СОГЛАШЕНИЕ № 01-26/7 /806-14/10
об информационном взаимодействии

г. Ижевск 30 октября 2017 г.

Комитет по делам записи актов гражданского состояния при Правительстве Удмуртской Республики, именуемый в дальнейшем (далее Комитет), в лице председателя Поповой Людмилы Александровны, действующего на основании Положения о Комитете, утвержденного постановлением Правительства Удмуртской Республики от 08.12.2014 № 507 и Закона Удмуртской Республики от 20.03.2007 № 8-РЗ «О наделении органов местного самоуправления в Удмуртской Республике государственными полномочиями на государственную регистрацию актов гражданского состояния», с одной стороны, иУправление Федеральной службы судебных приставов по Удмуртской Республике (далее УФССП), в лице и.о. руководителя - главного судебного пристава Удмуртской Республики Наговицына Игоря Владимировича, действующего на основании Положения о территориальном органе службы судебных приставов, с другой стороны, в целях обеспечения эффективного информационного взаимодействия на территории Удмуртской Республики, руководствуясь положениями Федерального закона от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» и Федерального закона от 21.07.1997 № 118-ФЗ «О судебных приставах», Федеральным законом от 01.02.2008 № 229-ФЗ «Об исполнительном производстве», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими нормативными правовыми актами заключили настоящее Соглашение о нижеследующем:

1.Общие положения

1.1.Настоящее Соглашение определяет порядок и условия автоматизированной обработки и обмена информацией в электронном виде по телекоммуникационным каналам связи с использованием средств электронной подписи (шифровальных (криптографических) средств), использования и признания электронной подписи электронных документов (далее - ЭД) и защиты информации при обмене ЭД между УФССП и Комитетом.

1.2. Настоящее Соглашение определяет порядок предоставления информации о смерти, заключении брака, расторжении брака, перемене имени гражданина — должника по исполнительному производству (далее - информация):

1.2.1. По запросу о заключения брака гражданина — должника по исполнительному производству предоставляется информация о фамилии (до и после заключения брака), имени, отчестве, гражданстве, дате и месте рождения.

1.2.2. По запросу о расторжении брака гражданина — должника по исполнительному производству предоставляется информация о фамилии (до и после расторжения брака), имени, отчестве, гражданстве, дате и месте рождения.

1.2.3. По запросу о смерти гражданина — должника по исполнительному производству предоставляется информация о фамилии, гражданстве, имени, отчестве, дате и месте рождения, дате смерти.

1.2.4. По запросу о перемене имени гражданина — должника по исполнительному производству предоставляется информация о фамилии, имени, отчестве, дате и месте рождения, гражданстве, фамилии, имени, отчестве после перемены фамилии.

1.3.При обмене информацией УФССП и Комитет руководствуются: Гражданским кодексом Российской Федерации,Семейным кодексом РФ, Федеральным законом от

15.11.1997 № 143-ФЗ «Об актах гражданского состояния», Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом №229-ФЗ «Об исполнительном производстве», Федеральным законом №118-ФЗ «О судебных приставах», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»,Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ЗакономУдмуртской Республики от 20.03.2007 № 8-РЗ «О наделении органов местного самоуправления в Удмуртской Республике государственными полномочиями на государственную регистрацию актов гражданского состояния», технической документацией на используемые средства электронной подписи (шифровальных (криптографических) средств), другими нормативными правовыми актами, а также настоящим Соглашением.

1.4. Предоставление информации осуществляется на безвозмездной основе.

1.5. Информация формируется из комплексной системы автоматизированной обработки «ЗАГС» (далее - КСАО «ЗАГС»). КСАО «ЗАГС» предназначена для автоматизации делопроизводства в органах ЗАГС, написана на языке программированияDelphi 7.0. База данных построена на СУБД MSSQL. Разработана фирмой «ИНТАР КОМ», г. Подольск, Московская область, тел. (4967) 57-38-80, являющейся правообладателем. Комитет обладает неисключительными правами пользования КСАО ЗАГС бессрочно.

1.6. УФССП и Комитет осуществляют обмен информацией в электронном виде (электронными документами) в соответствии с Регламентом обмена информацией в электронном виде между УФССП и Комитетом (далее -Регламент обмена, Приложение № 1).

1.7. При обмене ЭД УФССП и Комитет руководствуются Инструкцией по защите информации при обмене электронными документами (далее - Инструкция по защите, Приложение № 2).

1.8. По запросу УФССП (на адрес электронной почты zags-arhiv@mail.ru) Комитет представляет информацию в электронном виде по телекоммуникационным каналам связи с использованием средств электронной подписи (шифровальных (криптографических) средств на адрес электронной почты mvv@r18.fssprus.ru), в течение 5 (пяти) рабочих дней с даты получения электронного документа.

1.9. В случае отсутствия возможности отправки по каналам связи информация передается на магнитном носителе ответственному лицу, назначенному УФССП с сопроводительным письмом, подписанным председателем Комитета.

2. Обеспечение электронного документооборота

2.1. В соответствии со статьей 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УФССП и Комитет на основании настоящего Соглашения, признают электронную подпись в ЭД равнозначной собственноручной подписи уполномоченных должностных лиц УФССП и Комитета в документе на бумажном носителе, заверенном печатью.

2.2. Изготовление и сертификацию ключей электронной подписи и ключей проверки электронной подписи для УФССП и Комитетаосуществляет один из Удостоверяющих центров (далее - УЦ).

3. Условия обмена электронными документами и основания его прекращения

3.1. УФССП и Комитет самостоятельно устанавливают и обеспечивают

работоспособность аппаратных, аппаратно-программных средств защиты информации от несанкционированного доступа (далее - НСД) и средств электронной подписи (шифровальных (криптографических) средств), необходимых для осуществления информационного обмена.

3.2. УФССП и Комитет за свой счет оплачивают средства связи и каналы связи, необходимые для осуществления информационного обмена.

3.3. УФССП и Комитет обеспечивают использование комплектов программно-аппаратных средств защиты информации, в том числе средств электронной подписи (шифровальных (криптографических) средств), соблюдение технической документации и инструкций пользователей средств электронной подписи (шифровальных (криптографических) средств).

3.4. УФССП и Комитет назначают работников – ответственныхлиц за осуществление обмена ЭД, в том числе должностных лиц, наделенных правом подписи ЭД (назначаются работники, обладающие правом подписи указанныхдокументов на бумажных носителях).

3.5.Непосредственную эксплуатацию автоматизированного рабочего места ЭД (далее - АРМ ЭД), средств электронной подписи (шифровальных (криптографических) средств) (в том числе в составе АРМ ЭД) организуют и обеспечивают уполномоченные лица УФССП и Комитета.

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

3.6.1. 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.

3.6.2. Компрометация ключевой информации УФССП и Комитета. Порядок действий при компрометации ключей ЭП 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 УФССП и Комитет используют сертифицированные в установленном порядке средства электронной подписи (шифровальных (криптографических) средств), обеспечивающие в соответствии с требованиями ФСТЭК России безопасность конфиденциальной информации, не составляющей государственную тайну. Выбор конкретных видов средств электронной подписи (шифровальных (криптографических) средств) осуществляется с учетом их совместимости,

4.2. УФССП и Комитет признают стойкость используемых средств электронной подписи (шифровальных (криптографических) средств) достаточной для обеспечения конфиденциальности ЭД и подтверждения подлинности электронной цифровой подписи ЭД при условии соблюдения Инструкции по защите.

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

4.4. УФССП и Комитетсвоевременно предоставляют в УЦ в установленном порядке информацию, необходимую для изготовления и учета сертификатов ключей ЭП.

5.Права и обязанности

5.1. При обмене ЭД УФССП и Комитет вправе:

5.1.1. Отказать в приеме ЭД с указанием причины отказа.

5.1.2. Прекратить обмен ЭД при наличии оснований, предусмотренных пунктом 3.6 настоящего Соглашения.

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

5.2. При обмене ЭД УФССП и Комитет 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 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.

5.2.3. Обеспечить условия использования, хранения ключей электронной подписи и ключей проверки электронной подписи 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 подписи.

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 обязуется довести до органов ЗАГС Удмуртской Республики настоящее Соглашение об информационном взаимодействии.

6.2. Персональную ответственность за полноту, достоверность и своевременность передачи сведений о государственной регистрации актов гражданского состояния в электронном виде в КСАО «ЗАГС» несут руководители органов ЗАГС Удмуртской Республики.

6.3. УФССП и Комитет обязуются обеспечить конфиденциальность и безопасность обработки информации о персональных данных граждан, а также конфиденциальность информации, связанной с использованием средств электронной подписи (шифровальных (криптографических) средств).

6.4.УФССП обязуются обеспечить прием, сохранность и установленный порядок использования полученной информации в соответствии с Федеральным закономот 27.07.2006 № 152-ФЗ «О персональных данных».

7.Порядок разрешения разногласий

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

8. Срок действия Соглашения и порядок его изменения

8.1. Настоящее Соглашение вступает в силу с момента подписания обеими Сторонами и действует по 31 декабря 2017 года.

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

8.3. С момента подписания настоящего Соглашения Соглашение от 30.04.2014 года № 906-13/4/01-21/2 признается утратившим силу.

И.о. руководителя Управления Федеральной службы судебных приставов по Удмуртской Республике – главного судебного пристава Удмуртской Республики	Председатель Комитета по делам ЗАГС при Правительстве Удмуртской Республики
_____ Наговицын И.В.	_____ Попова Л.А.

Приложение № 1
к Соглашению об информационном взаимодействии
№ 01-26/7/906-14/10
от 30 октября 2017 г.

Регламент обмена информацией в электронном виде

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок подготовки и оформления электронных документов, предназначенных для обмена между УФССП по Удмуртской Республике (далее УФССП) и Комитетом по делам ЗАГС при Правительстве Удмуртской Республики (далее Комитет).

1.2. При взаимодействии УФССП и Комитетапередача и прием информации осуществляется в электронном виде.

2. Организационная структура

2.1.Прием и отправка электронных документов (далее - ЭД) осуществляется ответственными лицами УФССП и Комитета с использованием средств электронной подписи (шифровальных (криптографических) средств).

2.2 Формирование электронной подписи (далее - ЭП) для ЭД производится уполномоченными лицами УФССП и Комитета.

2.3.Проверка подлинности ЭП ЭД производится уполномоченными лицамиУФССП и Комитета.

3. Структура и формат файлов

3.1. Электронный документооборот осуществляется в следующих форматах и структурах:

3.1.1. «Запрос информации о смерти, заключении брака, расторжении браки, перемене имени граждан - должников по исполнительным производствам» (Приложение к Регламенту).

4. Порядок осуществления электронного документооборота

4.1. УФССП и Комитет 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 электронной подписи (шифровальных (криптографических) средств).

4.2. УФССП и Комитет при осуществлении электронного документооборота выполняют следующие действия при получении ЭД:

проводится контроль достоверности полученных сведений путем проверки корректности ЭП, при положительном результате проверки ЭП проводится дальнейшая работа с представленными сведениями;

в случае отрицательного результата при проверке подлинности ЭП ЭД УФССП и Комитет информируют друг друга, производится анализ причин неверности ЭП, после устранения причин некорректности направляют ЭД повторно.

4.3. В процессе передачи и приема сведений должны быть обеспечены меры по

предотвращению утечки информации, предусмотренные Приложением № 2 к настоящему Соглашению.

4.4.Все полученные в процессе электронного документооборота сообщения электронной почты в обязательном порядке должны проходить антивирусную проверку. В случае получения зараженного файла сведения, содержащиеся в сообщении, остаются без обработки.

4.5. Прием и обработка ЭД осуществляется с использованием программно-аппаратных средств УФССП и Комитета.

Приложение
к Регламенту обмена информацией в электронном виде

Передача данных:

ЗАПРОС	ОТВЕТ

<Request>
<Zapros>
<File_Name></File_Name>
//Наименование файла запроса
<Req_ID></Req_ID>
//Номер запроса
<User_ID></ User_ID>
//Идентификатор пользователя
<IPDate></IPDate>
//Дата регистрации запроса
<DeptorType></DeptorType>
//Тип 1 - Физ
<ReqType></ReqType>
//тип запроса 1 – о смерти, 2 – о заключении брака, 3 – о расторжении брака, 4 – о перемене имени
<Organization_Name></Organization_Name>
//Наименование организации инициирующей запрос
<Prs_Dep></Prs_Dep>
//Номер ОСП по справочнику
<SPIFio></SPIFio>
//Фамилия пристава
<Isp_Num></Isp_Num>
//Номер ИП
<IDSum></IDSum>
//Сумма долга
<IDNum></IDNum>
//Номер ИД
<Req_Date></Req_Date>
//Дата ИД
<DeptorName></DeptorName>
//Должник
<DeptorInn></DeptorInn>
//ИНН если есть
<DeptorAdr></DeptorAdr>
//Адрес должника
<DeptorBirthDate></DeptorBirthDate>
//Дата рождения
<DeptorPlaceBirth></DeptorPlaceBirth>
//Место рождения
</Zapros>
</Request>
	<Response>
	<otvet>
	<RESULT></RESULT>
	//Тип ответа. 1 – есть сведения, 2 – нет сведений, 3 – необходимо уточнение данных документа, удостоверяющего личность должника, 5 – запрос не принят к исполнению в связи с отсутствием обязательных реквизитов запроса.
	<File_Name></File_Name>
	// Наименование файла запроса
	<Req_ID></Req_ID>
	// Номер запроса
	<File_Exp_Name></File_Exp_Name>
	// Наименование файла ответа
	<Res_date></Res_date>
	//Дата ответа
	<DebtorName></DebtorName>
	// Должник ФИО
	<DebtorBirthDate></DebtorBirthDate>
	// Дата рождения
	<DebtorBirthYear></DebtorBirthYear>
	// Год рождения
	<Isp_Num></Isp_Num>
	// Номер ИП
	<Text></Text>
	//Ответ
	<Prs_Dep></Prs_Dep>
	// Номер ОСП по справочнику
	</otvet>
	</Response>

Приложение № 2
к Соглашению об информационном взаимодействии
№ 01-26/7/906-14/10 от 30 октября 2017г.

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 мероприятияпо защите информации при обмене электронными документами между УФССП поУдмуртской Республике (далее - УФССП) и Комитетом при Правительстве Удмуртской Республики (далее - Комитет), именуемые далее - Стороны.

1.2.Организационно-технические мероприятия по защите информации разработаны с учетом требований Положения о разработке, производстве, реализации иэксплуатации 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 сограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 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 сотрудниками Сторон, осуществляющими подготовку, обработку, отправку/получение, хранение и учетЭД, 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 3 (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 па 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 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 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 (один) год.

2.16. За 2 (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 ихуничтожение.

2.21. Администраторы безопасности Сторон организуют и обеспечивают хранение сертификатов ключей подписи в течение срока хранения ЭД, заверенныхсоответствующей 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: утратаносителей ключевой информации, утрата их с последующим обнаружением, хищение, несанкционированное копирование, передача их по линии связи в открытом виде, любыедругие виды разглашения ключевой информации, а также случаи, когда нельзя достоверно установить, что произошло с ключевой информацией и/или носителем (втом числе при выходе носителя из строя и отсутствии возможности опровергнуть наличие несанкционированных действий злоумышленника).

3.2. Действия сотрудников 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 2 (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 комплектаключей 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 с

использованием ЭП, проверка подлинности ЭП в 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 проведенияпрофилактических и ремонтных работ рабочих мест с целью выявления ипредупреждения неконтролируемого изменения их аппаратной части и/или программного обеспечения.

4.4. Доступ к данным рабочим местам предоставляется уполномоченным сотрудникам Сторон и Администраторам безопасности.

5. Защита информации при приеме/передаче электронных документов

5.1.В соответствии с требованиями ФСБ России безопасность информации, несоставляющей государственную тайну при передаче по открытым каналам связиобеспечивается использованием сертифицированных в установленном порядке средств электронной подписи (шифровальных (криптографических) средств).

5.2. В УФССП 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 Комитетезащита информации, передаваемой по каналамсвязи, обеспечивается использованием сертифицированного средства электроннойподписи (шифровальных (криптографических) средств) - КриптоПро CSP илисовместимого 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.

6. Контроль за выполнением требований по защите информации

6.1. Контроль за соблюдением требований по защите информации возлагается на Администраторов безопасности УФССП и Комитета.