лицом сопроводительное письмо на бумажном носителе.

5.3. Налоговые органы и органы ЗАГС при осуществлении электронного документооборота выполняют следующие действия при получении ЭД:

проводится контроль достоверности полученных сведений (проверка верности электронной цифровой подписи). При положительном результате проверки ЭЦП проводится дальнейшая работа с представленными сведениями. В случае получения недостоверных данных необходимо запросить подтверждение от отправителя о представленных сведениях, в том числе с повтором представления указанной информации.

в случае отрицательного результата при проверке подлинности ЭЦП ЭД налоговые органы и органы ЗАГС информируют друг друга, производится анализ причин неверности ЭЦП после чего направляют ЭД повторно.

5.4. Принятой считается только информация, прошедшая ФЛК – в Протоколе приема файла сведений отсутствуют ошибки приема сведений.

5.5. Если вся представленная информация не прошла ФЛК (количество документов, не прошедших ФЛК, совпадает с количеством заявленных документов), прием сведений не производится.

5.6. Все сведения не принятые налоговыми органами подлежат повторной отправке, в описанном выше порядке.

5.7. В процессе передачи и приема сведений должны быть обеспечены меры по предотвращению утечки информации.

5.8. Все полученные в процессе электронного документооборота сообщения электронной почты в обязательном порядке должны проходить антивирусную проверку.

5.9. Прием и обработка ЭД осуществляется с использованием программно-аппаратных средств принимающей стороны.

6. Виды документов, предоставляемые при взаимодействии налоговых органов и органов ЗАГС

6.1. Выгрузка данных по актам гражданского состояния в виде фалов txt.

6.2. Сопроводительный лист приема/передачи информации в виде файлов MS Word, MS Excel.

6.3. Протокол приема файла сведений от органов ЗАГС в виде файлов txt.

6.4.

7. Схема защищенного электронного документооборота с использованием электронных почтовых ящиков

Наименование налогового обмена	Электронный почтовый ящик	Наименование органа ЗАГС	Электронный почтовый ящик
Межрайонная ИФНС России № 2 по Удмуртской Республике	i1837zd@m37.r18.nalog.ru	Управление ЗАГС администрации г. Глазова	ardasheva@glazov.net
		Отдел ЗАГС администрации МО «Глазовский район»	maija@glazov.net
		Отдел ЗАГС администрации МО «Балезининский район»	ZAGS@glazov.net
		Отдел ЗАГС администрации МО «Юкаменский район»	zaguuu@udmnet.ru
		Отдел ЗАГС администрации МО «Ярский район»	Yaradmin@udmnet.ru
Межрайонная ИФНС России № 3 по Удмуртской Республике	i1828zd@m28.r18.nalog.ru	Управление ЗАГС администрации г. Воткинска	zagsgorvtk@udm.net
		Отдел ЗАГС администрации МО «Воткинский район»	rai_zags@vi-mail.ru
		Отдел ЗАГС администрации МО «Шарканский район»	sharkrono@udm.net
Межрайонная ИФНС России № 4 по Удмуртской Республике	i1809zd@m09.r18.nalog.ru	Отдел ЗАГС администрации МО «Игринский район»	igra-zags@udm.net
		Отдел ЗАГС администрации МО «Кезский район»	kezzags@udm.net
		Отдел ЗАГС администрации МО «Красногорский район»	krzags@udm.net
		Отдел ЗАГС администрации МО «Дебесский район»	debzags@udmnet.ru

		Отдел ЗАГС администрации МО «Як-Бодьинский район»	ozags@udm.net
Межрайонная ИФНС России № 5 по Удмуртской Республике	i1838zd@m38.r18.nalog.ru	Управление ЗАГС г. Сарапул	sar-zags@udm.net
		Отдел ЗАГС администрации МО «Сарапульский район»	sarzags@udm.net
		Отдел ЗАГС администрации МО «Камбарский район»	kama_admin@udmnet.ru
		Отдел ЗАГС администрации МО «Каракулинский район»	karak-zags@udm.net
		Отдел ЗАГС администрации МО «Киясовский район»	kijs-zags@udmnet.ru
Межрайонная ИФНС России № 6 по Удмуртской Республике	i1821zd@m21.r18.nalog.ru	Отдел ЗАГС администрации МО «Увинский район»	zagsuva@udm.net
		Отдел ЗАГС администрации МО «Вавожский район»	wawozhzags@udmnet.ru
		Отдел ЗАГС администрации МО «Селтинский район»	seltyzags@udm.net
		Отдел ЗАГС администрации МО «Сюмсинский район»	zags-sumsi@udmnet.ru
		Отдел ЗАГС администрации МО «Малопургинский район»	purga-zags@udm.net
Межрайонная ИФНС России № 7 по Удмуртской Республике	i1839zd@m39.r18.nalog.ru	Отдел ЗАГС администрации г. Можги	mozzags@udmnet.ru
		Отдел ЗАГС администрации МО «Можгинский район»	mozraizags@udm.net
		Отдел ЗАГС администрации МО «Алнашский район»	alnzags@udm.net
		Отдел ЗАГС администрации МО «Граховский район»	grahovzags@udm.net
		Отдел ЗАГС администрации МО «Кизнерский район»	kizzags@udm.net
Межрайонная ИФНС России № 8 по Удмуртской Республике	i1840zd@m40.r18.nalog.ru	Устиновский отдел ЗАГС Управления ЗАГС администрации г. Ижевска	ustzags@mail.izh.ru
Межрайонная ИФНС России № 9 по Удмуртской Республике	i1841zd@m41.r18.nalog.ru	Управление ЗАГС администрации г. Ижевска	uzags@mail.izh.ru
Межрайонная ИФНС России № 9 по Удмуртской Республике	i1841zd@m41.r18.nalog.ru	Управление ЗАГС администрации МО «Завьяловский район»	zags08@udm.net
ИФНС России по Ленинскому району г. Ижевска	i1832zd@m32.r18.nalog.ru	Ленинский отдел ЗАГС Управления ЗАГС администрации г. Ижевска	lenzags@mail.izh.ru

Приложение 1
к Регламенту обмена информацией в электронном виде
между налоговыми органами Удмуртской Республики
и органами ЗАГС Удмуртской Республики

Сопроводительный лист приема/передачи информации

Реестр № _____ от _____
(номер реестра с начала года) (дата составления реестра)

в _____
(наименование налогового органа)

Отправитель: _____
(наименование органа ЗАГС)

Представлены:

№ п/п	Наименование файла	Статистическая информация файла (дата создания, размер)	Количество представленных документов*	Количество документов, прошедших ФЛК**
1	2	3	4	5

Примечание:
* - указывается отправителем для сведения и контролируется при ФЛК (количество записей по физическим лицам);
** - указывается получателем по результатам ФЛК.

Ответственное лицо органа ЗАГС _____ / _____
(подпись) (ФИО)

Дата представления в налоговый орган: _____

Дата принятия в налоговом органе: _____

Ответственное лицо получателя _____ / _____
(подпись) (ФИО)

Приложение 2
к Соглашению
о порядке представления органами ЗАГС Удмуртской Республики
сведений о государственной регистрации рождения и смерти
в налоговые органы Удмуртской Республики в электронном виде с
использованием средств криптографической защиты информации

Инструкция
по защите информации при обмене электронными документами

1. Общие положения

1.1. Настоящая Инструкция по защите информации при обмене электронными документами (далее – Инструкция) определяет организационно-технические мероприятия по защите информации при обмене электронными документами между налоговыми органами Удмуртской Республики (далее – налоговые органы) и органами ЗАГС Удмуртской Республики (далее – органы ЗАГС) (далее – Стороны).

1.2. Организационно-технические мероприятия по защите информации разработаны с учетом требований Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13 июня 2001 № 152 (далее – Инструкция № 152) и обязательны к выполнению обеими Сторонами при осуществлении обмена электронными документами (далее – ЭД), заверенными электронной цифровой подписью (далее – ЭЦП), эксплуатации средств защиты информации, в том числе средств ЭЦП, а также обращении ключевой информации, используемой для криптографической защиты ЭД.

1.3. Организационно-технические мероприятия по обеспечению защиты информации при обмене ЭД обеспечивают:

конфиденциальность ЭД;

подлинность ЭД - подтверждение авторства и целостности ЭД;

разграничение и контроль доступа к средствам обмена ЭД;

сохранность в тайне содержания закрытых ключей ЭЦП и иных ключевых документов.

1.4. Настоящая Инструкция обязательна для выполнения всеми работниками Сторон, осуществляющими подготовку, обработку, отправку/получение, хранение и учет ЭД заверенных ЭЦП.

2. Управление ключевой системой

2.1. Ключевая система обмена ЭД состоит из ключей шифрования, ключей аутентификации, и ключей подписи уполномоченных лиц и соответствующих сертификатов.

2.2. Для владельцев сертификатов ключей подписи изготавливаются - рабочие комплекты ключевых документов, и его копии – резервные комплекты на случай выхода ключевых носителей из строя.

2.2. Стороны самостоятельно формируют заявки на изготовление ключей шифрования и ЭЦП.

2.3. Рабочий и резервный комплекты ключей, вырабатываются Удостоверяющим центром.

2.4. Администраторы безопасности Сторон обеспечивают контроль оформления заявлений на изготовление сертификатов ключей подписи.

2.5. Заявки на изготовление ключей шифрования и ЭЦП, оформленные и подписанные в установленном порядке, передаются Администраторами безопасности Сторон в Удостоверяющий центр (далее – УЦ).

2.6. УЦ в срок, не превышающий трех рабочих дней, изготавливает сертификаты ключей шифрования и подписи.

2.7. УЦ, изготовивший сертификаты ключей шифрования и ЭЦП, несет ответственность за соответствие сведений, указанных в сертификате ключа, сведениям, указанным в заявке на изготовление сертификата ключа и в предоставленных удостоверяющих документах.

2.8. Владельцы сертификатов ключей шифрования и ЭЦП Сторон или иные лица по доверенности получают изготовленные ключи в УЦ. После регистрации изготовленные сертификаты доводятся до пользователей сертификатов ключей.

2.9. УЦ обеспечивает формирование реестров изготовленных сертификатов ключей подписи и списков отозванных сертификатов. Администраторы безопасности Сторон обеспечивают своевременную выборку изготовленных списков отозванных сертификатов, их регистрацию и последующее доведение до пользователей сертификатов ключей шифрования и ЭЦП.

2.10. Администраторы безопасности Сторон обеспечивают порядок хранения, передачи, использования, уничтожения, а также учета ключевой информации и ее носителей в соответствии с требованиями Инструкция № 152, а также технической и эксплутационной документации на используемые средства криптографической защиты информации (далее – СКЗИ).

2.11. Рабочий и резервный комплекты ключей шифрования и ЭЦП хранятся отдельно.

2.12. Рабочий и резервный комплекты ключей шифрования и ЭЦП должны храниться в запираемых на ключ и опечатываемых индивидуальных хранилищах (шкафах, сейфах). В случае хранения закрытых ключей ЭЦП в хранилищах, доступ к которым имеют иные лица, закрытые ключи ЭЦП хранятся (сдаются на хранение) в отдельных упаковках, опечатанных владельцем сертификата ключа подписи.

2.13. Операторы и Администраторы автоматизированного рабочего места ЭД (далее – АРМ ЭД), осуществляющие использование ключей шифрования и ЭЦП, несут персональную ответственность за безопасность доверенной им ключевой информации и обязаны обеспечивать ее сохранность, неразглашение и нераспространение. Указанным работникам доводятся под роспись соответствующие положения Инструкции № 152, а также технической и эксплутационной документации на СКЗИ.

2.14. Срок действия ключей шифрования и ЭЦП и соответствующих сертификатов - 1 год.

2.15. За две недели до окончания срока действия сертификата ключа подписи, его владелец обязан уведомить об этом Администраторов безопасности Сторон. УЦ проводится процедура изготовления новых комплектов ключей шифрования и ЭЦП.

2.16. По истечении установленного срока Администраторы безопасности Сторон проводят плановую смену ключей шифрования и ЭЦП. Выведенные из обращения ключи шифрования уничтожаются установленным образом.

2.17. Датой ввода в действие ключей шифрования и ЭЦП является дата выпуска сертификата ключа подписи.

2.18. Владельцы сертификатов ключей шифрования и подписи получают право использования соответствующих закрытых ключей шифрования и ЭЦП для заверения ЭД с момента регистрации сертификата Администратором безопасности Сторон, но не ранее даты, указанной в сертификате.

2.20. После окончания срока действия сертификата ключа подписи его владелец прекращает использование соответствующих закрытых ключей, в трехдневный срок сдает их Администратору безопасности Сторон, который в установленном порядке производит их уничтожение.

2.21. Администраторы безопасности Сторон организуют и обеспечивают хранение сертификатов ключей подписи в течение срока хранения ЭД, заверенных соответствующей ЭЦП.

2.22. Администраторы безопасности Сторон организуют и контролируют порядок обращения с ключами шифрования и ключами ЭЦП Операторами и Администратором АРМ ЭД, а также владельцами сертификатов ключей подписи.

3. Компрометация ключевой информации

3.1. Под компрометацией (раскрытием) ключей шифрования или ключей ЭЦП понимаются: утрата носителей ключевой информации, утрата их с последующим обнаружением, хищение, несанкционированное копирование, передача их по линии связи в открытом виде, любые другие виды разглашения ключевой информации, а также случаи, когда нельзя достоверно установить, что произошло с ключевой информацией и/или ее носителем (в том числе при выходе носителя из строя и отсутствии возможности опровергнуть наличие несанкционированных действий злоумышленника).

3.2. Действия персонала при компрометации ключей ЭЦП:

3.2.1. При подозрении о компрометации рабочего комплекта закрытых ключей ЭЦП владелец соответствующего сертификата ключа немедленно прекращает использование соответствующего закрытого ключа ЭЦП и незамедлительно сообщает об этом Администратору безопасности.

3.2.2. При обнаружении обстоятельств, свидетельствующих о факте компрометации, Администратор безопасности соответствующей Стороны незамедлительно извещает о компрометации другую Сторону и УЦ с их последующим письменным уведомлением не позднее двух следующих рабочих дней.

3.2.3. УЦ в порядке, определенном регламентом УЦ заносит соответствующий сертификат ключа подписи в список отозванных сертификатов.

3.2.4. Администратор безопасности Стороны, получившей извещение о компрометации рабочего комплекта закрытых ключей ЭЦП, информирует пользователей сертификатов соответствующего ключа подписи и совместно с ними обеспечивает приостановку обработки ЭД, полученных после извещения и заверенных ЭЦП, соответствующей скомпрометированному ключу ЭЦП.

3.2.5. После подтверждения факта компрометации комплекта закрытых ключей ЭЦП осуществляется формирование нового комплекта ключей ЭЦП, и инициируются процедура изготовления и регистрации сертификата ключа подписи.

3.2.6. В зависимости от обстоятельств компрометации рабочего комплекта закрытых ключей ЭЦП, руководителем соответствующей Стороны может быть назначено служебное расследование с включением в комиссию представителей УЦ.

3.3. Действия персонала при компрометации ключей шифрования:

3.3.1. При подозрении о компрометации рабочего комплекта ключей шифрования Оператор или Администратор АРМ ЭД, обнаруживший факт компрометации, обязан немедленно приостановить обмен ЭД и незамедлительно сообщить об этом Администратору безопасности.

3.3.2. При обнаружении обстоятельств, свидетельствующих о факте компрометации, Администратор безопасности незамедлительно извещает о компрометации другую Сторону и УЦ.

3.4. Для восстановления обмена ЭД в случае выхода из строя рабочих ключевых носителей Администраторы безопасности Сторон обеспечивают переход на работу с резервными ключевыми носителями.

4. Защита информации при обработке электронных документов

4.1. Формирование, подготовка, обработка, хранение ЭД, заверение ЭД ЭЦП, проверка подлинности ЭЦП ЭД производятся на специально подготовленных рабочих местах уполномоченных работников Сторон, оборудованных необходимыми программно-техническими средствами, в том числе средствами ЭЦП и средствами защиты информации от несанкционированного доступа, в соответствии с технологиями, принятыми Сторонами.

4.2. Установленные на соответствующих рабочих местах средства ЭЦП и/или используемые в комплекте с ними СКЗИ обеспечивают в соответствии с требованиями ФСБ России безопасность конфиденциальной информации, не составляющей государственную тайну.

4.3. Администратор безопасности производит контроль проведения профилактических и ремонтных работ рабочих мест с целью выявления и предупреждения неконтролируемого изменения их аппаратной части и/или программного обеспечения.

4.4. Доступ к данным рабочим местам ограничивается соответствующими уполномоченными работниками Сторон и Администраторами безопасности.

5. Защита информации при приеме/передаче электронных документов

5.1. В соответствии с требованиями ФСБ России безопасность информации не составляющей государственную тайну при ее передаче по открытым каналам связи обеспечивается использованием сертифицированных в установленном порядке СКЗИ.

5.2. В налоговых органах защита информации, передаваемой по каналам связи, обеспечивается использованием сертифицированного СКЗИ – КриптоПро CSP или совместимого с ним по форматам сертификатов и криптографических сообщений.

5.3. В органах ЗАГС защита информации, передаваемой по каналам связи, обеспечивается использованием сертифицированного СКЗИ – КриптоПро CSP или совместимого с ним по форматам сертификатов и криптографических сообщений.

5.4. Размещение, установка, подключение, поэкземплярный учет и последующая эксплуатация указанных СКЗИ выполняется в соответствии с требованиями Инструкции № 152, а также технической и эксплутационной документации на них.

5.5. Прием/передача ЭД, проверка подлинности ЭЦП входящих ЭД и их предварительная обработка и учет, последующая обработка и учет исходящих ЭД, заверение их ЭЦП осуществляется на специально подготовленном рабочем месте – АРМ ЭД, оборудованном необходимыми программно-аппаратными средствами, в том числе средствами защиты информации и средствами телекоммуникаций, и имеющего подключение к необходимым сетям связи.

5.6. Для выполнения указанных выше функций Сторонами назначаются Операторы АРМ ЭД, обеспечивающие непосредственную эксплуатацию средств АРМ ЭД.

5.7. Требования к средствам защиты информации АРМ ЭД, к учету и контролю его аппаратной части и программного обеспечения, допуску к нему сотрудников Сторон аналогичны требованиям для рабочих мест сотрудников Сторон, уполномоченных правом ЭЦП.

5.8. Доступ посторонних лиц в помещения, в которых размещены указанные в настоящей статье СКЗИ, средства телекоммуникаций, а также средства АРМ ЭД должен быть ограничен. Двери данных помещений оборудуются замками, гарантирующими надежную защиту в нерабочее время.

6. Контроль за выполнением требований по защите информации

6.1. Контроль за соблюдением требований по защите информации возлагается на отдел информационной безопасности Управления и администраторов безопасности органов ЗАГС.