СОГЛАШЕНИЕ № 01-21/4 / 36-Р

о порядке представления органами ЗАГС Удмуртской Республики сведений о государственной регистрации рождения в Государственное учреждение-региональное отделение Фонда социального страхования Российской Федерации по Удмуртской Республике в электронном виде с использованием средств криптографической защиты информации

г.Ижевск 18.07. 2014 г.

Комитет по делам записи актов гражданского состояния при Правительстве Удмуртской Республики, именуемый в дальнейшем Комитет по делам ЗАГС, в лице председателя Поповой Людмилы Александровны, действующей на основании Положения, утвержденного Постановлением Правительства Удмуртской Республики от 15 мая 2006 г. №48, и Закона Удмуртской Республики от 20 марта 2007 г. №8-РЗ «О наделении органов местного самоуправления в Удмуртской Республике государственными полномочиями на государственную регистрацию актов гражданского состояния» с одной стороны, и Государственное учреждение - региональное отделение Фонда социального страхования Российской Федерации по Удмуртской Республике, именуемое в дальнейшем Региональное отделение, в лице Управляющего Лобановой Надежды Александровны, действующей на основании Положения, утвержденного приказом Фонда социального страхования Российской Федерации от 22.05.2002 г. №90 с другой стороны, в целях обеспечения эффективного взаимодействия по представлению сведений о государственной регистрации рождения граждан на территории Удмуртской Республики, руководствуясь положениями Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», Постановления Правительства Российской Федерации от 18.11.2013г. №1030 «Об утверждении Правил передачи органами записи актов гражданского состояния сведений о государственной регистрации рождения и смерти» заключили настоящее Соглашение о нижеследующем:

1.Общие положения

1.1. Настоящее Соглашение определяет порядок и условия предоставления органами записи актов гражданского состояния Удмуртской Республики (далее - органы ЗАГС) сведений о государственной регистрации рождения (далее – сведения о рождении) в Региональное отделение в электронном виде по телекоммуникационным каналам связи с использованием средств криптографической защиты информации (далее - СКЗИ) (средств шифрования и электронной подписи (далее - ЭП)), использования, признания ЭП электронных документов (далее - ЭД) и защиты информации при обмене ЭД).

1.2. При обмене информацией Региональное отделение и органы ЗАГС руководствуются: Гражданским кодексом Российской Федерации, Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федеральным законом от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», Федеральным законом от 29 декабря 2006 г. г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,

Постановлением Правительства Российской Федерации от 18 ноября 2013г. №1030 «Об утверждении Правил передачи органами записи актов гражданского состояния сведений о государственной регистрации рождения и смерти», технической документацией на используемые средства электронной подписи (шифровальных (криптографических) средств), другими нормативно-правовыми актами, а также настоящим Соглашением.

1.3. Региональное отделение и органы ЗАГС осуществляют обмен информацией в электронном виде (электронными документами) в соответствии с Регламентом обмена информацией в электронном виде между Региональным отделением и органами ЗАГС (Приложение №1).

1.4. Органы ЗАГС представляют сведения о государственной регистрации рождения граждан в электронном виде по телекоммуникационным каналам связи с использованием СКЗИ в Региональное отделение на адрес электронной почты zags-r@ro18.fss.ru в составе и форматах, определенных в Приложении №2 «Состав и форматы файлов обмена сведениями о государственной регистрации рождения граждан».

1.5. Региональное отделение и органы ЗАГС признают, что использование СКЗИ, которые реализуют шифрование и электронную подпись (далее — ЭП), достаточно для обеспечения конфиденциальности информационного взаимодействия Регионального отделения и органов ЗАГС, а также для подтверждения того что:

- электронный документ исходит от стороны, его передавшей (подтверждение авторства документа);
- электронный документ не претерпел изменений при информационном взаимодействии Регионального отделения и органов ЗАГС (подтверждение целостности и подлинности документа);
- электронный документ юридически эквивалентен документу на бумажном носителе.

1.6. При обмене ЭД Региональное отделение и органы ЗАГС руководствуются Инструкцией по защите информации при обмене электронными документами (Приложение №3).

1.7. В случае отсутствия возможности отправки по каналам связи, информация передается в виде списка на бумажном носителе или на магнитном носителе в опечатанном конверте посредством почтовой связи.

2.Обеспечение электронного документооборота

2.1. В соответствии со статьей 6 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи» Региональное отделение и органы ЗАГС на основании данного Соглашения, признают ЭП в ЭД равнозначной собственноручной подписи уполномоченных должностных лиц Регионального отделения и органов ЗАГС в документе на бумажном носителе, заверенном печатью.

2.2. Любой электронный документ, участвующий в электронном документообороте между Региональным отделением и органами ЗАГС, подписывается квалифицированной электронной подписью.

2.3. Региональное отделение и органы ЗАГС за свой счет приобретают, устанавливают и обеспечивают работоспособность необходимого программного обеспечения СКЗИ.

2.4. Региональное отделение и органы ЗАГС самостоятельно оплачивают средства связи и каналы связи, необходимые для обеспечения обмена ЭД.

3.Условия обмена электронными документами и основания его прекращения

3.1. Региональное отделение самостоятельно обеспечивает использование комплектов программно-аппаратных средств защиты информации, в том числе СКЗИ, соблюдение технической документации, инструкций пользователей СКЗИ и данного Соглашения.

3.2. Комитет по делам ЗАГС организует использование органами ЗАГС комплектов программно-аппаратных средств защиты информации, в том числе СКЗИ.

3.3. Региональное отделение 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 автоматизированного рабочего места ЭД, СКЗИ (в том числе в составе АРМ ЭД) организуют и обеспечивают уполномоченные лица Регионального отделения 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 Регионального отделения или одного из органов ЗАГС о приостановлении обмена ЭД, направленное в письменной форме не позднее, чем за тридцать календарных дней до даты начала приостановления обмена ЭД, указанной в заявлении. В случае поступления заявления от одного органа ЗАГС обмен прекращается только с этим органом ЗАГС.

3.5.3. Компрометация ключевой информации Регионального отделения или одного из органов ЗАГС.

При компрометации ключевой информации одного органа ЗАГС обмен прекращается только с этим органом ЗАГС.

3.6. Перед началом обмена Региональное отделение передает в органы ЗАГС сертификат открытого ключа одного из должностных лиц, ответственных за обмен сообщениями. Органы ЗАГС используют данный сертификат для шифрования передаваемой информации.

4. Использование средств криптографической защиты информации

4.1. Для обеспечения конфиденциальности и подлинности (подтверждения целостности и авторства) ЭД Региональное отделение и органы ЗАГС используют сертифицированные в установленном порядке СКЗИ, обеспечивающие безопасность конфиденциальной информации, не составляющей государственную тайну.

4.2. Региональное отделение и органы ЗАГС признают стойкость, используемых СКЗИ достаточной для обеспечения конфиденциальности ЭД и подтверждения подлинности электронной подписи ЭД при условии соблюдения требований нормативных документов по защите информации, технической и эксплуатационной документации на СКЗИ.

5. Права и обязанности

5.1.При обмене ЭД Региональное отделение и органы ЗАГС вправе:

5.1.1. Отказать в приеме ЭД с указанием причины отказа.

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

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

5.2.При обмене ЭД Региональное отделение и органы ЗАГС обязаны:

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

• входящие ЭД, прошедшие проверку подлинности ЭП, 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.

5.2.2. Обеспечить надлежащие условия использования, хранения ключей электронной подписи и средств электронной подписи в соответствии с требованиями законодательства.

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

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

5.2.5. Информировать удостоверяющий центр, выдающий электронную подпись, и участников электронного документооборота о фактах компрометации ключей электронной подписи.

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

5.3. Региональное отделение обязуется обеспечить прием, необходимую конфиденциальность, сохранность и установленный порядок использования полученной информации в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5.4. Комитет по делам ЗАГС обязуется довести до органов ЗАГС порядок передачи сведений о государственной регистрации рождения граждан в Региональное отделение.

5.5. Персональную ответственность за полноту, достоверность и своевременность передачи сведений несут руководители органов ЗАГС.

5.6. Комитет по делам ЗАГС при исполнении настоящего соглашения действует в рамках полномочий, определенных Законом Удмуртской Республики от 20 марта 2007 г. № 8-РЗ «О наделении органов местного самоуправления в Удмуртской Республике государственными полномочиями на государственную регистрацию актов гражданского состояния», Положением о Комитете по делам ЗАГС, утвержденным постановлением Правительства Удмуртской Республики от от 15 мая 2006 г. № 48.

6. Порядок разрешения разногласий

6.1.Споры и разногласия, вознкающие в связи с обменом ЭД, разрешаются в соответствии законодательством Российской Федерации.

6.2.Региональное отделение и органы ЗАГС обязуются принимать все возможные усилия для разрешения споров путем переговоров, направления претензий.

6.3.В случае невозможности разрешения конфликтной ситуации в рабочем порядке, спор подлежит рассмотрению в судебном порядке в соответствии с действующим законодательством.

7. Срок действия Соглашения и порядок его изменения

7.1.Настоящее Соглашение заключено на неограниченный срок и вступает в силу с момента подписания сторонами.

7.2.Все изменения и дополнения к настоящему Соглашению оформляются дополнительными соглашениями, подписанными Региональным отделением и Комитетом по делам ЗАГС.

7.3.В случае нарушения одной из сторон обязательств, предусмотренных настоящим Соглашением, другая сторона вправе в одностороннем порядке расторгнуть настоящее Соглашение, уведомив об этом в письменном виде другую сторону за 30 календарных дней до даты предполагаемого расторжения Соглашения.

7.4.Настоящее Соглашение составлено в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой Стороны.

7.5.К настоящему Соглашению прилагаются и являются его неотъемлемыми частями:

- Приложение №1 - Регламент обмена информацией в электронном виде между Региональным отделением и органами ЗАГС;
- Приложение №2 - Состав и форматы файлов обмена сведениями о государственной регистрации рождения граждан;
- Приложение №3 - Инструкция по защите информации при обмене электронными документами.

Управляющий Государственного учреждения - регионального отделения Фонда социального страхования Российской Федерации по Удмуртской Республике

_____ Н.А. Лобанова

М.П.

Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики

_____ Л.А. Попова

М.П.

Ответ – И.А. Столбова

Приложение №1
к Соглашению о порядке представления органами ЗАГС
Удмуртской Республики сведений о государственной регистрации
рождения в Государственное учреждение-региональное отделение
Фонда социального страхования Российской Федерации
по Удмуртской Республике в электронном виде с использованием
средств криптографической защиты информации
№ 01-21/4/36-ПО от «18» июля 2014 г.

Регламент обмена информацией в электронном виде между Региональным отделением и органами ЗАГС

Для осуществления обмена ЭД органы ЗАГС передают в Региональное отделение сведения о государственной регистрации рождения граждан в электронном виде. Региональное отделение направляет в органы ЗАГС протокол приема сведений.

Прием/передача сведений о государственной регистрации рождения граждан осуществляется ежедекадно не позднее **2, 12** и **22** числа каждого месяца.

Органы ЗАГС формируют файлы выгрузки сведений о государственной регистрации рождения граждан. Файлы выгрузки подписываются ЭП ответственного лица органа ЗАГС, шифруется на открытом ключе сотрудника Регионального отделения.

Органы ЗАГС средствами электронной почты формируют почтовое сообщение с вложением, содержащим подписанный ЭП ответственного лица архивный файл со сведениями о государственной регистрации рождения граждан, почтовое сообщение направляется Региональному отделению по каналам связи (по электронной почте).

Региональное отделение принимает файлы, проводит контроль достоверности полученных сведений (проверка подлинности ЭП). При положительном результате проверки проводится дальнейшая работа с полученными сведениями, оформляется протокол приема в электронном виде. Протокол подписывается ЭП ответственного лица Регионального отделения. Подписанный ЭП протокол направляется в орган ЗАГС электронной почтой.

Орган ЗАГС получает файл протокола приема информации, проверяет подлинность ЭП.

В случае отрицательного результата при проверке подлинности ЭП органы ЗАГС и Региональное отделение немедленно информируют друг друга о данном факте и проводят анализ причин неверности ЭП, после чего направляют ЭД повторно.

Все полученные в процессе электронного документооборота сообщения электронной почты в обязательном порядке проходят антивирусную проверку. Файлы, не прошедшие антивирусную проверку, к обработке не принимаются и немедленно сообщают друг другу о данном факте.

Управляющий Государственного учреждения - регионального отделения Фонда социального страхования Российской Федерации по Удмуртской Республике

_____ Н.А. Лобанова

м.п.

Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики

_____ Л.А. Попова

м.п.

Приложение № 2
к Соглашению о порядке представления органами ЗАГС
Удмуртской Республики сведений о государственной регистрации
рождения в Государственное учреждение-региональное отделение
Фонда социального страхования Российской Федерации
по Удмуртской Республике в электронном виде с использованием
средств криптографической защиты информации
№ 01-21/4/3670 от «18» июля 2014 г.

Состав и форматы файлов обмена сведениями о государственной регистрации рождения граждан

1. Передача сведений о государственной регистрации рождения граждан отделами ЗАГС означает направление персонифицированных данных в виде файла формата dbf (dBaseIII).

2. Для предоставления данных используется код ASCII, кодовая страница 866. Файл не должен содержать записей, помеченных как «удаленные».

3. Имя файла имеет вид r_RRMMGGN.dbf, где:

r – префикс, обозначающий, что передаются сведения о рождении;
RR — код района Удмуртской Республики,
MM — месяц,
GG — две последние цифры года,
N — порядковый номер файла, сформированного с начала месяца.

Классификатор кодов городов и районов Удмуртской Республики:

Код	Наименование города (района)	Код	Наименование города (района)
01	Первомайский и Октябрьский районы г. Ижевска	20	Каракулинский район
02	Устиновский и Индустриальный районы г. Ижевска	21	Кезский район
03	Ленинский район г. Ижевска	22	Кизнерский район
06	г. Воткинск	23	Киясовский район
07	г. Глазов	24	Красногорский район
08	г. Можга	25	Малопургинский район
09	г. Сарапул	26	Можгинский район
10	Алнашский район	27	Сарапульский район
11	Балезинский район	28	Селтинский район
12	Вавожский район	29	Сюмсинский район
13	Воткинский район	30	Увинский район
14	Глазовский район	31	Шарканский район
15	Граховский район	32	Юкаменский район

Код	Наименование города (района)	Код	Наименование города (района)
16	Дебесский район	33	Як-Бодьинский район
17	Завьяловский район	34	Ярский район
18	Игринский район		
19	Камбарский район		

Структура файлов:

№	Имя поля	Примечания
1	FAMB	Фамилия ребенка
2	NAMB	Имя ребенка
3	OTB	Отчество ребенка
4	POL	Пол
5	NAKT	Номер актовой записи
6	DAKT	Дата актовой записи
7	DATAB	Дата рождения ребенка
8	DATAB_TEXT	Примерная дата рождения ребенка
9	MRB_STA	Ребенок: месторождение - код государства
10	MRB_OBL	Ребенок: месторождение - код области
11	MRB_RAY	Ребенок: месторождение - код района
12	MRB_NPR	Ребенок: месторождение - населенный пункт районного подчинения
13	MRB_SOK	Ребенок: месторождение – код сельского округа
14	MRB_TEXT	Текст адреса места рождения ребенка
15	FAMM	Фамилия матери
16	NAMM	Имя матери
17	OTM	Отчество матери
18	FAMF	Фамилия отца
19	NAMF	Имя отца
20	OTF	Отчество отца
21	PRIM	Иные сведения и служебные отметки
22	ZAGSRAY	Номер ЗАГСа

Файлы передаются в архивном виде:

- архивирование и сжатие файлов осуществляется в формате ZIP;
- имя архива совпадает с именем соответствующего файла.

Результаты приема Региональным отделением сведений о государственной регистрации рождения граждан от органов ЗАГС оформляются протоколом приема файла в формате txt. Имя файла имеет вид: RRMMGGN.txt, где:

RR — код района Удмуртской Республики,

MM — месяц,

GG — год,

N — порядковый номер файла, сформированного в текущем месяце по району/городу.

Файл содержит следующие реквизиты: имя принятого файла, размер принятого файла, количество представленных документов, дата обработки файла. Каждый реквизит записывается в отдельной строке.

Управляющий Государственного учреждения - регионального отделения Фонда социального страхования Российской Федерации по Удмуртской Республике

_____ Н.А. Лобанова

М.П.

Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики

_____ Л.А. Попова

М.П.

Приложение № 3
к Соглашению о порядке представления органами ЗАГС
Удмуртской Республики сведений о государственной регистрации
рождения в Государственное учреждение-региональное отделение
Фонда социального страхования Российской Федерации
по Удмуртской Республике в электронном виде с использованием
средств криптографической защиты информации
№ 01-11/4/36-ро от «18» июня 2014 г.

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 Государственным учреждением - региональным отделением Фонда социального страхования Российской Федерации по Удмуртской Республи (далее – Региональное отделение) 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 февраля 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 подписью (далее - ЭП), эксплуатации средств защиты информации, в том числе средств ЭП, 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 ЭП и иных ключевых документов.

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

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.

2.3. Стороны самостоятельно формируют заявки на изготовление ключей шифрования и ЭП.

2.4. Рабочий и резервный комплекты ключей, вырабатываются Удостоверяющим центром (далее - УЦ).

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

2.6. Заявки на изготовление ключей шифрования и ЭП, оформленные и подписанные в установленном порядке, передаются Администраторами безопасности Сторон в Удостоверяющий центр.

2.7. УЦ в срок, не превышающий трех рабочих дней, изготавливает сертификаты ключей ЭП.

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

2.9. Владельцы сертификатов ключей ЭП Сторон или иные лица по доверенности получают изготовленные ключи в УЦ. После регистрации изготовленные сертификаты доводятся до пользователей сертификатов ключей.

2.10. 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 ЭП.

2.11. 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 эксплуатационной документации на используемые средства электронной подписи (шифровальных (криптографических) средств).

2.12. Рабочий и резервный комплекты ключей ЭП хранятся отдельно.

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

2.14. Операторы и Администраторы автоматизированного рабочего места ЭД (далее — АРМ ЭД), осуществляющие использование ключей ЭП, 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 эксплуатационной документации на средства электронной подписи (шифровальных (криптографических) средств).

2.15. Срок действия ключей ЭП и соответствующих сертификатов -1 год.

2.16. 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 ЭП.

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

2.18. Датой ввода в действие ключей ЭП является дата выпуска сертификата ключа подписи.

2.19. Владельцы сертификатов ключей шифрования и подписи получают право использования соответствующих закрытых ключей шифрования и ЭП 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 подписного владелец прекращает использование соответствующих ключей ЭП, 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 ЭП.

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

3. Компрометация ключевой информации

3.1. Под компрометацией (раскрытием) ключей ЭП 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 ЭП:

3.2.1. При подозрении о компрометации рабочего комплекта ключей ЭП владелец соответствующего сертификата ключа немедленно прекращает использование соответствующего ключа ЭП 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 ключей ЭП, информирует пользователей сертификатов соответствующего ключа подписи и совместно с ними обеспечивает приостановку обработки ЭД, полученных после извещения и заверенных ЭП, соответствующей скомпрометированному ключу ЭП.

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

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

3.3. 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 ЭП, проверка подлинности ЭП ЭД производятся на специально подготовленных рабочих местах уполномоченных работников Сторон, оборудованных необходимыми программно-техническими средствами, в том числе средствами ЭП и средствами защиты информации от несанкционированного доступа, в соответствии с технологиями, принятыми Сторонами.

4.2. Установленные на соответствующих рабочих местах средства ЭП и/или используемые в комплекте с ними средства электронной подписи (шифровальных (криптографических) средств) 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 предоставляется уполномоченным работникам Сторон и Администраторам 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 средства электронной подписи (шифровальных (криптографических) средств).

5.2. В Региональном отделении защита информации, передаваемой по каналам связи, обеспечивается использованием сертифицированного средства электронной подписи (шифровальных (криптографических) средств) - 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 средства электронной подписи (шифровальных (криптографических) средств) - КриптоПро CSP или совместимого с ним по форматам сертификатов и криптографических сообщений.

5.4. Размещение, установка, подключение, поэкземплярный учет и последующая эксплуатация указанных средств электронной подписи (шифровальных (криптографических) средств) выполняется в соответствии с требованиями Инструкции № 152, а также технической и эксплуатационной документации на них.

5.5. Прием/передача ЭД, проверка подлинности ЭП входящих ЭД и их предварительная обработка и учет, последующая обработка и учет исходящих ЭД, заверение их ЭП 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. Доступ посторонних лиц в помещения, в которых размещены указанные в настоящей статье средства электронной подписи (шифровальных (криптографических) средств), 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 администраторов безопасности Регионального отделения и органов ЗАГС.

Управляющий Государственного учреждения -регионального отделения Фонда социального страхования Российской Федерации по Удмуртской Республике	Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики
_____ Н.А. Лобанова	_____ Л.А. Попова
М.П.	М.П.