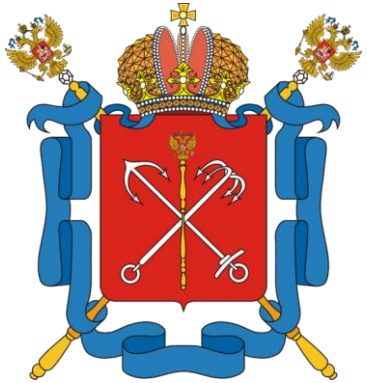
Комитет по информатизации и связи



Обеспечение соблюдения конфиденциальности информации, доступ к которой ограничен в соответствии с федеральными законами, в исполнительных органах государственной власти Санкт-Петербурга.
Сборник типовых (примерных) форм организационно-распорядительной документов

(версия по состоянию на 09.04.2014)

Санкт-Петербург 2014

	Термины и определения
	Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" *ст. 9* *2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.*
	Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" *ст. 3* *1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)* *ст. 3* *10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств*
	Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" *ст. 14* *1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.*
	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282. *1.16. Конфиденциальная информация — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.* *1.17. Конфиденциальность информации — состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.*

	Основные нормативные правовые акты и методические документы в соответствии с которыми разрабатываются организационно-распорядительные документы для проведения мероприятий по обеспечению соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами
	Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации" *1. Настоящий Федеральный закон регулирует отношения, возникающие при:* *1) осуществлении права на поиск, получение, передачу, производство и распространение информации;* *2) применении информационных технологий;* *3) обеспечении защиты информации.*
	Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных" *1.Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации*

	Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" *В соответствии с частью 3 статьи 18.1 Федерального закона "О персональных данных" Правительство Российской Федерации постановляет:* *Утвердить прилагаемый перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.*
	Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» *Отменило действие Постановление Правительства РФ от 17.11.2007 №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"* *Определило подход к определению уровней защищенности персональных данных, введенных Федеральным законом от 25.07.2011 №261-ФЗ* *Установило требования к защите персональных данных при их обработке в информационных системах персональных данных в зависимости от уровня защищенности*
	Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" *В целях реализации Федерального закона "О персональных данных" Правительство Российской Федерации постановляет:* *1) Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.*

	Приказ ФСТЭК России №21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных *Регулирует деятельность всех операторов персональных данных, кроме государственных информационных систем* *Заменил Приказ ФСТЭК РФ от 05.02.2010 № 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"*
	Приказ ФСТЭК России от 11.02.2013 №17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах *Регулирует деятельность по защите государственных информационных систем, в том числе при обработке персональных данных*

	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282 **2.1. Настоящий нормативно-методический документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений составляющих государственную тайну (далее — конфиденциальная информация), на территории Российской Федерации** *СТР-К применяется в качестве методического документа при реализации мер по защите технических средств государственных информационных систем (ЗТС.1), выбранных в соответствии с пунктом 21 и приложением №2 к Требованиям, утвержденным приказом ФСТЭК России от 11.02.2013 №17, в целях нейтрализации угроз безопасности информации, связанных с защитой информации, представленной в виде информативных электрических сигналов и физических полей (защита от утечки по техническим каналам).* *Иные положения СТР-К (раздел 3 "Организация работ по защите конфиденциальной информации", раздел 5 "Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах") могут применяться по решению обладателей информации, заказчиков и операторов государственных информационных систем в части, не противоречащей Требованиям, утвержденным приказом ФСТЭК России от 11.02.2013 № 17.* *Кроме того, положения СТР-К и РД АС применяются по решению обладателя информации (заказчиков, операторов информационных систем) для защиты информации, содержащей сведения конфиденциального характера (Указ Президента Российской Федерации от 6.03.1997 № 188 "Об утверждении перечня сведений конфиденциального характера"), обрабатываемой в информационных системах, которые в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" не отнесены к государственным информационным системам.*

	Требования по защите персональных данных установлены правительством Российской Федерации, а именно его постановлениями от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", в которых описаны вопросы неавтоматизированной обработки персональных данных и их обработки с использованием средств автоматизации. Обязанность по контролю исполнения требований, а также по разработке необходимых нормативных документов возложены на уполномоченные органы исполнительной власти. **Уполномоченными органами являются:** -Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор России); -Федеральная служба по техническому и экспортному контролю (ФСТЭК России); -Федеральная служба безопасности (ФСБ России). **Данные органы действуют строго в рамках своей компетенции.** **1. Роскомнадзор России** отвечает за общий контроль и надзор, представление интересов физических лиц при обработке их персональных данных в организациях. **2. ФСТЭК России** регламентирует вопросы технической защиты персональных данных. **3. ФСБ России -** вопросы криптографической защиты при передаче персональных данных по каналам связи. **При осуществлении своих функций знакомиться с персональными данными, обрабатываемыми в организации, имеют право только сотрудники Роскомнадзора.**

Примерные формы
организационно-распорядительных документов, регламентирующих организацию работ в органах исполнительной власти по обеспечению соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами

№	Наименование документа	Страница	Нормативные правовые акты и методические документы в соответствии с которыми разрабатываются организационно-распорядительных документы для АС и ИС			Примечание
			СТР-К	152-ФЗ ПП 1119 ПП 211 ПП687 Приказ 17 Приказ 21	149-ФЗ Приказ 17 СТР-К	
			АС не отнесенные к ИСПДн и ГИС Класс защищенности	**ИСПДн** Уровень защищенности	**ГИС** Класс защищенности (Уровень значимости+ масштаб информационной систем)	
1	2	3	4	5	6	7
1	**Приказ о назначении ответственного за организацию обработки персональных данных.** **ст. 18.1, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;* **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"** *п. 1 а) назначают ответственного за организацию обработки персональных данных в*	**35**		+		

	государственном или муниципальном органе из числа государственных или муниципальных служащих (далее - служащие) данного органа					
2	**Правила обработки персональных данных** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"** *б) утверждают актом руководителя государственного или муниципального органа следующие документы:* *правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных,*	**38**		**+**		
3	**Правила рассмотрения запросов субъектов персональных данных или их представителей** **Постановление Правительства РФ от 21.03.2012 №211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б правила рассмотрения запросов субъектов персональных данных или их представителей*	**41**		**+**		
4	**Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора*	**43**		**+**		
5	**Правила работы с обезличенными данными** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных**	**45**		**+**		

	Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами *п.1б правила работы с обезличенными данными*					
6	**Перечень информационных систем персональных данных** **Постановление Правительства РФ от 21.03.2012 №211"Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"** *п.1б перечень информационных систем персональных данных*	**47**		**+**		
7	**Перечень персональных данных, обрабатываемых в государственном или муниципальном органе** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;*	**51**		**+**		
8	**Перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных*	**54**		**+**		
9	**Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки**	**55**		**+**		

	персональных данных либо осуществление доступа к персональным данным **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным*					
10	**Должностная инструкция ответственного за организацию обработки персональных данных** (Раздел должностных инструкций (должностного регламента) сотрудников имеющих доступ к ИСПДн, в части обеспечения безопасности ПДн) **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"** *п.1б должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе*	**56**		+		
11	**Типовое обязательство работника непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного или муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей*	**58**		+		

12	**Типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных** **Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные** **Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *Статья 9. Согласие субъекта персональных данных на обработку его персональных данных* **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;*	**59**		+		
13	**Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1б порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных*	**64**		+		
14	**Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1 г) при обработке персональных данных, осуществляемой без использования средств*	**66**		+		

	автоматизации, выполняют требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"					
15	**Типовой план периодических проверок условий обработки персональных данных в организации в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1д) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа.*	**69**		**+**		
16	**Ведомость ознакомления служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных** **ст. 22.1, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных** *2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных* **Постановление Правительства РФ от 21.03.2012 №211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1е) **осуществляют ознакомление служащих** государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с*	**73**		**+**		

	положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных					
17	**Обучение работников по вопросам обработки персональных данных** **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1 е) организуют обучение указанных служащих;*	**74**		**+**		
18	**Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных** **Постановление Правительства РФ от 21.03.2012 №211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами** *п.1 з) согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.*	**75**		**+**		
19	**Уведомление об обработке (намерении осуществлять обработку) персональных данных** **Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *Статья 22. Уведомление об обработке персональных данных* *1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.* **Приказ Минкомсвязи России от 21.12.2011 № 346 "Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных"** *Утверждена форма Уведомления об обработке (о намерении осуществить обработку) персональных данных* **Приказ Роскомнадзора от 19.08.2011 № 706 «Об утверждении рекомендаций по ее заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».**	**81**		**+**		

20	**Политика оператора в отношении обработки персональных данных** **ст. 18.1, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;* **Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"** *2. Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.*	**83**		+		
21	**Приказ о назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе** (для каждой ИСПДн) **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.*	**88**		+		
22	**Приказ об организация режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных** **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *а) организация режима обеспечения безопасности помещений, в которых размещена информационная система*	**90**		+		
23	**Приказ об утверждении мест хранения носителей персональных данных**	**91**		+		

	Постановление Правительства РФ от 15.09.2008 №687"Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" *13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.* **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:* *б) обеспечение сохранности носителей персональных данных*					
24	**Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.**(для каждой ИСПДн) **ст. 88, "Трудовой кодекс Российской Федерации" от 30.12.2001 №197-ФЗ** *разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;* **ст. 19, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;* **Постановление Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей*	**92**		+		
25	**О доступе к содержанию электронного журнала сообщений** **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований**	**93**		+		

	к защите персональных данных при их обработке в информационных системах персональных данных" *15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.*					
26	**Приказ об утверждении перечня лиц, осуществляющих обработку персональных данных без использования средств автоматизации и имеющих к ним доступ.** **ст. 3, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *3) 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;* **Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"** *13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.*	**94**		**+**		
27	**Приказ об утверждении мест хранения персональных данных (материальных носителей) для осуществления их обработки без использования средств автоматизации.** **Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"** *13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.*	**95**		**+**		**В случае неавтоматизированной обработки ПДн**

28	**Ведомость ознакомления лиц о факте обработки ими персональных данных, без использования средств автоматизации и категориях обрабатываемых ими персональных данных** **Постановление Правительства РФ от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации***"* *6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).*	**96**		**+**		
29	**О журнале учета, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора** **Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"** *а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных*	**97**		**+**		
30	**Типовая форма журнала учета, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора** **Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования**	**98**		**+**		**При неавтоматизированной обработке**

	средств автоматизации" *8. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор*					
31	**Положение о порядке организации и проведения работ по защите конфиденциальной информации** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *3.5. Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом «Положении о порядке организации и проведения работ по защите конфиденциальной информации»*	**99**	**+**	**+**	**+**	
32	**Перечень сведений конфиденциального характера, подлежащих защите, в том числе персональных данных. Лист ознакомления** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *5.1.3. В качестве основных мер защиты информации рекомендуются:* *Документальное оформление перечня сведений конфиденциального характера, в том числе с учетом ведомственной и отраслевой специфики этих сведений;* **Указ Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера»**	**116**	**+**	**+**	**+**	
33	**Приказ о создании комиссии по классификации автоматизированных систем, обрабатывающих конфиденциальную информацию** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** 5.1.5. Классификация АС осуществляется на основании требований РД Гостехкомиссии России и настоящего раздела документа. 5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер, оптимизации выбора средств защиты информации и затрат на защиту информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении Ж).	**121**	**+**	**+**		
34	**Акт классификации автоматизированной системы, предназначенной для обработки конфиденциальной**	**123**	**+**	**+**	**+**	

	информации (для каждой системы) **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер, оптимизации выбора средств защиты информации и затрат на защиту информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении Ж).*					
35	**Перечень сотрудников (матрица доступа) допущенных к сведениям конфиденциального характера (персональным данным)** **ст. 2, Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации"** *5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам* **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *3.6. В организации должен быть документально оформлен перечень сведений конфиденциального характера (приложение Б), подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.* **"Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения"(утв. Гостехкомиссией РФ 30.03.1992)** *8. Матрица доступа - Таблица, отображающая правила разграничения доступа*	**124**	**+**	**+**	**+**	
36	**Список лиц, допущенных в защищаемое помещение** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *5.1.3. В качестве основных мер защиты информации рекомендуются:* *ограничение доступа персонала и посторонних лиц в ЗП и помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;*	**126**	**+**	**+**		
37	**Приказ об организации режима обеспечения безопасности помещений, предназначенных для обработки конфиденциальной информации** **"Специальные требования и рекомендации по технической защите конфиденциальной**	**127**	**+**	**+**	**+**	

	информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282. *4.2.1. В организации должен быть документально определен перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации,*					
38	**Приказ о назначении администратора защиты (безопасности) информации** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *1.5. Администратор защиты (безопасности) информации — лицо, ответственное за защиту АС от несанкционированного доступа к информации.* **"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных"(Выписка)(утв. ФСТЭК РФ 15.02.2008)** *Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.*	**130**	**+**	**+**		
39	**Инструкции по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных)** **Приказ ФСТЭК России 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"** *Учет машинных носителей персональных данных* **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;*	**136**	**+**	**+**		
40	**Типовая форма журнала учета машинных носителей конфиденциальной информации (персональных данных)** **п.2 ст.19 Федерального закона №152 "О персональных данных"** *п.п. 5) учетом машинных носителей персональных данных;* **Постановление Правительства №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"** *4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации*	**141**	**+**	**+**		

	их на отдельных материальных носителях персональных данных (далее - материальные носители) **ч.2 Приказа ФСТЭК №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"** *8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным* **Постановление Правительства РФ №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»** *2. В настоящих требованиях под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность (далее - материальный носитель).* **ст.13 Постановления Правительства РФ №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *б) обеспечение сохранности носителей персональных данных;*					
41	**Приказ о назначении ответственного за обеспечение функционирования и безопасности криптосредств, в случае их использования для безопасности персональных данных при их обработке в информационных системах персональных данных** **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных** *4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".* **Приказ ФСБ РФ от 09.02.2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"** *51. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:* *обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;* *собственником (владельцем) информационных ресурсов (информационных систем), в*	**142**	+	+		

	составе которых применяются СКЗИ; **"Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)** *2.6. Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее - ответственный пользователь криптосредств).*					
42	**Приказ о назначении (структурного подразделения) должностного лица за защиту информации** **Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"** *9. Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.* **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *2.15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ.*	**143**	**+**	**+**	**+**	
43	**Приказ о назначении комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)** **ст. 19, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных* **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.*	**145**		**+**		
44	**Инструкции о порядке резервирования и восстановления работоспособности технических**	**147**		**+**		

	средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных **Приказ ФСТЭК России 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"** *X. Обеспечение доступности персональных данных (ОДТ)* *Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы*					
45	**Инструкция о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций**	**153**		+		
46	**Руководство администратору по обеспечению безопасности информационных систем персональных данных** **Инструкция администратору по обеспечению безопасности информационных систем персональных данных** **Приказ Минздравсоцразвития РФ от 22.04.2009 № 205 "Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"** *Администратор по обеспечению безопасности информации* **"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)** *Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.* *5.1.* *К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.* **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *6.3.6. Мероприятия по обеспечению безопасности информации должны быть отражены в*	**159**		+		

	инструкциях, определяющих: *обязанности и ответственность пользователей и администратора безопасности при взаимодействии с Сетью;* **Руководящий документ «Защита от несанкционированного доступа к информации: Термины и определения». утвержден Гостехкомиссией России 30.03.1992** *Администратор защиты - это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации*					
47	**Типовая форма журнала учета средств криптографической защиты информации** **Приказ ФСБ РФ от 09.02.2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"** *48. СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ и их опытных образцов определяет ФСБ России.* **Приказ ФАПСИ от 13.06.2001 № 152 "Об утверждении 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"** *п.7 поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;*	**168**	**+**	**+**		**В случае использования СКЗИ**
48	**Типовая форма журнала учета ключевых носителей** **"Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)** *Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.*	**169**	**+**	**+**		**В случае использования СКЗИ**
49	**Типовая форма журнала выдачи носителей ключевой информации** **"Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)**	**170**	**+**	**+**		**В случае использования СКЗИ**

	Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.).					
50	**Типовая форма журнала учета сертифицированных технических средств защиты информации, эксплуатационной и технической документации к ним** **"Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования о защите информации" (далее - РД АС).** *-должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и занесением учетных данных в журнал* **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *2.16. Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации технические средства защиты информации.*	**171**	**+**	**+**		**В случае использования СКЗИ**
51	**Список лиц, допущенных к работе на автоматизированных системах или информационной системе персональных данных** **ст. 19, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных*	**173**		**+**		
52	**Акт определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)** (для каждой системы) **ст. 18.1, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** 5*) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом* **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.*	**174**		**+**		

53	**Акт установки средств защиты информации на объекте вычислительной техники - автоматизированное рабочее место** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *3.16. На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:* *закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка;*	**176**	**+**	**+**	**+**	**В случае использования СКЗИ**
54	**Акт об уничтожении материальных (машинных, бумажных носителей) конфиденциальной информации, персональных данных** **ст. 3, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются* ***материальные носители персональных данных****;* **Постановление Правительства РФ от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"** *б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.* *10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).*	**177**		**+**		**В случае достижения цели обработки**
55	**Модель угроз безопасности информации и модель нарушителя** **Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"** *Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель*	**178**	**+**	**+**	**+**	

	нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации. **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *3.8. На предпроектной стадии по обследованию объекта информатизации:* *определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта*					
56	**План мероприятий по технической защите конфиденциальной информации и персональных данных**	**220**	**+**	**+**		
57	**План внутренних проверок состояния защиты конфиденциальной информации**	**232**	**+**	**+**		
58	**Схема расположения объекта информатизации относительно границы КЗ, размещения АС и ЗП относительно контролируемой зоны, топологической схемы АС, схем коммуникаций, электропитания и заземления объекта** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.** *3.8. На предпроектной стадии по обследованию объекта информатизации:* *определяются условия расположения объекта информатизации относительно границ КЗ*	**234**	**+**	**+**		
59	**Заключение о готовности средств защиты информации к использованию и возможности их эксплуатации в информационной системе персональных данных** **Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования"** *- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации*	**240**	**+**	**+**		**В случае использования СКЗИ**

60	**Приказ об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.** **Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.** **Акт осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.** **ст. 18.1, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора*	**242**		+		
61	**Журнал учета проверок проводимых органами государственного контроля (надзора), органами муниципального контроля** **ст. 16, Федеральный закон от 26.12.2008 № 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"** *8. Юридические лица, индивидуальные предприниматели обязаны вести журнал учета проверок по типовой форме, установленной федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации.* **Приказ Минэкономразвития РФ от 30.04.2009 № 141 "О реализации положений Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"** *-Утвердить типовую форму журнала учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля согласно приложению 4.*	**255**		+	+	
62	**Положение о порядке обработки и обеспечении безопасности персональных данных** **Лист ознакомления работников с Положением порядке**	**257**		+		

	обработки и обеспечении безопасности персональных данных **ст. 18.1, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений* **ст. 68, "Трудовой кодекс Российской Федерации" от 30.12.2001 №197-ФЗ** *При приеме на работу (до подписания трудового договора) работодатель обязан ознакомить работника под роспись с правилами внутреннего трудового распорядка, иными локальными нормативными актами, непосредственно связанными с трудовой деятельностью работника, коллективным договором.* **ст.86** *8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;*					
63	**Журнал учета обращений граждан и запросов субъектов персональных данных (или их представителей) по вопросам обработки персональных данных** **Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *ст.14 . Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. 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,* *ст. 22.1* *3) 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.*	**265**		**+**		**Возможно ведение в электронной форме**
64	**Обязательство о неразглашении информации, содержащей персональные данные** **"Трудовой кодекс Российской Федерации" от 30.12.2001 №197-ФЗ** ***ст. 81*** *в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника;*	**266**		**+**		

	ст. 86 ***7)*** *защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;* **ст. 2, Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации"** ***7)*** *конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя*					
65	**Инструкция по организации резервного копирования** **ст. 19, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;* **Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"** *20.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.*	**267**		+	+	
66	**Инструкция по организации антивирусной защиты** **Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"** *20.6. Меры по* ***антивирусной защите*** *должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.*	**273**		+	+	
67	**Уведомление о получении персональных данных не от субъекта персональных данных** **ст. 18, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"** *3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию…*	**280**		+		

68	**Типовая форма уведомления субъекта персональных данных о необходимости дать согласие на предоставление персональных данных третьем лицам** **ст. 22, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных** *2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;*	**281**		+		
69	**Примерная форма ответа работодателя на запрос третьей стороны о передаче персональных данных работника с требованием соблюдения режима секретности (конфиденциальности) переданных персональных данных работника** **ст. 88, "Трудовой кодекс Российской Федерации" от 30.12.2001 №197-ФЗ** *предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;* **ст. 6, Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных»** *3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.*	**282**		+		
70	**План мероприятий по организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных** **"Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" Утверждены ФСТЭК России 15.02.2008** *3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн*	**283**		+		

	понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.					
71	**Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных** **"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК России 15.02.2008)** ***Раздел 3*** *режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.*	**286**		+		
72	**Журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств** **Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"** *Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций*	**290**		+		
73	**Положение о разрешительной системе доступа сотрудников к защищаемым информационным ресурсам** **"Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282** *3.6."В организации должен быть документально оформлен перечень сведений конфиденциального характера (приложение № 2), подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведения"*	**292**	+	+		
74	**Приказ о внесении изменений в документы, содержащие персональные данные работника (образец заполнения)** **ст. 20, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *3. 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 семи рабочих дней со дня*	**297**		+		

	предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.					
75	**Оформление дополнительного соглашения к трудовому договору, в связи с назначением ответственным за организацию обработки персональных данных** **р. III, "Трудовой кодекс Российской Федерации" от 30.12.2001 № 197-ФЗ** **Статья 72. Изменение определенных сторонами условий трудового договора** *Изменение определенных сторонами условий трудового договора, в том числе перевод на другую работу, допускается только по соглашению сторон трудового договора, за исключением случаев, предусмотренных настоящим Кодексом. Соглашение об изменении определенных сторонами условий трудового договора заключается в письменной форме.*	**298**		+		
76	**Перечень персональных данных, подлежащих защите при их обработке в информационных системах персональных данных** **ст. 19, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных*	**299**		+		
77	**Инструкция пользователя информационной системы персональных данных по обеспечению безопасности информации** **"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)** *Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования*	**302**		+		
78	**Заявление отзыв согласия на обработку персональных данных** **ст. 21, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки*	**305**		+		

	персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва					
79	**Уведомление об уточнении персональных данных** **ст. 5, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.*	**306**		+		
80	**Уведомление об уничтожении персональных данных** **ст. 14, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *3. 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 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 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 и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.*	**307**		+		
81	**Информационное письмо о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных** **ст. 22, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.*	**308**		+		
82	**Инструкция о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты**	**310**	+	+		

	Указ Президента РФ от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" *б) при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;*					
83	**Примерный проект договора о поручении обработки персональных данных третьим лицам** **Примерный проект соглашения о конфиденциальности** **ст. 6, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"** *5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.*	**319**		+		
84	**Инструкция о порядке проведения разбирательств по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности персональных данных** **Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования"** *проведение разбирательств и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационной системы общего пользования, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений*	**331**	+	+		

85	**Об электронном журнале безопасности** **Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"** *6. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:* *а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе*	**334**		+		
86	**Согласие субъекта на трансграничную передачу персональных данных** **ст. 12, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"** *4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:* *1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных*	**335**		+		
87	**Согласие субъекта на обработку биометрических персональных данных** **ст. 11, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"** *1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.*	**336**		+		
88	**Внесение изменений в трудовой договор при изменении персональных данных (смена фамилии и т.д.)**	**337**				
89	**Запрос субъекта персональных данных на получение информации, касающейся обработки его персональных данных** **ст. 14, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"** 7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных	**338**				
90	**Перечень основных действующих нормативных правовых актов и методических документов в**	**339**	+	+	+	

	области защиты информации					
	Полезная информация					
	ВСЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ	**349**				