УПРАВЛЕНИЕ ЗАПИСИ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ САМАРСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ «ЗАГС–РЕГИОН»

Молодогвардейская, 238, г. Самара, 443100, zags-region63@yandex.ru, тел.(846)337-06-51

ПРИКАЗ

13 апреля 2018 № 21

г. Самара

Об утверждении Политики в отношении обработки персональных данных и защите информации в ГБУ СО «ЗАГС–РЕГИОН»

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику в отношении обработки персональных данных в государственном бюджетном учреждении Самарской области «ЗАГС–РЕГИОН».

2. Создать комиссию по защите информации:

2.1. Утвердить состав комиссии по защите информации согласно приложению 1 к настоящему приказу.

2.2. Утвердить положение о комиссии по защите информации согласно приложению 2 к настоящему приказу.

3. Утвердить типовые формы документов по защите информации:

3.1. Журналы по защите информации согласно приложению 3 к настоящему приказу.

3.2. Протокол заседания комиссии по защите информации согласно приложению 4 к настоящему приказу.

3.3. Акт определения уровня защищенности ПДн при их обработке в ИСПДн согласно приложению 5 к настоящему приказу.

3.4. Акт об уничтожении персональных данных субъектов персональных данных согласно приложению 6 к настоящему приказу.

4. Утвердить перечень информационных систем персональных данных согласно приложению 7 к настоящему приказу.

5. Утвердить перечень обрабатываемых персональных данных согласно приложению 8 к настоящему приказу.

6. Утвердить инструкции и правила по защите информации:

– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 9 к настоящему приказу;

– Правила рассмотрения запросов субъектов персональных данных согласно приложению 10 к настоящему приказу;

– Инструкцию по организации резервного копирования, согласно приложению 11 к настоящему приказу;

– Инструкцию по организации парольной защиты, согласно приложению 12 к настоящему приказу;

– Инструкцию по организации антивирусной защиты, согласно приложению 13 к настоящему приказу;

– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно приложению 14 к настоящему приказу;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 15 к настоящему приказу;

– Инструкцию по обращению с криптосредствами согласно приложению 16 к настоящему приказу;

– Правила работы с обезличенными данными согласно приложению 17 к настоящему приказу;

– Порядок учета и использования съемных машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию согласно приложению 18 к настоящему приказу.

7. Настоящий приказ вступает в силу с момента его подписания.

8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.В. Довжик

Приложение 1
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

Состав комиссии по защите информации

Председатель комиссии	Пырсакова Юлия Леонидовна, заместитель директора
Члены комиссии	Килина Елена Николаевна, главный бухгалтер
	Белоусова Ирина Владимировна, инспектор по кадрам
	Никифоров Дмитрий Сергеевич, инженер-программист

Приложение 2
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных государственного бюджетного учреждения Самарской области «ЗАГС–РЕГИОН».

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Определение класса защищенности информационных систем персональных данных ГБУ СО «ЗАГС–РЕГИОН» на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников ГБУ СО «ЗАГС–РЕГИОН», участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются приказом директора ГБУ СО «ЗАГС–РЕГИОН».

3.4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников ГБУ СО «ЗАГС–РЕГИОН», участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети ГБУ СО «ЗАГС–РЕГИОН».

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

Приложение 3
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета средств криптографической защиты информации

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечания
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кот-рым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка Об уничтожении	

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатаци	Примечание

ЖУРНАЛ
учета ЭП

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

ЖУРНАЛ
учета ключей от режимных помещений, ключей от хранилищ, личных печатей от хранилищ

№ п/п	Ф.И.О.	Получил	Дата	Время	Отметка о возврате (подпись администратора)

ЖУРНАЛ
учета выдачи паролей

№ п/п	Дата получения пароля	Ф.И.О. получателя	Подпись получателя

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение 4
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13. 04.2018 № 21

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения _____

Место проведения _____

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих ГБУ СО «ЗАГС–РЕГИОН».

1. Слушали: _____
доложил(а) исходные данные об ИСПДн ГБУ СО «ЗАГС–РЕГИОН».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн ГБУ СО «ЗАГС–РЕГИОН» .

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС ГБУ СО «ЗАГС–РЕГИОН».

2. Слушали: _____
доложил(а) исходные данные об ИСПДн ГБУ СО «ЗАГС–РЕГИОН».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн ГБУ СО «ЗАГС–РЕГИОН» .

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС ГБУ СО «ЗАГС–РЕГИОН».

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

Приложение 5
к приказу ГБУ СО «ЗАГС – РЕГИОН»
от 13.04.2018 № 21

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн
«_____»

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– ИСПДн _____ представляет собой _____;

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются _____ категории персональных данных;

– Категории субъектов: _____;

– По наличию подключений к сети общего пользования и сети Интернет, ИСПДн _____ относится к системам _____ подключение;

– По режиму обработки персональных данных в информационной системе ИСПДн _____ относится к _____ режимам обработки;

– По разграничению прав доступа пользователей, ИСПДн _____ относится к системам _____ прав доступа пользователей;

– Технические средства ИСПДн _____ размещены на территории Российской Федерации по адресу: 443100, Самарская обл, город Самара, улица Молодогвардейская, 238, кабинет _____.

– Объем обрабатываемых в ИСПДн персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы _____ актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить _____ уровень защищенности (УЗ ___) персональных данных.

	_____	ФИО
Председатель комиссии		
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____2018 г.

Приложение 6
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

АКТ
Об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____ _____
(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____
подпись расшифровка

Члены комиссии: _____ _____
подпись расшифровка

_____ _____
подпись расшифровка

Приложение 7
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.09.2018 № 21

Перечень информационных систем персональных данных

Наименование	Адрес расположения
Информационная система персональных данных ГБУ СО «ЗАГС–РЕГИОН»: «1С: Зарплата и кадры бюджетного учреждения, 1С Бухгалтерия государственного учреждения»	443100, Россия, Самарская область, г. о. Самара, ул. Молодогвардейская, д. 238

Приложение 8
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ПЕРЕЧЕНЬ
обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
1. Обработка персональных данных в ИСПДн «1С: Зарплата и кадры бюджетного учреждения, 1С Бухгалтерия государственного учреждения»		
Общие сведения о работниках и гражданах – получателей услуг, лицах, обратившихся по вопросам заключения иных договоров, государственных контрактов.	**Перечень обрабатываемых ГБУ СО «ЗАГС – РЕГИОН» персональных данных работников:** — фамилия, имя, отчество; — дата рождения; — пол; — адрес (место жительства), контактный телефон; — страховой номер индивидуального лицевого счета; — серия, номер паспорта или данные иного документа, удостоверяющего личность, дата выдачи этих документов и наименование выдавшего их органа; — образование, профессия, специальность, занимаемая должность, ИНН, иная информация, в соответствии с законодательством Российской Федерации необходимая для заключения трудового договора. **Перечень обрабатываемых ГБУ СО «ЗАГС – РЕГИОН» персональных данных лиц – получателей услуг:** — фамилия, имя, отчество;	Реализация кадровой и бухгалтерской политики

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
	— дата рождения; — пол; — адрес (место жительства), контактный телефон; — страховой номер индивидуального лицевого счета; — серия, номер паспорта или данные иного документа, удостоверяющего личность, дата выдачи этих документов и наименование выдавшего их органа; — иная информация, в соответствии с законодательством Российской Федерации необходимая для предоставления заявителю услуг Учреждения; **Перечень обрабатываемых ГБУ СО «ЗАГС – РЕГИОН» персональных данных** лиц, обратившихся по различным вопросам, в том числе представителей юридических лиц, индивидуальных предпринимателей по вопросам заключения договоров и государственных контрактов; — фамилия, имя отчество; — серия и номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя; — сведения о дате выдачи указанного документа и выдавшем его органе; — адрес электронной почты, телефон; — образование, профессия, специальность, занимаемая должность, ИНН, иная информация, в соответствии с законодательством Российской Федерации необходимая для заключения договоров, государственных контрактов.	

Приложение 9
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

– Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

– Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

– Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

– Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных

данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

– Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 10
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– Подтверждение факта обработки персональных данных;

– Правовые основания и цели обработки персональных данных;

– Цели и применяемые оператором способы обработки персональных данных;

– Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);

– Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

– Сроки обработки персональных данных, в том числе сроки их хранения;

– Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для

раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта

персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

– Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

– В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

– Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

– Оператор обязан сообщить в уполномоченный орган по защите прав

субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 11
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ИНСТРУКЦИЯ
по организации резервирования

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

– Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

– Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

– Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

– Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств

защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему работниками учреждения, эксплуатирующими ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся работниками учреждения, эксплуатирующими ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы служебных помещений работников, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и работника учреждения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

Приложение 12
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ИНСТРУКЦИЯ
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

– Длина пароля должна быть не менее 8 символов;

– В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– При смене пароля новое значение должно отличаться от предыдущих;

– Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом

администратору информационной безопасности для принятия соответствующих мер.

Приложение 13
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность работников учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

2. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности должна быть выполнена антивирусная проверка на защищаемом сервере и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник учреждения самостоятельно или вместе с администратором информационной безопасности должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

– Приостановить работу в ИСПДн;

– Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, владельца зараженных файлов, а также работников учреждения, использующих эти файлы в работе;

– Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– Провести лечение или уничтожение зараженных файлов.

3. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в учреждении и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех работников учреждения, являющихся пользователями ИСПДн.

Приложение 14
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.09.2018 № 21

ПОРЯДОК

уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например,

утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение 15
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в ГБУ СО «ЗАГС–РЕГИОН» требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.

3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

4. Плановые проверки проводятся не чаще чем один раз в три месяца.

5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

6. Основанием для проведения проверки служит издание приказа «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

– соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;

– соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достаточность (избыточность) персональных данных для целей обработки

персональных данных, заявленных при сборе персональных данных;

– отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

– порядок и условия применения средств защиты информации;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих полномочий;

– требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес директора результаты проведения проверки в форме служебной записки.

Приложение 16
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ИНСТРУКЦИЯ
по обращению с криптосредствами

1. Общие положения

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

2. Требования по размещению, оборудованию и охране помещений

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

3. Порядок обращения с СКЗИ

Пользователи криптосредств обязаны:

– не разглашать информацию о ключевых документах;

– не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

– не допускать установки ключевых документов в другие ПЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы (Приложение). Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

– для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

– для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Приложение 17
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 № 21

ПРАВИЛА
работы с обезличенными данными

1.Общие положения

Настоящие Правила работы с обезличенными персональными данными ГБУ СО «ЗАГС–РЕГИОН» разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными в учреждении.

2.Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

– персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

– обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

– обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных ГБУ СО «ЗАГС–РЕГИОН» и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

– уменьшение перечня обрабатываемых сведений;
– замена части сведений идентификаторами;
– обобщение – понижение точности некоторых сведений;
– понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)
– деление сведений на части и обработка в разных информационных системах;
– другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

1. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:
– парольной политики;
– антивирусной политики;
– правил работы со съемными носителями (если они используется);
– правил резервного копирования;
– правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
– правил хранения бумажных носителей;
– правил доступа к ним и в помещения, где они хранятся.

Приложение 18
к приказу ГБУ СО «ЗАГС–РЕГИОН»
от 13.04.2018 №21

ПОРЯДОК
учета и использования съемных машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию

1. Общие положения

Настоящий Порядок разработан в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации». Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», и другими нормативными правовыми актами, и устанавливает порядок учета и использования машинных носителей информации для обработки персональных данных.

2. Порядок использования съемных машинных носителей информации

2.1. Под использованием съемных машинных носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

2.2. В ИС допускается использование только учтенных съемных машинных носителей информации, которые подвергаются регулярной ревизии и контролю.

2.3. К съемным машинным носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

2.4. Съемные машинные носители конфиденциальной информации предоставляются работникам учреждения в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у работника производственной необходимости.

3. Порядок учета, хранения и обращения со съемными машинными носителями конфиденциальной информации (персональных данных)

3.1. Все находящиеся на хранении и в обращении съемные машинные носители с конфиденциальной информацией (персональными данными) подлежат учёту.

3.2. Каждый съемный машинный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных машинных носителей конфиденциальной информации (персональных данных) осуществляет инженер - программист, на которого возложена функция хранения машинных носителей персональных данных. Факт выдачи съемного машинного носителя исполнителю фиксируется в журнале учета съемных машинных носителей конфиденциальной информации.

3.4. Пользователи получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ Пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

3.5. При использовании Пользователями машинных носителей с конфиденциальной информацией (персональными данными) необходимо:

- соблюдать требования настоящего Порядка;

- использовать машинные носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администратора ИС о любых фактах нарушения требований настоящего Порядка;
- бережно относится к машинным носителям конфиденциальной информации (персональных данных);
- обеспечивать физическую безопасность машинных носителей информации всеми разумными способами;
- извещать администратора ИС о фактах утраты (кражи) машинных носителей конфиденциальной информации (персональных данных).

3.6. При использовании машинных носителей конфиденциальной информации (персональных данных) запрещается:

- использовать носители конфиденциальной информации (персональных данных) в личных целях;
- передавать носители конфиденциальной информации (персональных данных) другим лицам (за исключением администратора ИС);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с общедоступными данными, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съёмные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

3.7. Любое взаимодействие (обработка, прием/передача информации), инициированное сотрудником между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев согласованных с администратором ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование машинных носителей информации.

3.8. В случае выявления фактов несанкционированного и/или нецелевого использования машинных носителей конфиденциальной информации (персональных данных) инициализируется служебная проверка, проводимая комиссией, состав и полномочия которой определяется приказом. По факту выясненных обстоятельств составляется акт расследования инцидента.

3.9. Информация, хранящаяся на машинных носителях конфиденциальной информации (персональных данных), подлежит обязательной проверке на отсутствие вредоносного ПО.

3.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные машинные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных машинных носителях осуществляется в порядке, установленном для документов для служебного пользования.

3.11. Вынос съемных машинных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения ответственных лиц.

3.12. В случае утраты или уничтожения съемных машинных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель учреждения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

3.13. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению в соответствии с «Порядком уничтожения документов и машинных носителей информации, содержащих персональные данные».

3.14. В случае увольнения работника, предоставленные ему машинные носители конфиденциальной информации (персональных данных) изымаются уполномоченным

сотрудником, на которого возложены функции хранения машинных носителей персональных данных.

4. Ответственность

Пользователи и администратор информационной системы, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами учреждения.