УНИВЕРСИТЕТ ИТМО

А.Д. Катаржнов

ОРГАНИЗАЦИОННО - РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Санкт-Петербург

2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.Д. Катаржнов

ОРГАНИЗАЦИОННО - РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ ОРГАНОВ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт - Петербург

2016

Катаржнов А.Д. Организационно – распорядительные документы органов власти, муниципальных образований и предприятий по защите персональных данных. – СПб: Университет ИТМО, 2016. – 133 с.

Учебное пособие разработано для методической помощи бакалаврам, обучающимся по направлению подготовки «Информационная безопасность» (ГОС-10.03.01). В учебном пособии рассматриваются требования нормативных правовых актов, стандартов, ведомственных документов по защите персональных данных, а также принципы и рекомендации по разработке ОРД, регламентирующих обработку персональных данных в ИСПДн органов государственной власти, муниципальных образованиях и предприятий. Учебное пособие может быть рекомендовано бакалаврам, обучающимся по направлению подготовки «Информационная безопасность» (ГОС-10.03.01), для подготовки и проведения практических занятий по дисциплине «Защита информационных систем персональных данных» (Б 3.2.13), руководителям и специалистам информационных, юридических и кадровых служб, IT подразделений и подразделений по технической защите информации.

Рекомендовано к печати Советом факультета информационной безопасности и компьютерных технологий (протокол № 3 от 30.03.2016 г.).

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

№ п/п	СОДЕРЖАНИЕ	Стр
1	Обозначения и сокращения.	5
2	Определения.	5
3	1. Основные принципы формирования организационно-распорядительных документов по защите персональных данных органов государственной власти, муниципальных образований и предприятий.	12
4	2. Рекомендации по получению исходных данных для разработки организационно-распорядительных документов по защите персональных данных органов государственной власти, муниципальных образований и предприятий.	15
5	3. Требования и рекомендации по перечню и содержанию организационно-распорядительных документов по защите персональных данных органов государственной власти, муниципальных образований и предприятий.	34
6	4. Требования и рекомендации по разработке документов по технической защите информации в информационных системах персональных данных.	43
7	5. Рекомендации по подготовке органов государственной власти, муниципальных образований и предприятий к проведению контроля и надзора за выполнением требований нормативных правовых актов Российской Федерации по защите персональных данных.	51
8	Приложение А. Перечень нормативных правовых актов и нормативно – методических документов по защите персональных данных.	60
9	Приложение Б. Типовые образцы анкет для проведения аудита (внутренней проверки) оператора персональных данных.	65
10	Приложение В. Процессы обработки оператором персональных данных «ПРИЕМ НА РАБОТУ», «УВОЛЬНЕНИЕ».	71
11	Приложение Г. Примерный перечень организационно-распорядительных, проектных и эксплуатационных документов на ИСПДн по обработке и защите персональных данных учреждения.	78
12	Приложение Д. Типовой образец «Положения об обработке персональных данных».	82
13	Приложение Е. Типовой образец «Положения по организации и проведения работ по обеспечению безопасности персональных данных».	90
14	Приложение Ж. Типовая должностная инструкция ответственного за организацию обработки персональных данных.	97

15	Приложение З. Типовое обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним контракта, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей.	99
16	Приложение И. Типовая форма согласия на обработку персональных данных.	100
17	Приложение К. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.	105
18	Приложение Л. Типовая инструкция о порядке доступа работников в помещения, в которых ведется обработка персональных данных.	107
19	Приложение М. Типовое положение об особенностях и правилах обработки персональных данных, осуществляемой без использования средств автоматизации.	109
20	Приложение Н. Типовой план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных.	112
21	Приложение О. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.	118
22	Приложение П. Перечень основных задач в области обеспечения защиты персональных данных и прогнозируемая оценка их трудоемкости без использования средств автоматизации.	121
23	Литература	133

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ:

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИС - информационная система
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ОРД - организационно-распорядительные документы
ОГВ и МСУ – органы государственной власти и местного самоуправления
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
РОСКОМНАДЗОР - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
САЗ – система анализа защищенности
СЗИ – средства (система) защиты информации
СЗПДн – система (подсистема) защиты персональных данных
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных
ФСТЭК России – Федеральная служба по техническому и экспортному контролю России
ФСБ России – Федеральная служба безопасности России
ФЗ – федеральный закон

ОПРЕДЕЛЕНИЯ:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.
Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование,

копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Документация (комплект документов) по технической защите информации на объекте информатизации - объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по назначению и сфере действия, и регламентирующих деятельность по технической защите информации на объекте информатизации.

Доступность - свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Доступ к информации – возможность получения информации и ее использования.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность - свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

Целостность - неизменность информации в процессе ее передачи или хранения.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию,

оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемые информационные ресурсы - информационные ресурсы, яв-ляющиеся предметом собственности и подлежащие защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информационных ресурсов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и / или выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила

разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записи ключей и атрибутов доступа (паролей) на бумажные носители и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или блокировать аппаратные средства.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи,

звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1 ОСНОВНЫЕ ПРИНЦИПЫ ФОРМИРОВАНИЯ ОРГАНИЗАЦИОННО - РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ

1.1 Общие положения

1.1.1 Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных (ПДн), а также определяющие цели обработки ПДн, их состав, действия (операции), совершаемые с ПДн, в соответствии с ФЗ № 152-ФЗ «О персональных данных», являются операторами ПДн.

В соответствии с требованиями ст.18.1 указанного ФЗ оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ и принятыми в соответствии с ним нормативными правовыми актами. К такой мере, в частности, относится документирование управленческой деятельности в отношении обработки и защиты ПДн.

1.1.2 Документирование управленческой деятельности операторов ПДн — это совокупность, выполняемых согласно определенным правилам действий, по записи и оформлению соответствующей информации на материальных носителях в виде бумажных или электронных документов. На основе нормативных правовых актов, руководящих и нормативных документов в области ПДн операторы ПДн разрабатывают локальные акты, а также внутренние организационно-распорядительные, нормативно-методические и иные документы, уточняющие порядок осуществления деятельности по обеспечению потребностей в документированной информации с учетом конкретных условий функционирования и особенностей управления процессами обработки ПДн.

1.1.3 В настоящее время общая регламентация делопроизводства осуществляется на основе следующих нормативных актов и документов [1-9]:

- Государственная система документационного обеспечения управления (ГСДОУ).
- Государственный стандарт РФ ГОСТ Р5П41-98 «Делопроизводство и архивное дело. Термины и определения».

- Государственный стандарт РФ ГОСТ Р6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».
- Типовая инструкция по делопроизводству в федеральных органах исполнительной власти (2000 г.).
- Общероссийский классификатор управленческой документации (ОКУД) ОК 011-93 (1993 г., с изм.. и доп. 1999-2002 гг.).
- Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления (1995 г.).
- Основные правила работы архивов организаций (2002 г.).
- Методические рекомендации ВНИИДАДФАС РФ «Унификация текстов управленческих документов» (1998 г.)
- Методические рекомендации ВНИИДЛДФАС РФ «Организационно - распорядительная документация. Требования к оформлению документов» (2003 г.).
- Методические рекомендации ВНИИДАД ФАС РФ «Ведение делопроизводства в организации» (2004 г.).

1.1.4 Методические рекомендации «Организационно-распорядительная документация. Требования к оформлению документов» предназначены для руководства в процессе осуществления деятельности по оптимизации состава ОРД с учетом положений ГОСТ Р6.30-2003. В документе содержится краткая характеристика некоторых новых терминов и определений, используемых в делопроизводстве, а также методические рекомендации, но основным вопросам, касающимся оформления ОРД учреждения (предприятия).

1.1.5 Документы составляют от юридического лица (органа государственной власти, местного самоуправления, предприятия), ответственного за их разработку. Текст документа должен отвечать следующим общим требованиям:

- соответствовать действующим нормативным правовым, организационно-распорядительным и нормативным документам в области защиты информации и иметь ссылки на них (при необходимости);
- содержать конкретные и обоснованные требования, рекомендации (предложения) и решения, основанные на фактах, обоснованных теоретическими положениями и расчетными методиками;
- состоять из кратко, четко, в логической последовательности изложенных формулировок, не допускающих различных толкований.

Составление и оформление документа должно соответствовать типовой форме, установленной для данной разновидности документа.

1.1.6 При оформлении документов применяют формат А4. Текст печатают через полтора или два межстрочных интервала. Реквизиты документа отделяют друг от друга двумя – тремя межстрочными интервалами. Реквизиты, состоящие из нескольких строк, печатают через один

межстрочный интервал. Наименование вида документа печатают прописными буквами.
Оформление тестовых документов должно соответствовать требованиям ГОСТ 2.106.
Номера страниц должны быть поставлены в правом верхнем или нижнем углу поля листа арабскими цифрами без слова «страница (стр.)» и знака препинания. Сокращение русских слов и словосочетаний – в соответствии с требованиями ГОСТ 7.12. Оформление иллюстраций (рисунков, чертежей, схем, графиков, диаграмм, карт) должно соответствовать требованиям ГОСТ 2.105, ГОСТ2.106, ГОСТ 3.1105, ГОСТ 2.125.

1.1.7 При разработке ОРД, определяющих порядок обработки и защиты ПДн операторам рекомендуется применять иерархию документов, представленную на рис. 1.
Положения – документы, определяющие общие подходы и требования по обработке и защите персональных данных оператора персональных данных.
Регламенты – документы, устанавливающие порядок проведения мероприятий по обработке и защите персональных данных.

Рисунок 1. Иерархия организационно-распорядительной документации

Инструкции – документы, содержащие детализированные правила и указания по осуществлению определенных операций по обработке и защите персональных данных, изложенных в положениях и регламентах.
Учетные документы – документы, содержащие записи о мероприятиях и результатах деятельности по обработке и защите персональных данных. К учетным документам относятся, например:

- журналы;

- реестры;
- перечни;
- протоколы;
- акты;
- листы ознакомления.

1.1.9 С целью унификации форматов документов рекомендуется придерживаться следующей структуры разделов при разработке ОРД:

Цель документа – в данном разделе рекомендуется указывать цели и назначение документа;

Область применения документа – в данном разделе рекомендуется указывать перечень лиц, на которых распространяется действие данного документа;

Основные положения документа – в данном разделе размещается основная содержательная часть документа;

Лист регистрации изменений документа – данный раздел предназначен для фиксации любых изменений, вносимых в текст данного документа;

Лист ознакомления с документом – данный раздел предназначен для регистрации ознакомления пользователей данного документа с его содержанием.

1.1.10 Порядок разработки и ввода в действие документации.

Все документы, регламентирующие порядок обработки и защиты ПДн, операторам следует разрабатывать в соответствии с требованиями нормативных правовых актов, руководящих и нормативных документов, перечень которых приведен в Приложении А, и вводить в действие правовыми актами и руководящими документами оператора ПДн.

Каждый работник, который допущен к обработке ПДн, должен быть ознакомлен с ОРД, регламентирующими порядок обработки и защиты ПДн, в части, его касающейся, под роспись.

2 РЕКОМЕНДАЦИИ ПО ПОЛУЧЕНИЮ ИСХОДНЫХ ДАННЫХ ДЛЯ РАЗРАБОТКИ ОРГАНИЗАЦИОННО – РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ

2.1 Получение исходных данных для разработки ОРД по защите ПДн операторам ПДн рекомендуется проводить на основе контроля соответствия обработки ПДн федеральному закону РФ от 27.06.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам в соответствии с ГОСТ Р ИСО/МЭК 27001-2006. Необходимость проведения контроля соответствия обработки ПДн, обрабатываемых в ИСПДн Федеральному закону РФ от 27.07.2006 г.

№152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам, обусловлена требованием ст. 18.1 вышеуказанного закона. Указанный контроль оператор ПДн может проводить в форме аудита или внутренней проверки [10].

2.2 Нормативно-методической базой для проведения контроля соответствия обработки ПДн федеральному закону РФ от 27.06.2006 № 152-ФЗ «О персональных данных» являются нормативные правовые акты, руководящие и нормативно – методические документы по защите персональных данных, перечень которых приведен в Приложении А.

2.3 Целью контроля является плановая оценка состояния системы безопасности ПДн, позволяющая не только выявить недостатки и ее несоответствия требованиям нормативных правовых актов, но и разработать, а также реализовать мероприятия по их устранению.

2.4 В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012 г. № 1119, контроль за выполнением требований по защите ПДн организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

2.5 Контроль соответствия обработки ПДн, обрабатываемых оператором ПДн федеральному закону РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» и, принятых в соответствии с ним, нормативным правовым актам представляет собой обследование существующих процессов обработки ПДн и анализ их соответствия требованиям действующего законодательства. Главная задача контроля - обратить внимание руководителя организации – оператора персональных данных, на проблемные участки и предложить план совершенствования работы.

Контроль позволяет:

- выполнить прямое требование ст.18.1 Федерального закона «О персональных данных»;

- определить существующие угрозы ПДн;

- оценить степень соответствия процессов обработки ПДн требованиям законодательства РФ;

- оценить существующие риски для организации в случае невыполнения требований нормативных правовых актов и руководящих документов регуляторов по защите ПДн;

- получить рекомендации по приведению процессов обработки ПДн в соответствие с действующим законодательством РФ;

- определить меры, необходимые для приведения процессов обработки ПДн в соответствие с требованиями законодательства РФ по защите ПДн;

- оценить и минимизировать затраты на приведение обработки ПДн в соответствие с требованиями законодательства РФ по защите ПДн;

- получить информацию, необходимую для дальнейших работ по созданию (модернизации) системы защиты ПДн и разработки ОРД по их защите.

2.6 Работы по контролю состояния безопасности ПДн рекомендуется проводить в соответствии с этапами проведения комплексного аудита информационной безопасности, включающего:

- инициирование процедуры контроля;

- сбор информации;

- анализ данных контроля;

- выработка рекомендаций по устранению недостатков;

- подготовка отчета о результатах контроля.

2.7 Для проведения контроля оператора ПДн, на предмет наличия/отсутствия признаков работы с ПДн рекомендуется провести моделирование его деятельности по обработке ПДн. Моделирование таких процессов может включать:

- получение исходных данных и анализ организационной структуры органа власти, организации (предприятия), а также функций структурных подразделений, на которые возложена работа с ПДн. Основными методами сбора информации в ходе проверки являются рассмотрение нормативных правовых актов и ОРД, определяющих цели, задачи, порядок выполнения работ, связанных с обработкой ПДн, собеседование членов комиссии с работниками, осуществляющими обработку ПДн, заполнение опросных

листов (анкет) и анализ предоставленных документов. Примерные варианты указанных анкет приведены в Приложении Б.

- выявление процессов деятельности оператора по работе с ПДн, и/или процессов управления, затрагивающих вопросы обработки ПДн. Типовыми процессами обработки ПДн являются: «ПРИЕМ НА РАБОТУ», «УВОЛЬНЕНИЕ», «ЗАРАБОТНАЯ ПЛАТА», «ОТПУСКА», «КОМАНДИРОВКИ» и т.п. Примеры описания процессов обработки ПДн «ПРИЕМ НА РАБОТУ» и «УВОЛЬНЕНИЕ» приведены в Приложении В.

- подготовку отчета о проверке с описанием процессов деятельности оператора по работе с ПДн и оценкой степени соответствия процессов обработки ПДн требованиям законодательства РФ, в том числе, наличие (отсутствие) необходимых ОРД, определяющих порядок обработки и защиты ПДн и их соответствие нормативным правовым актам и требованиям регуляторов в области ПДн.

Для анализа ОРД оператора по работе с ПДн рекомендуется:

- построить описательную модель нормативного правового обеспечения деятельности оператора по обработке ПДн, учитывающей специфику деятельности оператора. В качестве такой модели может рассматриваться перечень ОРД, необходимых оператору для выполнения требований нормативных правовых актов, стандартов, руководящих и методических документов регуляторов: Роскомнадзора, ФСТЭК и ФСБ России, а также, при наличии, и отраслевых рекомендаций по их форме и содержанию.

- выявить локальные правовые акты и ОРД оператора, регулирующие (затрагивающие) вопросы обработки и защиты ПДн. Провести анализ их формы и содержания.

- подготовить раздел отчета о проверке с описанием состояния обработки ПДн и оценкой соответствия ОРД оператора установленным требованиям, а также с предложениями по изменению и/или дополнению уже существующих ОРД, регулирующих вопросы обработки и защиты ПДн.

2.8.Для оценки состояния организации обработки и обеспечения безопасности ПДн необходимо ответить на следующие вопросы:

1. Обрабатываются ли оператором ПДн.

2. Какие ИС используются для обработки ПДн (ГИС, МИС, иные).

3. Каков вид обработки ПДн используется оператором: автоматизированная, смешанная или без использования средств автоматизации.

4. Какие ОРД регламентируют порядок обработки и защиты ПДн. Соответствуют ли перечень ОРД и разработанные документы требованиям законодательства РФ, организации обработки и защиты ПДн.

5. Зарегистрирована ли организация (предприятие) в качестве оператора ПДн (в случаях определенных ФЗ № 152-ФЗ "О персональных данных»). Кто выступает субъектами обработки ПДн.

6. Получены ли, в установленных нормативными правовыми актами случаях, согласия субъектов ПДн на обработку их ПДн в письменной форме.

7. Соответствуют ли категории ПДн, на которые получено согласие от субъектов ПДн на их обработку, фактическим категориям ПДн.

8. Соответствует ли количество согласий на обработку ПДн количеству субъектов ПДн, которые должны давать такие согласия.

9. Удовлетворяет ли форма письменного согласия на обработку ПДн субъекта обработки требованиям ФЗ №152-ФЗ "О персональных данных".

10. Цели, основания и установленные сроки обработки ПДн.

11. Какое количество записей о субъектах ПДн обрабатывается в ИСПДн. Какое количество записей о субъектах ПДн обрабатывается без использования средств автоматизации.

12. Обрабатываются ли ПДн граждан, не связанных с оператором трудовыми отношениями. Если да, то какие категории ПДн работников и других субъектов ПДн обрабатываются оператором.

13. Какая информация о работниках и других субъектах ПДн обрабатывается оператором. Существует ли утвержденный перечень ПДн. Есть ли необходимость и правовые основания обработки всех категорий ПДн.

14. Установлены ли классы ИСПДн (для ГИС и МИС) и уровни защищенности персональных данных (для иных ИС) и требования к их защите.

15. Между какими ИС циркулируют ПДн. Какие категории ПДн передаются по каналам связи. Каким образом обеспечивается защита каналов связи и циркулирующих по этим каналам ПДн.

16. Проведены ли мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн.

17. Назначены ли работники или подразделение, ответственные за обеспечение обработки и безопасности ПДн, в установленных нормативными документами случаях.

18. Проинформированы ли лица, обрабатывающие ПДн, о факте их обработки, категориях ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами ФОИВ, органов исполнительной власти субъектов РФ, а также локальными правовыми актами и ОРД оператора. Допущены ли приказом руководителя указанные лица к обработке ПДн.

19. Обособлены ли ПДн от иной информации. Фиксируются ли на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы.

20. Есть ли письменные расписки об ознакомлении с ОРД, регламентирующими обработку и защиту ПДн. Соответствует ли количество расписок количеству лиц, обрабатывающих ПДн.

21. Есть ли у оператора ПДн типовые формы документов, характер информации в которых предполагает (или допускает) включение в них ПДн.

22. Ведутся ли журналы (реестры, книги), содержащие ПДн, необходимые для однократного пропуска субъекта ПДн на территорию оператора.

23. Осуществляется ли обработка ПДн таким образом, чтобы в отношении каждой категории ПДн можно было определить места их хранения (материальные носители) и установить перечень лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ. Если да, то какие мероприятия для этого проводятся. Если не проводятся, то по какой причине.

24. Соблюдаются ли при хранении материальных носителей ПДн условия, обеспечивающие их сохранность и исключающие несанкционированный к ним доступ. Как обеспечиваются такие условия. Какие должностные лица

ответственны за реализацию указанных мер и каким документом предусмотрена ответственность.

25. Введены ли в действие локальными правовыми актами (приказами) оператора ОРД, регламентирующие порядок обработки и обеспечения безопасности ПДн.

26. Введен ли режим обеспечения безопасности ПДн. Если да, то ограничен ли доступ к ним. Производится ли учет лиц, получивших доступ к ПДн, и (или) лиц, которым такая информация была предоставлена или передана.

27. Регулируются ли отношения по использованию ПДн работников на основании трудовых договоров (согласия на обработку) и с контрагентами (на основании гражданско-правовых договоров).

28. Есть ли в организации (предприятии) ПДн, переданные контрагентами. Если есть, то на каком основании передана данная информация. Какие меры по ее охране предусмотрены контрагентом. Какие меры принимаются для защиты информации контрагентов. Достаточны ли эти меры. Соответствуют ли они уровню защиты, оговоренному всеми сторонами.

2.9 Чтобы установить степень соответствия защиты ПДн при их обработке в ИСПДн требованиям нормативных правовых актов и руководящих документов регуляторов, целесообразно ответить на вопросы:

1. Какие ОРД и документы на систему защиты ИСПДн оператора регулируют безопасность ПДн при их обработке в ИСПДн.

2. Контролируется ли порядок допуска работников к обработке ПДн в ИСПДн и без использования средств автоматизации.

3. Каким образом контролируется деятельность работников при обработке ПДн.

4. На основании каких документов предоставляется доступ к ИСПДн контрагентам.

5. Каким образом контролируется деятельность контрагентов в ИСПДн.

6. Существует ли реальная необходимость доступа контрагентов к ПДн, есть ли возможность без ущерба для деятельности оператора отключить контрагентов от ИСПДн.

7. Насколько политика взаимодействия ИСПДн оператора и контрагентов (настройки межсетевого экрана, граничного маршрутизатора и т.п.) соответствует реальным потребностям в межсетевом взаимодействии. Есть ли необходимость дополнить или изменить правила взаимодействия.

8. Каков порядок получения доступа к ресурсам ИСПДн работникам оператора и работникам контрагентов.

9. Применяются ли дополнительные программные и аппаратные средства для защиты ИСПДн.

2.10 При проведении инвентаризации ПДн необходимо установить законность обработки персональных данных.

В случае необходимости обработки ПДн правовыми основаниями для их обработки могут являться:

- законы субъектов РФ, постановления Правительства РФ, субъектов РФ, иные нормативные правовые акты;

- перечень соответствующих кодов ОКВЭД в свидетельстве о государственной регистрации юридического лица;

- соответствующие виду деятельности пункты в «Положении…», «Уставе…» организации (предприятия);

- иные нормативные правовые акты органов власти, организаций, касающиеся обработки ПДн.

При отсутствии соответствующих нормативных правовых актов и соответствующих статей в учредительных и ОРД оператора ПДн необходимо подготовить рекомендации по их разработке.

2.11 В случае, если по результатам контроля будет установлено, что обработка ПДн осуществляется без использования средств автоматизации, необходимо руководствоваться требованиями постановления Правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.12 При выявлении материальных носителей, на которых осуществляется запись биометрических ПДн, а также осуществляется хранение биометрических ПДн вне ИСПДн, необходимо руководствоваться «Требованиями к материальным носителям биометрических

персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» утвержденными постановлением Правительства Российской Федерации от 6.07.2008 года N 512.

2.13 В ходе контроля процессов автоматизированной обработки ПДн в ИСПДн необходимо определить их тип для определения требований нормативных правовых актов и нормативно - методических документов регуляторов по защите ПДн.

В соответствии со ст. 13 ФЗ №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» информационные системы делятся на:

1) государственные информационные системы (ГИС) - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы (МИС), созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2.14 Признаками ГИС (МИС) являются:

- основания ее создания: федеральные законы РФ, законы субъектов РФ, правовые акты государственных органов РФ;

- цели создания ГИС (МИС): реализация полномочий государственных органов, обеспечение между ними обмена информацией, а также иных, установленными федеральными законами целей;

- источники финансирования при создании ГИС (МИС): федеральный бюджет, государственные внебюджетные фонды.

При отсутствии указанных признаков ИСПДн относится к иным информационным системам, на которые не распространяются требования по защите информации для ГИС (МИС).

2.15 В ходе контроля ИСПДн необходимо провести:

- анализ информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, входящих в состав ИСПДн,

- анализ технической и эксплуатационной документации ИСПДн и ее соответствия требованиям нормативно-методических документов по защите ПДн с целью выявления объектов и субъектов доступа, правил разграничения доступа, изучения информационных потоков в ИСПДн, определения состава используемых для обработки информации средств вычислительной техники и средств защиты информации;

- испытания отдельных технических и программных средств ИСПДн, средств и системы защиты информации в целом на соответствие установленным требованиям;

- испытания защищенности ИСПДн в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации.

2.16 При проведении оценки защищенности ИСПДн объектами оценки могут быть:

- организационно - распорядительная, конструкторская и эксплуатационная документация на ИСПДн, регламентирующая защиту информации в ИСПДн;

- программно – технические элементы ИСПДн;

- ИСПДн в целом.

2.17 Исходными данными для анализа организационно – распорядительной, конструкторской и эксплуатационной документации на ИСПДн являются:

- техническое задание (формуляр) на ИСПДн;

- технический проект на ИСПДн (СЗИ ИСПДН);

- акт классификации (для ГИС и МИС);

- акт определения уровня защищенности ПДн для иных ИСПДн;

- приказы, указания, решения, инструкции, связанные с проектированием и эксплуатацией ИСПДн;

- сертификаты на используемые средства защиты, аттестат соответствия по требованиям безопасности на ИСПДн (для ГИС и МИС), а при наличии установленных требований, для иных ИСПДн;

- ОРД разрешительной системы доступа персонала к защищаемым ресурсам ИСПДн;

- перечень и категории ПДн, обрабатываемых в ИСПДн.

В процессе анализа исходных данных осуществляется сбор информации о структуре ИСПДн, распределении адресного пространства, используемом аппаратном и программном обеспечении, информационных потоках, настройках СЗИ, схемах аутентификации, пропускной способности каналов между компонентами ИСПДн и т.д.

Полученная информация в дальнейшем используется для анализа организации и технологии обработки и защиты информации в ИСПДн, для выбора объектов и средств защиты.

2.18 Контроль организации работ по защите информации при ее обработке в ИСПДн осуществляется в следующем объеме:

1. Анализ функциональных связей подразделений при обработке ПДн в ИСПДн.

2. Инвентаризации информационных ресурсов с ПДн.

3. Анализ структуры и технологического процесса обработки информации в ИСПДн.

4. Проверка фактического соответствия состава и структуры программно-технических средств ИСПДн конструкторской и эксплуатационной документации.

5. Проверка состояния организации работ и выполнения организационно-технических требований по защите информации.

2.19 На основе анализа полученных исходных данных формируются:

- перечень объектов доступа (терминалы, ЭВМ, узлы сети, каналы связи, внешние устройства ЭВМ (в том числе межсетевые экраны, маршрутизирующее оборудование, коммутирующее оборудование, сервера удаленного доступа, сервера управления доступом, УБП, устройства VPN и т.д.), программы, тома, каталоги, файлы, записи, поля записей);

- перечень субъектов доступа;

- пользователи и процессы (программы пользователей), имеющие возможность доступа к объектам защиты штатными средствами ИСПДн;

- лица, действующие от имени уполномоченного пользователя и подчиненные всем правилам политики безопасности (например, процессы UNIX);

- лица, действующие как особый функциональный процесс, который может, в свою очередь, действовать от имени многих пользователей (например, функции, которые характерны для архитектуры клиент/сервер);

- перечень штатных средств доступа к информации в ИСПДн;

- перечень используемых в ИСПДн средств защиты информации;

- описание информационных потоков, включая таблицы маршрутизации для межсетевых экранов и маршрутизаторов, таблицы маршрутизации для выделенных виртуальный частных сетей, схемы подключения к коммутирующему оборудованию с указанием принадлежности к виртуальной вычислительной сети и/или виртуальной частной сети, перечень телефонных номеров, используемых для организации удаленного доступа, перечень рабочих мест (с указанием физических и логических сегментов подключения), с которых осуществляется удаленное управление;

- описание реализованных правил разграничения доступа.

2.20 В ходе контроля проверяется соответствие описания технологического процесса обработки и хранения защищаемой информации реальному процессу с анализом разрешенных и запрещенных связей между субъектами и объектами доступа и привязкой к конкретным СВТ и штатному персоналу. По результатам контроля уточняется схема процесса обработки ПДн с привязкой к конкретным средствам обработки и штатному персоналу.

2.21 Проверка соответствия состава и структуры программно-технических средств ИСПДн проводится экспертно-документальным методом в следующей последовательности:

1. Производится проверка полноты и достаточности представленных документов и соответствия их содержания требованиям стандартов и иных руководящих документов по безопасности информации.

2. Проверяется соответствие сведений (типов, заводских номеров, мест установки и т.д.), приведенных в:

- перечне технических и программных средств, а также средств защиты информации, входящих в ИСПДн;

- сертификатах соответствия требованиям по безопасности информации на программные и технические средства защиты информации.

Проверка считается успешной, если представленная документация соответствует требуемому перечню, не содержит противоречивых сведений и оформлена в соответствии с требованиями стандартов и руководящих документов, а номенклатура, структура программно-технических средств ИСПДн и их размещение соответствуют сведениям, изложенным в документации на ИСПДн и средства защиты информации.

2.22 Выявление информационных ресурсов ИСПДн рекомендуется проводить на основе их инвентаризации. На основании инвентаризации информационных ресурсов и состава ПДн должен быть сделан вывод о категории и перечне обрабатываемых ПДн.

2.23 Проверка состояния организации работ и выполнения требований по защите ПДн осуществляется экспертно-документальным методом в следующей последовательности:

- проверка наличия оформленных разрешений на допуск персонала к обработке ПДн и соответствия практики их допуска.

- проверка установленного порядка хранения и уничтожения носителей информации.

- проверка учета и маркирования носителей информации.

- оценка соответствия разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным СВТ и штатному персоналу разрешительной системы доступа персонала к защищаемым ПДн на всех этапах их обработки в ИСПДн.

Проверка считается успешной, если организация работ соответствует требованиям по безопасности информации.

2.24 Проверка ИСПДн на соответствие требованиям по защите информации включает в себя:

- выбор инструментальных средств и методики испытаний в соответствии с конфигурацией ИСПДн;

- идентификацию применяемых в ИСПДн сертифицированных средств защиты информации;

- проверку подсистемы управления доступом;

- проверку подсистемы регистрации и учета;

- проверку криптографической подсистемы;

- проверку подсистемы обеспечения целостности.

Проверки осуществляются с использованием выбранных средств контроля защищенности и анализа, а также в соответствии с методикой испытаний, согласованной с организацией - оператором ИСПДн.

Исследуя физическую, логическую и принципиальную схемы корпоративной или локальной сети (информационное пространство организации), следует обратить внимание на то, сколько имеется точек соприкосновения с другими сетями, для чего эти контакты нужны, какие правила настроены на межсетевых экранах и т.д. Необходим постоянный контроль с целью устранять периодически возникающие каналы утечки информации или направления неэффективной траты средств на программное обеспечение.

Получив ответы на поставленные вопросы, представляется возможным достаточно полно оценить состояние системы обеспечения безопасности ПДн в организации и разработать мероприятия для устранения выявленных нарушений.

2.25 Для разработки ОРД по защите ПДн рекомендуется рассмотреть следующие направления:

- защита объектов, входящих в состав ИСПДн;

- защита процессов, процедур и программ обработки информации;

- защита каналов связи;

- управление системой защиты информации.

2.26 По результатам проведения контроля составляется отчет, который должен содержать описание текущего состояния режимов обработки и

защиты ПДн с оценкой соответствия их обработки ФЗ от 27.07.2006 г. №152 - ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам. В отчете указывается место и адрес организации, где проведена проверка, в том числе в филиалах (при их наличии). Отчет должен быть утвержден руководителем организации - оператора ПДн и согласован с руководителями подразделений или должностными лицами, ответственными за обработку и обеспечение безопасности ПДн.

2.27 В отчете рекомендуется привести:

- сведения об обрабатываемых в организации ПДн, целях и основаниях их обработки, документах, в которых они содержатся, лицах, осуществляющих такую обработку, и др.;

- перечень и описания процессов решения уставных и бизнес-задач, в ходе которых обрабатываются ПДн;

- перечень и описания ИСПДн, в которых осуществляется обработка ПДн;

- оценка состояния системы обеспечения безопасности ПДн;

- перечень выявленных несоответствий нормативным правовым актам, руководящим и методическим документам по защите ПДн и рекомендации по их устранению.

2.28 При описании ИСПДн она может быть представлена как:

1. Автоматизированное рабочее место, если вся обработка ПДн производится в рамках одного рабочего места.

2. Локальная информационная система, если вся обработка ПДн производится в рамках одной локальной вычислительной сети.

3. Распределенная информационная система, если обработка ПДн производится в рамках комплекса автоматизированных рабочих мест и / или локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа. В такой ИСПДн ее элементы разнесены территориально, например, в ИСПДн включена сеть филиала, и связь между территориально удаленными элементами осуществляется по каналам сетей общего пользования и / или международного информационного обмена.

2.29 Для каждой ИСПДн должны быть определены:

- перечень обрабатываемых ПДн;

- состав объектов защиты**;**

- объем записей ПДн;

- тип ИСПДн по категории ПДн.

В соответствии с Постановлением Правительства РФ от 1.11.2012 г. №1119 определены следующие типы ИСПДн:

1. ИСПДн является информационной системой, обрабатывающей специальные категории ПДн, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн.
2. ИСПДн является информационной системой, обрабатывающей биометрические ПДн, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям ПДн.
3. ИСПДн является информационной системой, обрабатывающей общедоступные ПДн, если в ней обрабатываются ПДн субъектов персональных данных, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».
4. ИСПДн является информационной системой, обрабатывающей иные категории ПДн, если в ней не обрабатываются персональные данные, указанные в п.п.1-3.
5. ИСПДн является информационной системой, обрабатывающей ПДн сотрудников оператора, если в ней обрабатываются ПДн только указанных сотрудников. В остальных случаях ИСПДн является информационной системой, обрабатывающей ПДн субъектов персональных данных, не являющихся сотрудниками оператора.

2.30 Для каждой ИСПДн должна быть нарисована конфигурация ИСПДн раскрывающая схематичное взаиморасположение элементов системы. Конфигурация может быть нарисована в любом графическом редакторе. Условные обозначения элементов ИСПДн приведены на рисунке 2.

Пример структуры и состава ИСПДн, основным элементом которой является сервер баз данных ORACLE показан на рис. 3.

В соответствии с приведенным примером к БД ORACLE осуществляют доступ операторы и разработчики ИСПДн, авторизуясь под своими доменными учетными записями в домене Domain. К БД ORACLE также имеют удаленный доступ операторы филиала. Удаленный доступ организуется по сети общего пользования и международного обмена – Интернету. Операторы филиала вначале авторизуются в своем домене Domain-F, подключаются по сети Интернет к терминальному серверу Terminal Server, авторизуясь на нем под учетной записью основного домена Domain. Затем операторы филиала авторизуются в БД ORACLE.

2.31 Для каждой ИСПДн должно быть нарисовано территориальное расположение ИСПДн относительно контролируемой зоны (КЗ) организации оператора ПДн, и описана структура обработки ПДн. Структура обработки ПДн должна включать всю последовательность шагов по их вводу, обработке и передаче в другие ИСПДн. Структура обработки ПДн может быть описана как в текстовом, так и в графическом виде.

2.32 Для каждой ИСПДн должны быть определены группы пользователей участвующие в обработке ПДн. Для всех групп должен быть определен перечень прав и уровень доступа в соответствии с «Положением о разрешительной системе доступа» в «Матрице доступа».

Для каждой ИСПДн должен быть определен список пользователей - работников оператора, участвующих в обработке ПДн.

2.33 Для каждой ИСПДн должны быть определены типы угроз и актуальные угрозы безопасности ПДн в соответствии с НМД ФСТЭК и ФСБ России. Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИСПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

В соответствии с Постановлением Правительства РФ от 1.11.2012 г. № 1119 угрозы ИСПДн делятся на 3 типа.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных

(не декларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

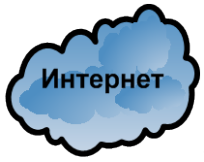
– Группа пользователей ИСПДн.

– АРМ пользователей ИСПДн.

– Сервер, например, почтовый, файловый, proxy сервер, сервер приложений.

– Сервер баз данных.

– Межсетевой экран.



– Сеть общего доступа и / или международного обмена, например, Интернет.

– Направление информационного взаимодействия.

Рис. 2 Условные обозначения элементов ИСПДн

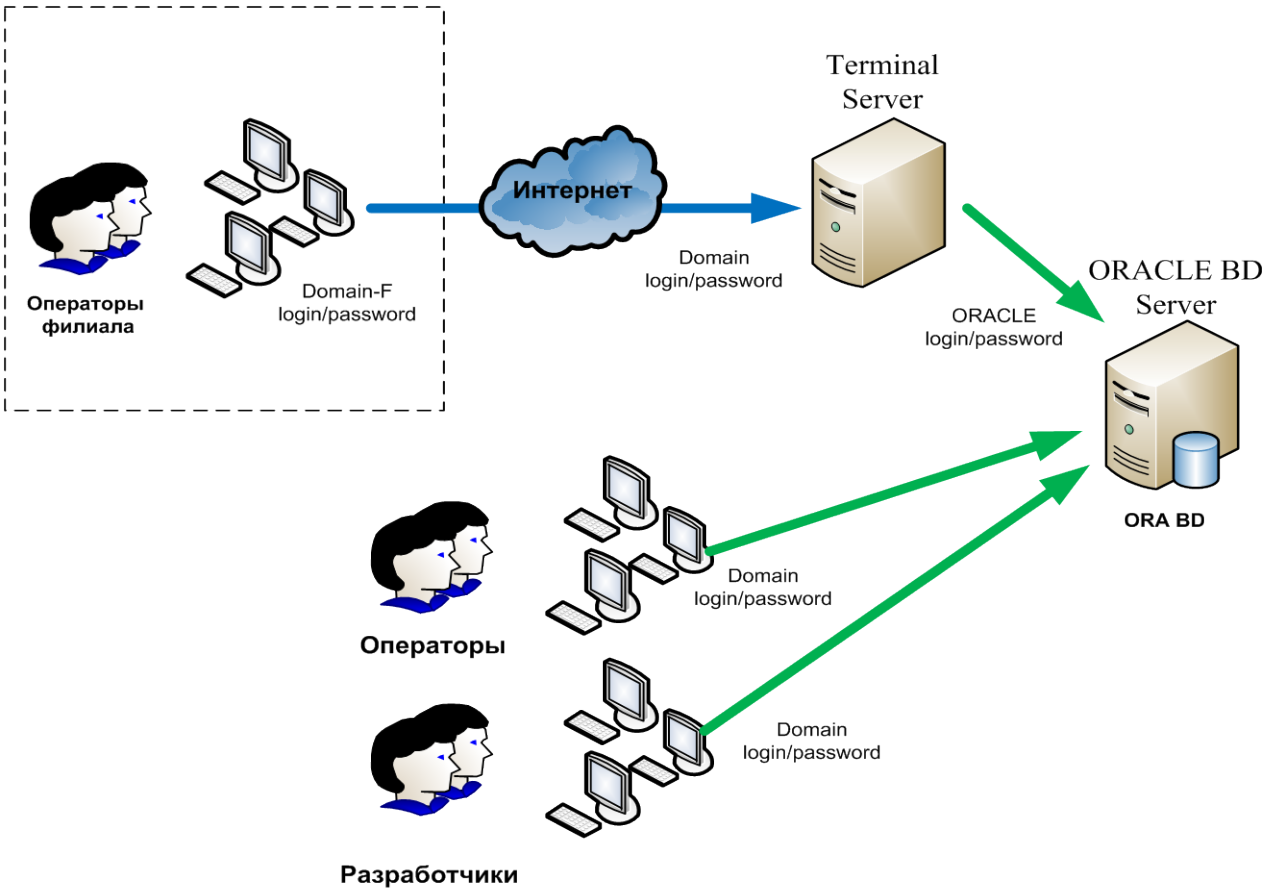


Рис.3 Пример структуры и состава ИСПДн

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием не документированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием не документированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности ПДн, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 181 ФЗ «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 ФЗ «О персональных данных».

2.34 Для каждой ИСПДн должен быть определен уровень защищенности ПДн. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных в соответствии с требованиями Правительства РФ от 1.11.2012 г. №1119.

Для каждой ИСПДн должны быть определены и описаны все меры защиты, включая использование как штатного ПО (операционные системы и программы), так и специально установленных систем безопасности. Для оценки и описания характеристик имеющихся технических мер защиты необходимо использовать материалы Технического задания и Технического проекта на ИСПДн.

2.35 Для каждой ИСПДн должны быть определены имеющиеся организационные меры защиты ПДн и разработаны предложения в план мероприятий по защите ПДн. Разработку указанных предложений необходимо провести на основе действующих нормативных правовых актов, руководящих и методических документов в области обработки и защиты ПДн.

2.36 С целью устранения нарушений, выявленных в ходе контроля, оператором ПДн могут быть приняты решения:

- привлечь к проведению работ по защите ПДн стороннюю организацию, имеющую лицензию по защите конфиденциальной информации;

- ввести в штат организации специалистов, которые будут на постоянной основе заниматься выявленными проблемами;

- наделить дополнительными обязанностями по защите ПДн должностных лиц организации – оператора ПДн.

3 ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ПЕРЕЧНЮ И СОДЕРЖАНИЮ ОРГАНИЗАЦИОННО – РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ

3.1 Общие положения.

3.1.1 В соответствии с требованиями ФЗ "О персональных данных" (ст.18.1) оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

К таким мерам могут, в частности, относится издание оператором, являющимся юридическим лицом, документов, определяющих:

- политику оператора в отношении обработки и защиты ПДн;

- локальных актов по вопросам обработки и защиты ПДн;

- локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ по вопросам обработки и защиты ПДн, устранение последствий таких нарушений.

3.1.2 Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн. Оператор, осуществляющий сбор ПДн с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно - телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно - телекоммуникационной сети.

3.1.3 В соответствии с разъяснениями Роскомнадзора – органа власти уполномоченного в сфере защиты прав субъектов ПДн, четкий перечень ОРД по защите ПДн в настоящее время законодательно не установлен, и форма их жестко не регламентирована, за исключением ОГВ и МСУ.

Для ОГВ и МСУ постановлением Правительства РФ от 21.03.2012 № 211 утвержден перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ №152 - ФЗ „О персональных данных“ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

В частности, перечень ОРД по защите ПДн государственного или муниципального органа должен включать в себя:

1. Правила рассмотрения запросов субъектов ПДн или их представителей.

2. Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным законом, а также принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора ПДн.

3. Правила работы с обезличенными ПДн в случае их обезличивания.

4. Перечень ИСПДн.

5. Перечни ПДн, 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.

6. Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн.

7. Должностной регламент (должностные обязанности) или должностную инструкцию ответственного за организацию обработки ПДн в государственном или муниципальном органе.

8.Типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей.

9. Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка ПДн и т.д."

3.1.4 Сборник примерных форм документов по обеспечению безопасности ПДн в исполнительных органах г. Москва опубликован в свободном доступе на сайте департамента информационных технологий г. Москвы: http://dit.mos.ru/legislation/metods/infosec/text520.html.

Перечень и сборник типовых (примерных) форм ОРД по защите информации, включающей ПДн для исполнительных органов государственной власти (ИОГВ) Санкт-Петербурга, размещен на сайте технической поддержки УТС Смольного: //support./uts.vpn (раздел «Документация).

ОРД аппарата Губернатора и Правительства Ленинградской области, как оператора ПДн, определены приказом аппарата Губернатора и Правительства Ленинградской области от 9 октября 2015 г. № 01-02/10.

3.1.5 В приложениях к приказу Росстандарта от 25.07.2013 N 249-к "О реализации требований постановления Правительства Российской Федерации от 21 марта 2012 г. N 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" определены:

1. Правила обработки ПДн, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере ПДн, а также определяющие для каждой цели обработки ПДн содержание обрабатываемых персональных данных, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Правила рассмотрения запросов субъектов ПДн или их представителей;

3. Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами;

4. Правила работы с обезличенными ПДн совместно с Перечнем должностей федеральной государственной гражданской службы Федерального агентства по техническому регулированию и метрологии, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

5. Перечень ИСПДн, обрабатываемых в Федеральном агентстве по техническому регулированию и метрологии;

6. Перечень должностей федеральной государственной гражданской службы, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн, включая доступ в информационных системах;

7. Должностная инструкция лица, ответственного за организацию ПДн;

8. Обязательство о неразглашении информации, содержащей ПДн;

9. Форма согласия федерального государственного гражданского служащего на обработку ПДн;

10. Форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн;

11. Порядок доступа служащих в помещения, в которых ведется обработка ПДн.

Для операторов ПДн, не являющихся ОГВ и МСУ, примерный перечень ОРД учреждения (предприятия) приведен в Приложении Г.

3.2 Рекомендации по содержанию документов уровня положений

3.2.1 Документы уровня положений определяют основные требования к обработке и защите персональных данных оператора персональных данных, а также ответственность и обязанности работников и ответственных лиц в части обработки и защиты персональных данных. В документах уровня положений устанавливаются требования к следующим аспектам организации обработки и обеспечения безопасности ПДн**:**

- категории субъектов ПДн, чьи данные обрабатываются;
- состав обрабатываемых ПДн, цели, сроки, правовые основания, порядок и условия их обработки;
- порядок взаимодействия с субъектами ПДн;
- порядок организации доступа лиц к обработке ПДн;
- порядок организации обмена ПДн со сторонними организациями;
- порядок организации учета и хранения носителей ПДн;
- порядок уничтожения ПДн после достижения целей обработки;
- порядок организации и меры по обеспечению безопасности ПДн, обрабатываемых оператором ПДн как с использованием средств автоматизации, так и без их использования;
- порядок проведения контрольных мероприятий и действий по их результатам;
- порядок реагирования на нарушение правил обработки и (или) обеспечения безопасности ПДн.

3.2.2 Оператору ПДн рекомендуется разработать следующий перечень положений:

1. Положение об обработке ПДн.
2. Положение об обеспечении безопасности ПДн.

3.3 Рекомендации по содержанию документов уровня регламентов

3.3.1 Документы уровня регламентов содержат описания основных процессов, связанных с реализацией требований, изложенных в документах уровня положений, с указанием ответственных, сроков исполнения, порядка отчетности и контроля.

Оператору ПДн рекомендуется ввести следующий перечень регламентов:

1. Регламент предоставления доступа к ПДн, определяющий порядок:
   - предоставления работникам доступа к ПДн, обрабатываемым как с использованием средств автоматизации, так и без их использования;
   - осуществления контроля со стороны ответственных лиц за предоставленными правами на доступ к ПДн с целью исключения возможных нарушений;
   - отзыва или пересмотра прав доступа работников в случае увольнения или изменения их должности и функциональных обязанностей;
2. Регламент реагирования на запросы субъектов ПДн, определяющий порядок:

- приема, регистрации и учета запросов и обращений субъектов ПДн (или их законных представителей);
- рассмотрения и обработки запросов или обращений субъектов ПДн (или их законных представителей) на получение информации, касающейся обработки их ПДн;
- рассмотрения и обработки запросов или обращений субъектов ПДн (или их законных представителей) на предоставление доступа к своим ПДн;
- рассмотрения и обработки запросов субъектов ПДн (или их законных представителей) в случае выявления недостоверных ПДн, относящихся к соответствующему субъекту;

3. Регламент проведения классификации государственных и муниципальных ИСПДн (определения уровня защищенности персональных данных для иных информационных систем), определяющий порядок:
- формирования комиссии для классификации (определения уровня защищенности) ИСПДн;
- проведения классификации (определения уровня защищенности) ИСПДн;
- пересмотра классов (уровня защищенности) ИСПДн по замечаниям регулирующих органов и (или) при изменении их структуры и особенностей функционирования;

4. Регламент организации внутреннего аудита (проверки) на соответствие требованиям к обработке и защите ПДн, определяющий порядок:
- организации и управления программой аудита оператора ПДн;
- проведения внутренних и внешних аудитов оператора ПДнс целью проверки выполнения установленных требований к обработке и обеспечению безопасности ПДн;

5. Регламент учета, хранения и уничтожения носителей ПДн, определяющий порядок:
- ведения учета электронных и бумажных носителей ПДн;
- организации хранения носителей ПДн, включая требования к местам хранения и допуску к ним;
- утилизации и уничтожения электронных и бумажных носителей ПДн;

6. Регламент резервного копирования ПДн, определяющий порядок:
- определения массивов информации, подлежащих резервному копированию, мест хранения резервных копий и требований по безопасности, а также периодичность создания резервных копий и сроки их хранения;
- восстановления ПДн из резервных копий;

7. Регламент взаимодействия с регулирующими органами в области обработки и защиты ПДн, определяющий порядок действий работников в случаях:

- проведения плановых и внеплановых контрольных мероприятий регулирующими органами;
- обработки отдельных запросов от регулирующих органов;
- проведения мероприятий по итогам проверок или полученных запросов от регулирующих органов;

8. Регламент реагирования на инциденты информационной безопасности, определяющий порядок:
- идентификации и классификации инцидентов информационной безопасности;
- реагирования на инциденты информационной безопасности;
- взаимодействия с внешними организациями (в том числе при необходимости контролирующими органами) в рамках реагирования на инциденты информационной безопасности;
- проведения анализа и выявления возможных причин произошедших инцидентов информационной безопасности;
- проведения разбирательств и выполнения последующих действий по итогам инцидентов информационной безопасности;

9. Регламент эксплуатации средств криптографической защиты информации (в случае использования средств криптографической защиты информации для обеспечения безопасности ПДн), определяющий порядок:
- установки, настройки и обслуживания средств криптографической защиты информации, используемых для обеспечения безопасности ПДн;
- учета средств криптографической защиты информации, технической и эксплуатационной документации к ним;
- учета лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных;
- контроля за соблюдением условий использования криптосредств.

3.4 Рекомендации по содержанию документов уровня инструкций

3.4.1 Документы уровня инструкций содержат детальные указания по выполнению отдельных операций или видов деятельности, связанных с обработкой и защитой ПДн.

В документах уровня инструкций рекомендуется определить:
- единый порядок сбора, систематизации, накопления, хранения, использования, уничтожения и других видов автоматизированной и неавтоматизированной обработки ПДн для работников, непосредственно участвующих в их обработке;
- основные правила по обеспечению безопасности ПДн для работников, непосредственно участвующих в обработке ПДн;
- правила установки, администрирования и обслуживания технических средств защиты, используемых для обеспечения безопасности ПДн;

- дополнительные правила, относящиеся к выполнению определенных действий или решению определенных задач персоналом в рамках обработки и защиты ПДн.

3.4.2 Оператору ПДн рекомендуется ввести следующий перечень инструкций (или включить дополнительными разделами в должностные инструкции работника):

1. Инструкция работнику по правилам обработки и обеспечению безопасности ПДн, определяющая основные правила, которые необходимо соблюдать работнику, участвующему в обработке ПДн.
2. Инструкция администратору по организации антивирусной защиты систем обработки ПДн, определяющая правила установки, администрирования и обслуживания средств антивирусной защиты.
3. Инструкция администратору по организации парольной защиты в системах обработки ПДн, определяющая правила организации парольной защиты, в частности требования к сложности, периодичности обновления, местам хранения паролей для ИСПДн.

3.5 Требования к документам уровня учетных документов

3.5.1 Документы уровня учетных документов предназначены для фиксации результатов проведенных мероприятий по обработке и защите ПДн.

Так как документы данного уровня являются свидетельствами выполняемой деятельности по выполнению установленных требований по обработке и защите ПДн, то к их хранению и учету должны предъявляться повышенные требования. Срок и порядок хранения таких документов должны быть утверждены нормативными актами оператора ПДн в соответствии с требованиями федерального законодательства. Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения приведен в разделе II приложения к приказу Минкультуры России от 25.08.2010 N 558.

3.5.2 Оператору ПДн рекомендуется, как минимум, ввести следующий перечень учетных документов:

1. Перечень ПДн, обрабатываемых в организации.
2. Перечень подразделений и работников, допущенных к обработке ПД.
3. Перечень ИСПДн.
4. Журнал учета обращений субъектов ПДн.
5. Журнал учета мероприятий по защите информации.
6. Журнал учета и выдачи машинных носителей ПДн.
7. Журнал учета ремонтно-восстановительных работ на основных технических средствах.
8. Журнал учета хранилищ носителей персональных данных.
9. Журнал учета используемых криптосредств, эксплуатационной и технической документации к ним.

10. Акт об уничтожении носителей ПДн.
11. Обязательство о неразглашении сведений конфиденциального характера (ПДн).

3.6 Типовые образцы и формы организационно – распорядительных документов.

3.6.1 В приложениях к УП ОРД ПДн приведены типовые образцы и формы следующих ОРД:
1. «Положение об обработке персональных данных» (Приложение Д).
2. «Положение по организации и проведения работ по обеспечению безопасности персональных данных» (Приложение Е).
3. Должностная инструкция ответственного за организацию обработки персональных данных (Приложение Ж).
4. «Обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним контракта, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение З).
5. Форма согласия на обработку персональных данных (Приложение И).
6. Форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои ПДн (Приложение К).
7. Инструкция о порядке доступа работников в помещения, в которых ведется обработка персональных данных (Приложение Л).
8. Положение об особенностях и правилах обработки персональных данных, осуществляемой без использования средств автоматизации (Приложение М).
9. План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных (Приложение Н).
10. Уведомление об обработке (о намерении осуществлять обработку персональных данных) (Приложение О).

3.7 Оценка требуемых ресурсов и персонала по выполнению требований к документированию процессов обработки и защиты персональных данных

3.7.1 Документирование управленческой деятельности операторов ПДн, с учетом необходимости разработки и поддержания в актуальном состоянии значительного числа ОРД, требует проведения оценки ресурсов и персонала необходимых для выполнения требований к документированию процессов обработки и защиты ПДн.
В соответствии с [11] расчет требуемого количества персонала проводится по формуле:

$$P=Q*C:T*R \quad (1)$$

где:

Q - объем выполняемых операций в год с учетом периодичности их выполнения;

C - трудоемкость выполнения одной операции;

T - годичный объем, выполняемых одним человеком;

R - коэффициент невыхода на работу по болезни, отпусками т.п..

Итоговый систематизированный перечень основных задач в области обеспечения защиты ПДн и прогнозируемая оценка их трудоемкости без использования средств автоматизации для организации, имеющей до 1000 АРМ и серверов приведены в Приложении П. Анализ оценки трудоемкости указанных задач показывает необходимость автоматизации процессов администрирования средств защиты информации и разработки ОРД по защите ПДн.

4 ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ ДОКУМЕНТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Для документального закрепления организационных и технических мер по технической защите информации (ТЗИ) для ГИС (МИС), предназначенных для обработки информации ограниченного доступа, не составляющей государственную тайну (в том числе ПДн) разрабатывается комплект документов в соответствии с ГОСТ 34.201, требованиями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти (ФОИВ) и национальных стандартов по защите информации, обеспечивающий выполнения следующих работ:

- формирование требований к системе ТЗИ;
- разработка (проектирование) системы ТЗИ;
- внедрение системы ТЗИ;
- аттестация ГИС и МИС на соответствие требованиям безопасности информации (для иных ИС их аттестация проводится по решению руководителя организации (предприятия) - оператора персональных данных);
- обеспечение защиты информации в ходе эксплуатации аттестованной ИС;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

4.2 Формирование и документальное закрепление требований к защите информации в ИС, разработка (проектирование) системы ТЗИ и ее внедрение организуются руководителем организации – оператором персональных данных с учетом ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 51583, нормативных правовых актов и методических документов уполномоченных ФОИВ.

4.3 Аттестация ИС на соответствие требованиям безопасности информации и документальное закрепление ее результатов организуется руководителями ОГВ, МСУ и проводятся до ввода ИС в постоянную эксплуатацию в соответствии с положениями нормативных правовых актов и методических документов уполномоченных ФОИВ и национальных стандартов по защите информации.

4.4 Обеспечение защиты информации в ходе эксплуатации аттестованной ИС, а также обеспечение защиты информации при выводе ее из эксплуатации или после принятия решения об окончании обработки информации, осуществляются руководителем ОГВ и МСУ, организации (предприятия) в соответствии с эксплуатационной документацией на систему защиты информации ИСПДн и ОРД по защите информации.

4.5 Для организации и реализации системы ТЗИ ИС разрабатывают следующие основные комплекты документов:

а) документы ИС, разрабатываемые в ходе проведения работ по формированию и документальному закреплению требований к защите информации, разработке (проектированию) системы ТЗИ и ее внедрению, включающие:

- техническое задание на создание системы ТЗИ;
- проектную и эксплуатационную документацию системы ТЗИ;
- материалы предварительных и приемочных испытаний системы ТЗИ;
- модель угроз безопасности информации;
- технический паспорт;
- описание технологического процесса обработки информации в ИС;
- перечень защищаемых информационных ресурсов ИС;
- акт классификации (для ГИС и МИС);
- акт определения уровня защищенности ПДн в ИСПДн (для иных ИС).

б) документы, разрабатываемые органом по аттестации объектов информатизации (ОИ) на соответствие требованиям безопасности информации, устанавливающие порядок аттестационных испытаний ОИ и содержащие его результаты, включающие:

- программу и методики аттестационных испытаний;
- протоколы аттестационных испытаний;
- заключение о соответствии ОИ требованиям безопасности информации;
- аттестат соответствия требованиям безопасности информации.

в) ОРД по ТЗИ, устанавливающие правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации

аттестованной ИС, а также порядок ввода в действие и эксплуатации ИС, обеспечения защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

4.6 Содержание документов должно отвечать следующим основным требованиям:

- обеспечивать терминологическое единство документов;
- соответствовать действующим нормативным правовым актам и национальным стандартам в области защиты информации и иметь, при необходимости, ссылки на них;
- состоять из четко, кратко, логически последовательно изложенных формулировок, не допускающих различных толкований;
- обеспечивать непротиворечивость и взаимосогласованность основных положений различных видов документов, входящих в типовой комплект.

4.7 Техническое задание на создание системы защиты информации должно разрабатываться с учетом ГОСТ 34.602, ГОСТ Р 51583, нормативных правовых актов и методических документов уполномоченных ФОИВ.

4.8 Проектная и эксплуатационная документация системы защиты информации должна разрабатываться с учетом РД 50-34.698-90 и ГОСТ Р 51583, нормативных правовых актов и методических документов уполномоченных ФОИВ.

4.9 Материалы предварительных и приемочных испытаний системы защиты информации должны разрабатываться с учетом ГОСТ 34.603.

4.10 Модель угроз безопасности информации должна разрабатываться с учетом и национальных стандартов по защите информации, нормативных правовых актов и методических документов уполномоченных ФОИВ.

4.11 Технический паспорт должен содержать:

- общие сведения об ИСПДн (наименование, место расположения, сведения о категории и классе (уровне) защищённости ИСПДн объекта (регистрационные номера и даты утверждения актов определения класса (уровня защищенности ПДн), сведения о ее вводе в эксплуатацию (номер и дату акта или приказа руководителя организации-владельца о вводе ИСПДн в эксплуатацию вносят в технический паспорт после получения аттестата соответствия ОИ требованиям безопасности информации);
- состав оборудования ИСПДн (перечень ОТСС и ВТСС, их тип, заводской (инвентарный) номер, размещение на объекте; перечень СЗИ, их наименование и тип, заводской (инвентарный) номер; сведения о сертификатах соответствия требованиям безопасности информации, маркировке знаками соответствия, месте и дате установки СЗИ);
- сведения о специальных проверках и специальных исследованиях ОТСС, о сертификатах соответствия технических, программных и программно-технических средств, СЗИ, требованиям безопасности информации, о лицензиях на программные продукты;

- сведения о специальных объектовых исследованиях; сведения об аттестации ОИ на соответствие требованиям безопасности информации; сведения об оценке и (или) контроле эффективности защиты информации (вносятся в технический паспорт после аттестации);
- схему размещения ОИ относительно границ контролируемой зоны;
- схему размещения всех технических средств и СЗИ, установленных на ОИ, расположения линий электропитания и заземления, охранной и пожарной сигнализаций, телефонизации и оповещения, отопления и вентиляции для ВП, схему информационных потоков распределенных АС;
- данные по учету проведения регламентных проверок (наименование организации, проводившей проверку, дата проведения проверки, номер протокола);
- лист регистрации изменений (порядковый номер и дата введения изменений, наименование документа, фиксирующего изменения, номер изменённого (исправленного) листа паспорта, подпись лица, внесшего изменение).

4.12 Описание технологического процесса обработки информации в ИСПДн содержать:
- сведения о наименовании ИСПДн, его назначении, уровне конфиденциальности обрабатываемой на ней информации;
- сведения о программном обеспечении, используемом для осуществления технологического процесса обработки информации, его назначении и месте установки (логический диск, каталог и т. п.);
- описание режима работы ИСПДн и установленной разграничительной системы доступа пользователей к защищаемой информации, программам, каталогам и файлам (описание процедуры идентификации и аутентификации);
- сведения о правах пользователей на обработку и хранение файлов с защищаемой информацией;
- сведения об установленных операционной системе, системе защиты информации от НСД и антивирусной защите.

4.13 Перечень защищаемых информационных ресурсов в ИСПДн, должен содержать: наименование ИСПДн, наименование ресурсов, данные об уровне конфиденциальности ресурсов.

4.14 Акт классификации ГИС (МИС) должен содержать:
- наименование АС, ее место расположения (адрес);
- сведения о составе комиссии, проведшей классификацию;
- сведения об условиях эксплуатации (режим обработки информации, права доступа к информации), характере обрабатываемой информации (высшая степень секретности (уровень конфиденциальности) обрабатываемой информации), документах, в соответствии с которыми присваивается класс защищенности;
- сведения об установленном классе защищенности от НСД к информации.

4.15 Документы, разрабатываемые органом по аттестации ОИ на соответствие требованиям безопасности информации должны соответствовать требованиям национальных стандартов по вопросам аттестации ОИ, а также нормативным правовым актам и методическим документам уполномоченных ФОИВ и храниться в организации - владельце ОИ вместе с другими документами ОИ.

4.16 ОРД по ТЗИ на ОИ должны разрабатываться в соответствии с требованиями нормативных правовых актов и методических документов уполномоченных ФОИВ и национальных стандартов в области защиты информации и определять правила и процедуры:

- управления (администрирования) системой защиты информации;
- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ОИ и (или) к возникновению угроз безопасности информации, и реагирования на них;
- управления конфигурацией (составом) аттестованного ОИ и его системы защиты информации;
- контроля (мониторинга) за обеспечением уровня защищенности информации;
- защиты информации при выводе ОИ из эксплуатации или после принятия решения об окончании обработки информации.

4.17 Типовые формы документов по ТЗИ на ОИ (в том числе актов, приказов протоколов, разрабатываемых в соответствии с РД 50-34.698-90 определяются руководителем организации-обладателя ОИ с учетом требований нормативных правовых актов и методических документов уполномоченных ФОИВ, национальных стандартов.

4.18 Документы по ТЗИ разрабатывают с учетом требований ГОСТ 34.602, ГОСТ 34.201, ГОСТ 51583, РД 50-34.698-90, а также нормативных правовых актов и методических документов уполномоченных ФОИВ.

Разработку, согласование и утверждение документов по ТЗИ на ОИ проводят в соответствии с таблицей 1.

4.19 Введение в действие документов, указанных в таблице 1, осуществляется с момента их утверждения.

Основанием для введения ОИ в эксплуатацию является получение организацией - обладателем ОИ аттестата соответствия ОИ требованиям безопасности информации.

4.20 Аттестат соответствия ОИ требованиям безопасности информации, заключение по результатам аттестационных испытаний, материалы аттестационных испытаний, перечень защищаемых информационных ресурсов, описание технологического процесса обработки информации, Акт классификации, технический паспорт брошюруют вместе, как правило, с учетом приведённого в таблице 1 порядка.

4.21 Оформление документов выполняют в соответствии с требованиями ГОСТ 2.105, ГОСТ 2.106.

Т а б л и ц а 1 – Требования к разработке, согласованию и утверждению документов по технической защите информации на объекте информатизации

Наименование документа	**Ответственный за разработку документ**	**Кем подписывается (с кем согласовывается) документ)**	**Кем утверждается документ**
Техническое задание на создание системы защиты информации	В соответствии с ГОСТ 34.602, ГОСТ Р 51583		
Проектная и эксплуатационная документация системы защиты информации	В соответствии с ГОСТ 34.201, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 51583		
Материалы предварительных и приемочных испытаний системы защиты информации	В соответствии с ГОСТ 34.601, ГОСТ 34.603, ГОСТ Р 51583		
Модель угроз безопасности информации	Руководитель ОИ	Руководителем ОИ (с руководителем подразделения по защите информации и с руководителем подразделения режима и безопасности организации)	Руководителем (заместителем руководителя) организации
Перечень защищаемых информационных ресурсов (только для АС)	Руководитель ОИ	Руководителем ОИ (с руководителем подразделения по защите информации и с руководителем подразделения режима и безопасности организации)	Руководителем (заместителем руководителя) организации

Наименование документа	Ответственный за разработку документ	Кем подписывается (с кем согласовывается) документ)	Кем утверждается документ
Описание технологического процесса обработки информации (только для АС)	Руководитель ОИ	Руководителем подразделения по защите информации, руководителем ОИ, администратором защиты информации на ОИ	Руководителем (заместителем руководителя) организации
Акт классификации (только для АС)	Руководитель ОИ	Председателем и членами комиссии, классифицирующими ОИ	Руководителем (заместителем руководителя) организации
Технический паспорт	Руководитель ОИ	Руководителем ОИ (с руководителем подразделения по защите информации)	Руководителем (заместителем руководителя) организации
Документы, разрабатываемые органом по аттестации ОИ на соответствие требованиям безопасности информации	В соответствии с национальными стандартами по вопросам аттестации ОИ, а также нормативным правовым актам и методическим документам уполномоченных ФОИВ		
Организационно-распорядительные документы по защите информации	В соответствии с нормативными правовыми актами и методическими документами уполномоченных ФОИВ, а также типовыми формами, определяемыми руководителем организации		

4.22 При оформлении документов применяют гарнитуру шрифта Times New Roman или Arial, кегль 12-14. При оформлении приложений к документам допускается использовать кегль 11. Документы выполняют на одной стороне листа формата А4 (210х297 мм).

4.23 Текст документов печатают через один или полтора междустрочных интервала, поле с левой стороны текста должно быть шириной не менее 25 мм, сверху и снизу – 20 мм, а справа – 10 мм. Реквизиты документов

печатают через один междустрочный интервал и центрируют по левому краю. Разрешается выполнять центрирование реквизитов по центру. Реквизиты документов отделяют друг от друга двумя-тремя междустрочными интервалами

4.24 Даты в документах оформляют арабскими цифрами словесно-цифровым способом (например, 8 июня 2012 г.) или цифровым способом (например, 08.06.2012).

4.25 Названия организаций, фирм, изделий и другие имена собственные в документах приводят на языке оригинала. Допускается транслировать имена собственные и приводить названия организаций в переводе на русский язык с добавлением (при первом упоминании) названия на языке оригинала.

4.26 Документы в зависимости от их объема и сложности структуры текста подразделяют на пункты, или на пункты и подпункты, или на разделы и пункты, или на разделы, подразделы и пункты, или на разделы, подразделы, пункты и подпункты.

Разделы, подразделы, пункты и подпункты нумеруют арабскими цифрами. После номера раздела, подраздела, пункта и подпункта в тексте документа ставят точку. Если раздел, подраздел или пункт состоит из одного соответственно подраздела, пункта или подпункта, то этот подраздел, пункт или подпункт не номеруется.

Внутри пунктов или подпунктов могут быть приведены перечисления. Перед элементами перечисления дефисы не ставят. При необходимости ссылки в тексте документа хотя бы на один из элементов перечисления перед элементами перечисления ставят строчные буквы русского алфавита, начиная с буквы «а» (за исключением букв ё, з, й, о, ч, ъ, ы, ь), после которых ставят круглую скобку.

Для дальнейшей детализации перечислений используют арабские цифры, после которых ставят круглую скобку, а запись производят с абзацного отступа в четыре знака.

4.27 Разделы и подразделы должны иметь заголовки. Пункты и подпункты заголовков не имеют.

Заголовки разделов и подразделов располагают по центру относительно текста документа и печатают полужирным шрифтом с прописными буквами без точки в конце, не подчёркивая.

4.28 Номера страниц документа проставляют в центре нижней части поля листа арабскими цифрами без точки. Номер страницы на титульном листе (первом листе) документа не проставляют.

4.29 Сокращение русских слов и словосочетаний - в соответствии с требованиями ГОСТ 7.12.

4.30 Разработку документов, содержащих сведения, составляющие информацию ограниченного доступа, осуществляют с учетом требований действующего законодательства.

Документы, содержащие сведения о способах и методах ТЗИ на объектах информатизации, в которых обрабатывается (циркулирует) информация, доступ к которой ограничен федеральными законами или по желанию обладателя информации, должны иметь пометку не ниже «Для служебного пользования». При этом гриф ограниченного распространения должен быть не ниже чем для документов, приводимых в библиографии в качестве ссылочных. При необходимости допускается приводить обозначения (без наименований) документов с более высоким грифом ограничения распространения.

5 РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ К ПРОВЕДЕНИЮ КОНТРОЛЯ И НАДЗОРА ЗА ВЫПОЛНЕНИЕМ ТРЕБОВАНИЙ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫ

5.1 В настоящее время Уполномоченным органом по защите прав субъектов ПДн, в соответствии со ст. 23 ФЗ «О персональных данных», является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), преобразованная из Федеральной службы по надзору в сфере связи и массовых коммуникаций в соответствии с указом Президента РФ от 3 декабря 2008 года № 1715. На эту федеральную службу возлагается задача обеспечения контроля и надзора за соответствием обработки операторами ПДн требованиям ФЗ «О персональных данных».

5.2 Цель контроля и надзора - проверка соответствия требованиям законодательства содержания ПДн и способов их обработки целям их обработки.

5.3 Предметом государственного контроля (надзора) за соответствием обработки ПДн требованиям законодательства РФ в области ПДн являются:

- документы, характер информации в которых предполагает или допускает включение в них ПДн;

- информационные системы ПДн;

- деятельность по обработке ПДн.

5.4 Уполномоченный орган по защите прав субъектов ПДн имеет право (ст. 23 ФЗ «О персональных данных»):

- запрашивать у операторов (физических или юридических лиц) информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

- осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

- требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

- принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований ФЗ «О персональных данных»;

- обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн и представлять интересы субъектов ПДн в суде;

- направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;

- привлекать к административной ответственности лиц, виновных в нарушении ФЗ «О персональных данных».

5.5 Приказом Минкомсвязи от 14.11.2011 г. № 312 утвержден «Административный регламент проведения проверок Роскомнадзором». Основанием для включения проверки в план является начало осуществления оператором деятельности по обработке ПДн, а также истечение трех лет со дня государственной регистрации Оператора в качестве юридического лица и окончания последней плановой проверки. Планы проверок размещены на сайте Роскомнадзора по ссылке http://www.rsoc.ru/plan-and-reports/contolplan/.

Видами проверок в соответствии с ФЗ № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при

осуществлении государственного контроля (надзора) и муниципального контроля» являются плановые, внеплановые, документарные, выездные.

5.6 Внеплановые проверки проводятся по следующим основаниям:

- истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства РФ в области персональных данных;

- поступление в Службу или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации, в том числе о следующих фактах;

- возникновение угрозы причинения вреда жизни, здоровью граждан;

- причинение вреда жизни, здоровью граждан;

- приказ руководителя Службы или руководителя территориального органа Службы, изданный в соответствии с поручениями Президента и Правительства РФ;

- нарушение прав и законных интересов граждан действиями (бездействием) операторов при обработке их ПДн;

- нарушение операторами требований законодательства РФ в области ПДн, а также при несоответствии сведений, содержащихся в уведомлении об обработке ПДн, фактической деятельности;

- нарушения прав и законных интересов граждан действием (бездействием) операторов при обработке их ПДн;

- нарушение оператором требований законодательства РФ в области ПДн, а также о несоответствии сведений, содержащихся в уведомлении об обработке ПДн, фактической деятельности.

5.7 Приоритетными категориями операторов для проведения проверок являются:

- операторы, на деятельность которых поступали жалобы граждан о нарушении их прав и законных интересов;

- операторы, к ведению которых предположительно относятся ИСПДн, базы которых распространяются в ИТКС Интернет и на розничных рынках;

- операторы, осуществляющие обработку специальных категорий ПДн.

5.8 Должностные лица Службы или ее территориального органа при проведении проверок вправе в пределах своей компетенции (п. 6 Регламента):

- выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области ПДн;

- составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;

- обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн;

- использовать технику и оборудование, принадлежащие Службе или ее территориальному органу;

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения проверки;

- получать доступ к ИСПДн в режиме просмотра и выборки необходимой информации;

- направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке, если условием лицензии на осуществление такой деятельности предусмотрен запрет на передачу ПДн третьим лицам без согласия в письменной форме субъекта ПДн;

- принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушениями требований законодательства РФ в области ПДн;

- требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн.

5.9 Для оценки эффективности принимаемых оператором технических мер по обеспечению безопасности ПДн при их обработке в негосударственных (иных) ИСПДн Роскомнадзор или его территориальный орган в рамках проверки привлекают экспертов, экспертные организации, включенные в установленном порядке в реестр граждан и организаций, привлекаемых в качестве экспертов, экспертных организаций к проведению мероприятий по контролю (п.42.1 Регламента).

5.10 Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.

В случае возникновения необходимости срок проведения проверки может быть продлен, но на срок не более двадцати рабочих дней.

5.11 Оператор обязан учитывать эти полномочия при проведении мероприятий по контролю и надзору, а также предоставлять информацию и документы, необходимые для реализации полномочий, предоставленных федеральными законами надзорному органу.

Операторам ПДн следует обратить особое внимание на те документы, которые будут рассматриваться в ходе проведения проверки.

К таким документам в соответствии с пунктом 67 Регламента относятся:

- уведомление об обработке ПДн;

- документы, необходимых для проверки фактов, содержащих признаки нарушения законодательства РФ в области ПДн, изложенных в обращениях граждан и информации, поступившей в Службу или ее территориальный орган;

- документы, подтверждающих выполнение оператором предписаний об устранении ранее выявленных нарушений законодательства РФ в области ПДн;

- письменное согласие субъекта ПДн на обработку его ПДн;

- документы, подтверждающие соблюдение требований законодательства РФ при обработке специальных категорий и биометрических ПДн;

- документы, подтверждающие уничтожение оператором ПДн по достижении цели их обработки;

- локальные акты оператора, регламентирующих порядок и условия обработки ПДн;

- документы по результатам исследования (обследования) ИСПДн, в части, касающейся ПДн субъектов ПДн, обрабатываемых в ней.

5.12 Проверка оператора завершается составлением и вручением оператору акта проверки. В случае выявления по результатам проверки нарушения требований законодательства РФ в области ПДн, оператору, вместе с актом, выдается предписание об устранении выявленных нарушений (п.85 Регламента).

5.13 Типовыми нарушениями требований законодательства по результатам проверок Роскомнадзора являются:

- операторы осуществляют обработку ПДн без уведомления уполномоченного органа по защите прав субъектов ПДн;

- обработка ПДн осуществляется без предварительного согласия субъекта ПДн;

- ПДн сотрудников проверенных организаций передавались третьему лицу без согласия работников и без заключения соответствующего договора, предусматривающего обязанность по обеспечению конфиденциальности и безопасности ПДн при их обработке;

- не приняты необходимые организационные меры для защиты ПДн от неправомерного или случайного доступа к ним.

Возможные последствия проверок вытекают из перечисленных полномочий и могут составлять:

- получение предписаний на устранение выявленных нарушений;

- наложение административных штрафов;

- приостановление или прекращение обработки ПДн, осуществляемой с нарушением требований ФЗ «О персональных данных»;

- принятие мер по приостановлению действия или аннулированию основных лицензий операторов;

- возбуждение уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн.

5.14 Задача контроля и надзора за выполнением технических требований по обеспечению безопасности ПДн возложена на федеральный орган исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России), и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в ИСПДн. В соответствии с ФЗ от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в ФЗ «О персональных данных» изменились контрольные полномочия ФСТЭК и ФСБ России, которые уполномочены осуществлять контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПДн при их обработке только в государственных ИСПДн. По решению Правительства РФ с учетом значимости и содержания обрабатываемых ПДн возможен контроль

ИСПДн, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся ГИС (МИС).

5.15 В соответствии с частью 1 ст. 18.1 ФЗ №152-ФЗ «О персональных данных» оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим ФЗ или другими федеральными законами. Таким образом, оператор, в ходе проверки, не только показывает документы, но и подтверждает меры по защите ПДн, чем удовлетворяет (или не удовлетворяет) уполномоченный орган регулятора и (или) приглашенного эксперта.

5.16 Типовыми ошибками, выявленными в ходе проверок выполнения требований законодательства по защите ПДн в сфере компетенции ФСТЭК России являются:

- отсутствие требований по технической защите ПДн в ТЗ и проектной документации на ИСПДн;

- незавершенность классификации (определения уровней защищенности ПДн в ИСПДн) или ее ошибочность;

- невыполнение работ по анализу угроз информационной безопасности и отсутствие модели угроз ПДн;

- отсутствие или незавершенность разработки необходимого комплекта ОРД по защите ПДн;

- отсутствие или несоответствие требованиям ФСТЭК России необходимых мер по защите ПДн;

- отсутствие учета машинных носителей информации;

- отсутствие в должностных регламентах должностных лиц, ответственных за защиту ПДн, обязанностей и полномочий по выполнению установленных требований;

- отсутствие или недостаточность необходимого количества подготовленных специалистов по ТЗИ.

5.17 ФСБ России по результатам проверок использования средств криптозащиты к числу типовых недостатков относит:

- использование средств криптозащиты отличных от эталонных сертифицированных версий;

- невыполнение отдельных требований по порядку эксплуатации криптосредств, предусмотренных технической документацией;

- несоответствие отдельных документов оператора, регламентирующих вопросы защиты ПДн положениям нормативно-методических документов ФСБ России.

5.18 Оператор обязан:

- учитывать полномочия надзорных органов при проведении мероприятий по контролю и надзору, а также предоставлять информацию, необходимую для реализации полномочий, предоставленных федеральными законами надзорному органу;

- ежегодно в начале года проверять наличие оператора в «Сводном плане проверок субъектов предпринимательства» на сайте Генеральной Прокуратуры и Планах проведения плановых проверок Роскомнадзора, ФСТЭК и ФСБ России.

5.19 В случае получения оператором уведомления о проведении проверки лицам, ответственным за организацию обработки и защиты ПДн необходимо:

- собрать комплект необходимых документов с учетом требований нормативных правовых актов, ведомственных документов (при их наличии) и п.64.1 Административного регламента Роскомнадзора, Административных регламентов ФСТЭК и ФСБ России.

При проведении проверки соблюдения требований к обеспечению безопасности персональных данных ФСТЭК и ФСБ России необходимо подготовить следующие документы:

- учредительные документы (устав) учреждения (предприятия);

- модель угроз, разработанную в соответствии с методическими рекомендациями ФСТЭК и ФСБ России;

- документы, подтверждающие разработку системы защиты ПДн, обеспечивающей нейтрализацию актуальных угроз ПДн (техническое задание, технический проект, действующие сертификаты на средства защиты информации (СЗИ) и криптографической защиты информации (СКЗИ), акты установки СЗИ/СЗКИ, бухгалтерские документы на их приобретение и т.п.);

- ОРД по обеспечению безопасности ПДн;

- аттестат соответствия ИСПДн, протоколы испытаний и заключения о возможности эксплуатации (для ГИС и МИС);

- документы, подтверждающие обучение лиц, использующих СЗИ/СКЗИ, правилам работы с ними;

- должностные инструкции лиц, использующих СЗИ/СКЗИ;

- журнал учета носителей ПДн;

- приказ о допуске лиц к обработке ПДн;

- приказ о допуске к работе с СКЗИ;

- документы, подтверждающие проведение контроля за проведением мероприятий по защите ПДн;

При этом ответственным лицам рекомендуется:

- сформировать указанный комплект документов и, в соответствии с ежегодными планами работ, поддерживать их актуальность;

- проверить правильность заполнения всех необходимых журналов и документов, разрабатываемых по типовым формам (например - акты уничтожения персональных данных);

- проинструктировать работников основных структурных подразделений, работающих с ИСПДн, о порядке работы и защиты ПДн в соответствии с разработанными ОРД и эксплуатационными документами;

- организовать оперативный просмотр электронных журналов обращений пользователей информационных систем к ПДн, а так же журналов учета СЗИ/СЗКИ и других форм учета;

- определить ответственного сотрудника, который будет сопровождать проверяющих;

- утвердить в соответствии с внутренними требованиями документооборота необходимые документы для обеспечения режима безопасности персональных данных.

Рекомендуется обязательное участие в мероприятиях по контролю и надзору должностных лиц оператора, ответственных за обработку и защиту ПДн, начальников отделов вычислительной техники, информационной безопасности и юридического отдела.

ПРИЛОЖЕНИЕ А

ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ И НОРМАТИВНО – МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

3. Федеральный закон от 27.12.2002 г. г. №184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4.05.2011 г. г. №99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

6. Федеральный закон от 29 ноября 2010 г. N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации".

7. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. ,N 197-ФЗ

8. «Доктрина информационной безопасности Российской Федерации», утверждена Указом Президента Российской Федерации от 9.09.2000 г. № Пр.-1895.

9. Указ Президента Российской Федерации от 16.08.04 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

10. Указ Президента Российской Федерации от 06.03.97г. № 188 « Об утверждении перечня сведений конфиденциального характера».

11. Постановление Правительства Российской Федерации от 3.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

12. Постановление Правительства Российской Федерации от 3.03.2012 г.

№ 171 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

13. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

14. Постановление Правительства РФ от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения

обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами операторами, являющимися государственными или муниципальными органами».

15. Постановление Правительства РФ от 6.07.2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

16. «Специальные требования и рекомендации по технической защите

конфиденциальной информации» Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. №282.

17. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15.02.2008 г.;

18. Приказ ФСТЭК России от 11.02.13 г. №17 «Мероприятия по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

19. Методический документ "Меры защиты информации в государственных информационных системах" (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.).

20. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

21. Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

22. Приказ Министерства связи и массовых коммуникаций от14.11.2011 г. №312 «Об утверждении административного Регламента исполнения Роскомнадзором государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных»

23. Концепции создания единой государственной информационной системы в сфере здравоохранения, утвержденной приказом Минздравсоцразвития России от 28 апреля 2011 г. N 364.

24. «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной защиты, труда и занятости» утвержденными директором департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009г.

25. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости от 23.12.2009.

26. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года

27. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Решение председателя Гостехкомиссии России от 30 марта 1992 г.

28. Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Решение председателя Гостехкомиссии России от 30 марта 1992 года.

29. Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Решение председателя Гостехкомиссии России от 30 марта 1992 года.

30. Руководящий документ. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997г.

31. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования».

32. ГОСТ 34. «Информационная технология. Комплекс стандартов на автоматизированные системы».

33. ГОСТ 34.601-90. «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

34. ГОСТ 34.603-92. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем».

35. ГОСТ 50922-2006 «Защита информации. Основные термины и определения».

36. ГОСТ Р 50923-96 «Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения».

37. ГОСТ Р 50948-2001. «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности».

38. ГОСТ Р 50949-2001. «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности».

39. ГОСТ 51583-2000 «Порядок создания АС в защищенном исполнении».

40. ГОСТ 12.2.032-78 «Система стандартов безопасности труда. Рабочее место при выполнении работ сидя. Общие эргономические требования».

41. ГОСТ 12.2.003-91 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности».

42. ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности».

43. СП 2.2.1.1312-03 «Санитарно-эпидемиологические правила».

44. СанПиН 2.2.2/2.4. 1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работ".

45. СН 512-78 «Инструкция по проектированию зданий и помещений для электронно-вычислительных машин».

46. Государственная система документационного обеспечения управления (ГСДОУ);

47. Государственный стандарт РФ ГОСТ Р5П41-98 «Делопроизводство и архивное дело. Термины и определения»;

48. Государственный стандарт РФ ГОСТ Р6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»;

49. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти (2000 г.);

50. Общероссийский классификатор управленческой документации

(ОКУД) ОК 011-93 (1993 г., с изм.. и доп. 1999-2002 гг.);

51. Санитарные нормы и правила СанПин 2.2.2 / 2.4.1340-03 «Гигиенические требования к персональным ЭВМ и организации работы»10;

52. Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления (1995 г.);

53. Квалификационный справочник должностей служащих (1998 г., с изм. и доп. 1999—2002 гг.)11;

54. Основные правила работы архивов организаций (2002 г.);

55. Методические рекомендации ВНИИДАДФАС РФ «Унификация текстов управленческих документов» (1998 г.).

ПРИЛОЖЕНИЕ Б. ТИПОВЫЕ ОБРАЗЦЫ АНКЕТ ДЛЯ ПРОВЕДЕНИЯ АУДИТА (ВНУТРЕННЕЙ ПРОВЕРКИ) ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

АНКЕТА №1

Общая информация о компании

Общая информация о компании

Название компании:	
Сфера деятельности:	
Физический адрес:	

Определения

Персональные данные (ПДн) *– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. В частности, к ПДн относятся фамилия, имя, отчество, дата рождения, адрес, место работы и должность и др.*

Обработка персональных данных – *любое действие, совершаемых с использованием ПДн, включая сбор (получение), запись, накопление, хранение, изменение, использование, передачу, удаление и др.*

Информационная система персональных данных *(ИСПДн) – совокупность ПДн, содержащихся в базах данных, и информационных технологий (технических средств), обеспечивающих их обработку. В качестве ИСПДн на этапе обследования могут выступать: 1С, электронная почта, корпоративный сайт, телефонная база и др.*

Текущее состояние работ

В таблице перечислены основные этапы работ по организации процессов обработки и защиты информации (до начала разработки системы защиты ПДн). В соответствующем столбце отметьте работы, которые уже были выполнены в компании.

Таблица – Текущее состояние работ по организации обработки и защиты ПДн

Процесс	+ / –	Примечание
Проведено обследование процессов и систем компании, в которых обрабатываются ПДн		
Разработаны документы, устанавливающие порядок обработки ПДн в компании		
Назначен сотрудник (подразделение), ответственный за организацию обработки ПДн в компании		
В Роскомнадзор направлено Уведомление об обработке персональных данных		
Проведена классификация (для ГИС и МИС) ИСПДн		
Проведено определение уровня защищенности ПДн в ИСПДн (для иных ИСПДн)		
Разработана модель угроз безопасности ПДн		
Разработано техническое задание на создание системы защиты ПДн		

АНКЕТА № 2

Обследование

Процессы

В таблице 1 перечислены основные процессы, общие для большинства компаний. В соответствующих столбцах знаками “+” или “–“ укажите те процессы компании, в ходе которых осуществляется обработка (в т.ч. хранение) ПДн, а также передан ли рассматриваемый процесс на аутсорсинг (выполняется сторонней компанией).

При необходимости, дополните таблицу необходимым числом строк с названиями процессов компании, отсутствующих в таблице. Где это применимо, в графе Примечание укажите наименования используемых автоматизированных систем (по таблице 2).

Таблица 1 – Процессы, в ходе которых обрабатываются ПДн

Процесс	Обработка ПДн (+ / –)	Аутсорсинг (+ / –)	Примечание (используемые АС)
Работа с персоналом			
Бухгалтерский учет			

Процесс	Обработка ПДн (+ / –)	Аутсорсинг (+ / –)	Примечание (используемые АС)
Кассовые операции			
Системное администрирование			
Охрана и контроль доступа			
Заключение договоров			
Работа с контрагентами			
Привлечение клиентов			
Ваш_процесс_1			
Ваш_процесс_2			

Автоматизированная обработка

Автоматизированная обработка *– обработка ПДн с помощью средств вычислительной техники.*

В таблице 2 укажите автоматизированные системы (АС) компании, в которых обрабатываются ПДн (рекомендуется проанализировать участие АС в процессах , приведенных в таблице 1).

В соответствующем столбце перечислите имеющиеся эксплуатационную документацию на рассматриваемую АС (руководства по эксплуатации, описания и др.).

Для облегчения понимания структуры АС рекомендуется приложить к анкете соответствующие схемы (топологии). При невозможности предоставить схему какой-либо АС, в столбце Примечание введите ее краткое описание (например, *1 физ. сервер + база данных, доступ с АРМов бухгалтеров, в отдельной подсети)*

Таблица 2 – Автоматизированные системы, в которых обрабатываются ПДн

АС, в которой обрабатываются ПДн	Эксплуатационные документы	Примечание (описание АС)
Ваша_АС_1		
Ваша_АС_2		

Филиалы

При обработке ПДн в филиалах (или дополнительных офисах) компании, в ходе обследования для получения необходимой информации может потребоваться их посещения. В таблице укажите информацию о тех филиалах компании, сотрудники которых осуществляют обработку персональных данных (проанализируйте их участие в процессах и используемые АС).

В соответствующем столбце для каждого филиала укажите наименования процессов и АС по таблицам 1 и 2.

Таблица 3 – Филиалы компании, в которых обрабатываются ПДн

Наименование филиала	Адрес	Выполняемые процессы и используемые АС
Ваш_филиал_1		
Ваш_филиал_2		
…		

АНКЕТА № 3

Документы

Документы

В таблице перечислены основные локальные нормативные документы, регламентирующие процессы обработки и защиты информации). В соответствующем столбце отметьте документы, существующие в компании.

При необходимости, дополните таблицу необходимым числом строк с названиями документов, отсутствующих в таблице.

Таблица – Документы, регламентирующие обработку ПДн

Наименование документа	**Примерное содержание**	**+ / –**	**Примечание**
Политика (положение, концепция) обработки персональных данных	Требования к процессам обработки и защиты ПДн в компании		
Инструкция по обработке ПДн	Порядок (регламент) действий по обработке ПДн сотрудниками		
Инструкция по реагированию на запросы субъектов	Порядок (регламент) действий по подготовке ответов на запросы		
Инструкция по защите ПДн	Порядок (регламент) выполнения требований по защите ПДн		
Инструкция по устранению нарушений при обработке ПДн	Порядок (регламент) устранения допущенных нарушений		
Перечень обрабатываемых ПДн	Перечень ПДн, целей, оснований и сроков их обработки		
…			
Списки сотрудников, имеющих право на обработку ПДн (в т.ч. в ИСПДн)	Список сотрудников, которые имеют право работать с ПДн		
Ваш_документ_1			
Ваш_документ_2			
…			

АНКЕТА № 4

Техническая защита персональных данных

Необходимые сведения

Решение по технической защите ПДн разрабатывается исходя из результатов классификации (определения уровня защищенности ПДн) ИСПДн и модели угроз и оформляется в виде проекта Технического задания на создание системы защиты ПДн (СЗПДн).

Для разработки СЗПДн необходимо:

- отчет или иной документ с результатами обследования;
- сведения об ИСПДн (описания, схемы, эксплуатационная документация и др.);
- акты классификации (уровня защищенности ПДн) ИСПДн;
- модели угроз безопасности ПДн в ИСПДн;
- перечень средств защиты и сведения об имеющихся у них сертификатах.

В зависимости от содержания предоставленных документов может потребоваться необходимость уточнения полученных сведений.

Средства защиты

При разработке решения по технической защите ПДн целесообразно использовать, где это возможно, уже имеющиеся в компании сертифицированные СЗИ. В таблице укажите информацию о СЗИ, установленных в ИСПДн.

В соответствующем столбце для каждого филиала укажите наименование, номер и срок действия сертификата на СЗИ (если такой имеется), а также наименование выдавшего его органа.

Таблица 3 – Средства защиты

Средство защиты	Сертификат	АС, в которых установлено средство защиты
Средство_защиты_1		
Средство_защиты_2		

ПРИЛОЖЕНИЕ В

Процесс обработки персональных данных «ПРИЕМ НА РАБОТУ»

Описание процесса

Процесс обработки персональных данных «Прием на работу» включает действия, начиная с написания новым работником заявления о приеме на работу и заканчивая моментом начала выполнения им своих обязанностей.

Схема процесса приведена на рисунке В.1.

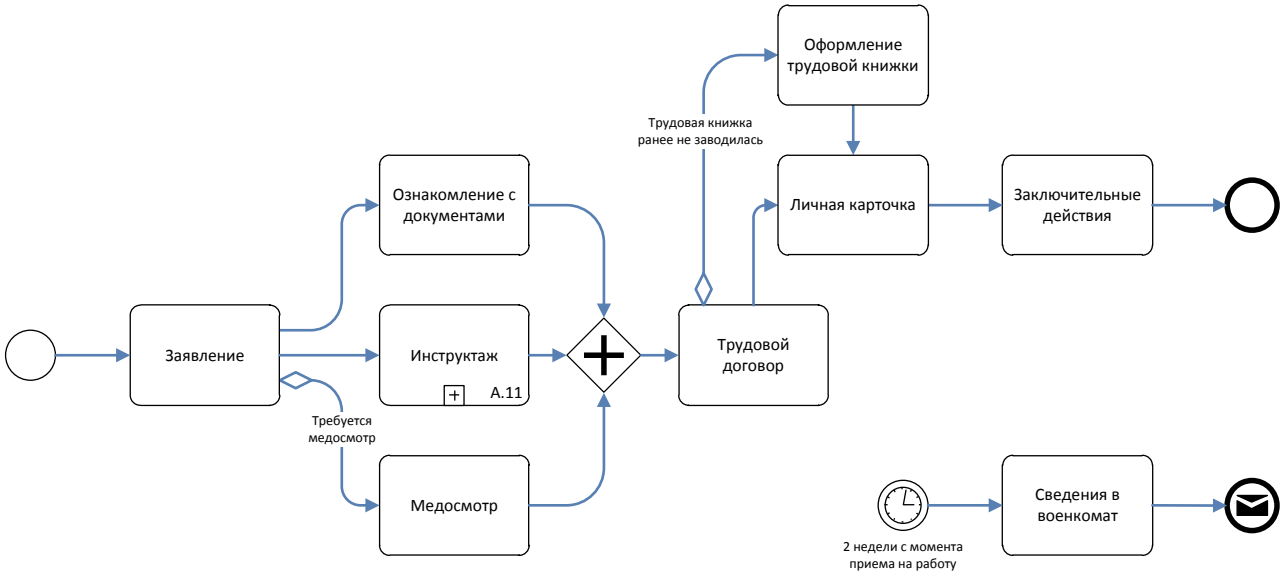


Рисунок В.1 – Схема процесса «Прием на работу»

Заключительные действия включают передачу необходимых для начисления заработной платы документов в бухгалтерию, выдачу электронного пропуска, создание учетных записей и др.

Сведения об обработке персональных данных

Обрабатываются следующие персональные данные:

- адрес места жительства (фактический и регистрации), дата регистрации по месту жительства и гражданство;
- дата и место рождения,
- личная подпись;

- место работы, должность, а также дополнительная информация о текущем месте работы (вид и характер работы, стаж, дата приема на работу и др.);
- номер телефона (домашний, мобильный);
- пол;
- сведения о близких родственниках;
- сведения о заработной плате, размере оклада и прочих выплатах;
- сведения о наличии противопоказаний;
- сведения о наличии социальных льгот;
- сведения об образовании (ВУЗ, квалификация, специальность, знания иностранных языков и др.);
- семейное положение,
- фотография;
- Ф.И.О.

Дополнительно обрабатываются персональные данные, содержащиеся в следующих документах:

- документ о воинском учете;
- документы об образовании;
- паспорт или иной документ, удостоверяющий личность;
- свидетельство о присвоении ИНН;
- страховое свидетельство государственного пенсионного страхования;
- трудовая книжка;
- копия свидетельства о браке;
- копия свидетельств о рождении (детей).

Все персональные данные получаются непосредственно от субъектов.

Сведения о материальных носителях персональных данных

Персональные данные содержатся в следующих документах:

1. Заявления:
    - Заявление о приеме на работу;
    - Заявление на удержание стоимости трудовой книжки;
    - Заявление на выдачу электронного пропуска;
    - Заявка на создание учетных записей;
2. Документы установленной формы:
    - Направление на медосмотр;
    - Трудовой договор;
    - Приказ о приеме на работу;
    - Личная карточка Т-2;
    - Сведения в военкомат;

3. Журналы, книги, списки ознакомления:

- Списки ознакомления с внутренними документами;
- Лист ознакомления с должностной инструкцией;
- Журнал учета должностных инструкций;
- Журналы проведения инструктажей;
- Журнал регистрации трудовых договоров и изменений к ним;
- Приходно-расходная книга по учету бланков трудовой книжки и вкладышей в нее;
- Книгу учета движения, выдачи трудовых книжек и вкладышей.

4. Копии документов субъекта.

Также в Учреждении на период работы хранится трудовая книжка.

Используемые ИСПД:
- «Бухгалтерия и кадры»;
- Корпоративный портал ЗАО «….» (заявка на создание учетных записей);
- «Локальная сеть …» (подготовка документов).

Дополнительно заводятся учетные записи в ИСПДН «Lotus» и Домен, заносится информация в телефонную базу «….».

Цели и основания обработки персональных данных

Обработка персональных данных осуществляется в следующих целях:
- трудоустройство и обеспечение условий труда работника;
- обеспечение функционирования учреждения (подтверждение ознакомления сотрудника с внутренними документами, выдачи документов и др.);
- обеспечение охраны труда;
- оформление трудовой книжки;
- обеспечение условий труда работника (создание учетных записей, выдача пропуска и др.);
- предоставление сведений в военкомат;
- информационное обеспечение.

Основанием обработки персональных данных, в соответствии со ст.6 ФЗ-152 является необходимость выполнения требований федеральных законов:
- Трудовой кодекс РФ;
- Федеральный закон «Об обязательном пенсионном страховании в Российской Федерации» №167-ФЗ от 15.12.2001 г.;
- Федеральный закон «Об основах обязательного социального страхования» №165-ФЗ от 16.07.1999 г.;
- Федеральный закон «О воинской обязанности» №53-ФЗ от 28.03.1998.

В ряде случаев основанием обработки является письменное согласие сотрудника.

Доступ к персональным данным

К персональным данным имеют доступ следующие должностные лица:
- директор;
- менеджер по персоналу;
- главный бухгалтер;
- инженер по охране труда.

В ходе процесса персональные данные передаются ввоенкомат по месту прописки (на основании Федерального закона «О воинской обязанности и военной службе» от 28 марта 1998 года № 53-ФЗ).

Документы, содержащие персональные данные, хранятся в шкафах на рабочих местах менеджера по персоналу (пом. №), главного бухгалтера (пом. №) и инженера по охране труда (пом. №).

Сроки хранения и перечень лиц, ответственных за хранение документов, содержащих персональные данные, приведены в таблице В.1.

Таблица В.1

Документ	Ответственный	Срок хранения
Заявление о приеме на работу	Менеджер по персоналу	См. примечание
Списки ознакомления с внутренними документами	Менеджер по персоналу	До замены документа
Лист ознакомления с должностной инструкцией	Менеджер по персоналу	До замены документа
Журнал учета должностных инструкций	Менеджер по персоналу	До замены документа
Журналы проведения инструктажей	Инженер по охране труда	До замены документа
Направление на медосмотр (заключение медкомиссии)	Менеджер по персоналу	См. примечание
Трудовой договор	Менеджер по персоналу	См. примечание
Журнал регистрации трудовых договоров и изменений к ним	Менеджер по персоналу	До замены документа

Документ	Ответственный	Срок хранения
Приказ о приеме на работу	Главный бухгалтер, менеджер по персоналу	См. примечание
Заявление на выдачу электронного пропуска	Менеджер по персоналу	До момента передачи в ЗАО «ЭВРИКА»
Заявление на удержание стоимости трудовой книжки	Главный бухгалтер	5 лет
Приходно-расходная книга по учету бланков трудовой книжки и вкладышей в нее	Менеджер по персоналу	3 года
Трудовая книжка сотрудника	Менеджер по персоналу	На период работы
Книгу учета движения, выдачи трудовых книжек и вкладышей	Менеджер по персоналу	50 лет
Личная карточка Т-2	Менеджер по персоналу	См. примечание
Копии документов у менеджера по персоналу	Менеджер по персоналу	См. примечание
Копии документов в бухгалтерии	Главный бухгалтер	5 лет
Сведения в военкомат	Менеджер по персоналу	3 года

Процесс обработки персональных данных «УВОЛЬНЕНИЕ»

Описание бизнес-процесса

Схема процесса приведена на рисунке В.2

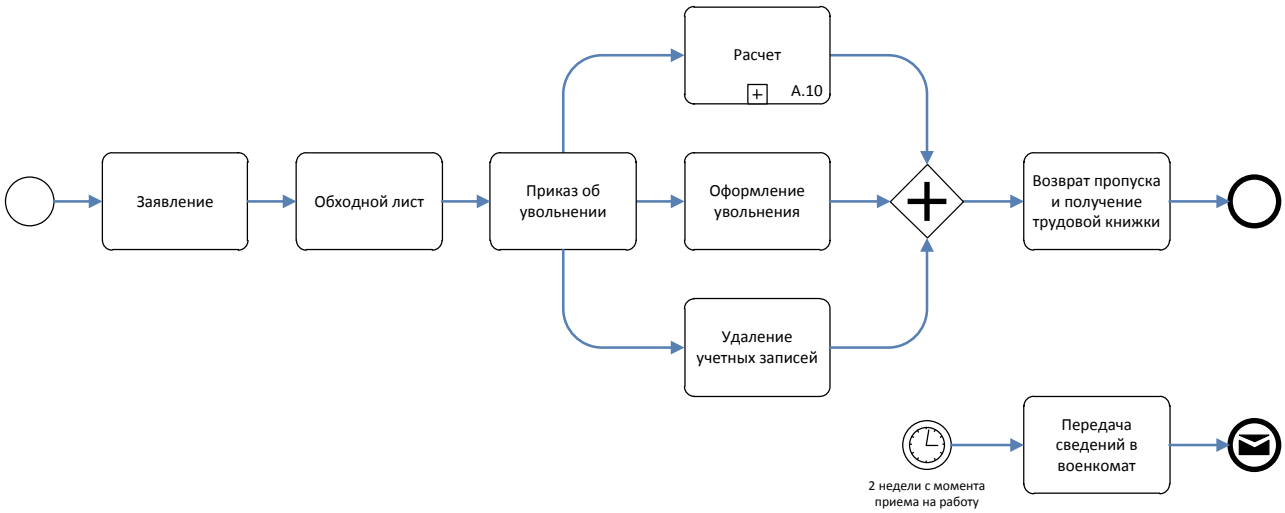


Рисунок В.2 – Схема бизнес-процесса «Увольнение»

Сведения об обработке персональных данных

В ходе бизнес-процесса обрабатываются следующие персональные данные:
- личная подпись;
- место работы и должность;
- сведения о заработной плате, размере оклада и прочих выплатах;
- Ф.И.О.

Используются персональные данные, полученные непосредственно от субъекта при приеме на работу.

Сведения о материальных носителях персональных данных

Персональные данные содержатся в следующих документах:
- Заявление об увольнении;
- Обходной лист;
- Записка-расчет;
- Дополнительное соглашение;
- Приказ об увольнении.

Дополнительно используются документы и ИСПДн, указанные в описании бизнес-процесса «Прием на работу» (Приложение В.1).

Цели и основания обработки персональных данных

Обработка персональных данных в ходе бизнес-процесса осуществляется в целях:
- увольнение сотрудника;
- предоставление сведений в военкомат.

Основанием обработки персональных данных, в соответствии со ст.6 ФЗ-152 является необходимость выполнения требований федеральных законов:
- Трудовой кодекс РФ;
- Федеральный закон «О воинской обязанности» №53-ФЗ от 28.03.1998.

Доступ к персональным данным

К персональным данным имеют доступ следующие сотрудники:
- директор;
- менеджер по персоналу;
- главный бухгалтер.

В ходе бизнес-процесса персональные данные передаются следующим организациям в военкомат по месту прописки (на основании Федерального закона «О воинской обязанности и военной службе» от 28 марта 1998 года № 53-ФЗ).

Документы, содержащие персональные данные, хранятся в шкафах на рабочих местах менеджера по персоналу (пом. №…) и главного бухгалтера (пом. №…).

Сроки хранения и перечень лиц, ответственных за хранение документов, содержащих персональные данные, приведены в таблице В.2.

Таблица В.2

Документ	**Ответственный**	**Срок хранения**
Заявление об увольнении	Менеджер по персоналу	1 год с момента увольнения сотрудника, 75 лет в архиве
Обходной лист	Менеджер по персоналу	
Приказ об увольнении	Менеджер по персоналу	
Дополнительное соглашение	Менеджер по персоналу	
Записка-расчет	Главный бухгалтер	5 лет

ПРИЛОЖЕНИЕ Г

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО – РАСПОРЯДИТЕЛЬНЫХ, ПРОЕКТНЫХ И ЭКПЛУАТАЦИОННЫХ ДОКУМЕНТОВ НА ИСПДн ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ

№ п/п	Наименование документа
1	**Правовые акты (Приказы)**
1.1	О мерах по защите персональных данных, обрабатываемых в Учреждении от неправомерного или случайного доступа к ним
1.2	О проведении внутренней проверки Учреждении по вопросам соответствия требованиям ФЗ «О персональных данных»
1.3	О назначении ответственного должностного лица (создании постоянно-действующей комиссии) по организации обработки и защиты персональных данных».
1.4	О назначении подразделения (лица), ответственного за безопасность обработки персональных данных.
1.5	О создании комиссии по определению уровня защищенности персональных данных в информационных систем персональных данных
1.6	Об определении перечня должностей персонала, допущенных к обработке персональных данных в Учреждении для выполнения ими служебных (трудовых) обязанностей
1.7	Об определении помещений для обработки персональных данных. Приложение №1 к приказу. Перечень помещений, предназначенных для обработки персональных данных
1.8	Об ознакомлении работников с положениями законодательства Российской Федерации по защите персональных данных и документами, определяющими политику в отношении обработки персональных данных.
2	**Организационно – распорядительные документы**
2.1	Концепция информационной безопасности информационных систем персональных данных в Учреждении
2.2	Политика информационной безопасности информационных систем персональных данных в Учреждении
2.3	Правила проведения внутренней проверки соответствия обработки персональных данных, обрабатываемых в Учреждении ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам.

2.4	Положение об обработке и обеспечении безопасности персональных данных в Учреждении
2.5	Перечень персональных данных работников и клиентов, обрабатываемых в ИСПДн и без использования средств автоматизации в Учреждении
2.6	Перечень должностей работников, допущенных к обработке персональных данных в Учреждении для выполнения ими служебных (трудовых) обязанностей
2.7	Инструкция о порядке рассмотрения обращений граждан - субъектов персональных данных, либо их представителей, а также уполномоченного органа по защите прав субъектов персональных данных
2.8	Инструкция по защите персональных данных, обрабатываемых без использования средств автоматизации
2.9	Акт определения уровня угроз персональным данным обрабатываемых в ИСПДн
2.10	Листы ознакомления работников Учреждения непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных, с документами и локальными актами, определяющими политику в отношении обработки персональных данных
2.11	Согласие работника на обработку персональных данных
2.12	Отзыв согласия на обработку персональных данных
2.13	Заявление-согласие субъекта на получение его персональных данных у третьей стороны
2.14	Заявление-согласие субъекта на передачу его персональных данных третьей стороне
2.15	Обязательство работника о неразглашении информации, содержащей персональные данные
2.16	Списки работников для организации допуска в помещения, предназначенные для обработки персональных данных
2.17	Уведомление об обработке персональных данных
3	**Технические документы на ИСПДн**
3.1	Техническое задание на разработку системы обеспечения безопасности информации ИСПДн учреждения
3.2	Технический проект на создание системы обеспечения безопасности информации ИСПДн учреждения
3.3	Модель угроз персональным данным ИСПДн

3.4	Акт определения уровня защищенности ПДн, обрабатываемых в ИСПДн (для иных ИС)
4	**Эксплуатационные документы**
4.1	Инструкция администратора ИСПДн
4.2	Инструкция администратора безопасности ИСПДн
4.3	Инструкция пользователя ИСПДн
4.4	Должностные инструкции работников Учреждения, имеющих доступ к информационным системам персональных данных с разделом (типовым приложением) в части обеспечения безопасности персональных данных в процессе их обработки
4.5	Инструкция по учету съемных носителей информации ИСПДн
4.6	Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн
4.7	Акты установки средств защиты информации в ИСПДн
4.8	Акты уничтожения персональных данных
4.9	Журнал учета сертифицированных средств защиты информации, эксплуатационной и технической документации к ним
4.10	Журнал учета электронных носителей персональных данных
4.11	Журнал учета ключевых носителей
4.12	Журнала учета средств криптографической защиты информации
5	**Плановые документы**
5.1	План работ по приведению в соответствие обработки персональных данных в Учреждении ФЗ Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам
5.2	План работ по защите персональных данных, обрабатываемых в Учреждении, в соответствии с ФЗ Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами.
5.3	План работы комиссии по проведения внутренней проверки соответствия обработки персональных данных, обрабатываемых в Учреждении ФЗ РФ от 27.07.2006 г.№152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам
5.4	План работ по обеспечению соответствия обработки персональных данных Учреждении ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» на 2014 год
5.5	План работ по защите персональных данных, обрабатываемых в Учреждении в соответствии с ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» на год

6	**Отчетные документы**
6.1	Отчет о результатах внутренней проверки соответствия обработки персональных данных, обрабатываемых в Учреждении ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»
6.2	Отчет о выполнении Плана работ по защите персональных данных, обрабатываемых в Учреждении в соответствии с ФЗ Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных» на год

ПРИЛОЖЕНИЕ Д

ТИПОВОЙ ОБРАЗЕЦ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

УТВЕРЖДАЮ

_____

[НАИМЕНОВАНИЕ
ДОЛЖНОСТИ РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]

« ___ » _____ 201. г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
[НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

Санкт-Петербург 201[ ]

ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение документа

1.1.1 Положение об обработке персональных данных в информационных системах персональных данных [НАИМЕНОВАНИЕ] (далее – Положение) определяет порядок сбора, хранения, передачи и иных видов обработки персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.1.2 Положение разработано в соответствии с ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 1.11. 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в ИСПДн», «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687.

1.1.3 Цель Положения – определение особенностей обработки персональных данных субъектов персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.2 Область действия документа

1.2.1 Действие Положения распространяется на ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], в которых осуществляется обработка персональных данных как с использованием средств автоматизации, так и без использования таковых.

1.2.2 Все работники [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], допущенные к работе с персональными данными, обрабатываемыми в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись.

1.3 Вступление в силу документа

1.3.1 Настоящее Положение вступает в силу с момента его утверждения [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] и действует бессрочно до замены его новым Положением.

1.3.2 Все изменения в Положение вносятся приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

2 КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ В [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] ПЕРСОНАЛЬНЫХ ДАННЫХ И ЦЕЛИ ИХ ОБРАБОТКИ

2.1 Персональные данные, обрабатываемые в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], относятся к сведениям конфиденциального характера.

2.2 Состав персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], определен в Перечне персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], утвержденном Приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], и содержит следующие категории персональных данных (в скобках указаны цели их обработки):

- персональные данные работников (исполнение обязательств по трудовому договору);

- персональные данные клиентов (исполнение обязательств по договору с клиентом);

- персональные данные клиентов по ОПС (исполнение обязательств по договору ОПС);

- персональные данные, обрабатываемые при трансферагентской деятельности (регистрация и передача в ПФР в электронном виде заявлений застрахованных лиц).

3 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В [ОРГАНИЗАЦИИ]

3.3 Сбор, хранение и уничтожение персональных данных.

3.1.1 Персональные данные поступают в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] непосредственно от субъекта на основании договорных отношений или от третьей стороны в рамках исполнения норм действующего законодательства Российской Федерации, обрабатываются и хранятся в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ не дольше, чем этого требуют цели обработки персональных данных и требования действующего законодательства Российской Федерации.

3.1.2 Если персональные данные работника [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] можно получить только от третьей стороны, то субъект персональных данных уведомляется о факте их получения заранее. При этом получение персональных данных работника от третьих лиц происходит в соответствии с Регламентом обмена (выдачи) информации.

3.1.3 В случае получения персональных данных правопреемника от лица, вступившего с [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] в договорные отношения, ответственность за уведомление правопреемника о факте передачи его персональных данных для обработки в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] возлагается на данное лицо.
3.1.4 Сроки хранения информации, содержащей персональные данные субъектов, определяются Перечнем персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].
3.1.5 Персональные данные субъектов обрабатываются в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] как в электронном виде (автоматизированная обработка), так и на бумажных носителях (обработка без использования средств автоматизации).

3.1 Особенности обработки персональных данных с использованием средств автоматизации.

3.2.1 Обработка персональных данных с использованием средств автоматизации осуществляется в ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]. Состав ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] определен Перечнем ИСПДн в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

3.2.2 Машинные носители данных, предназначенные для обработки персональных данных, подлежат обязательной регистрации и учету в соответствии с [НАИМЕНОВАНИЕ ДОКУМЕНТА, РЕГЛАМЕНТИРУЮЩЕГО ПРАВИЛА УЧЕТА И ХРАНЕНИЯ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ].

3.3 Особенности обработки персональных данных без использования средств автоматизации

3.3.1 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях.
3.3.2 Не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы. Для обработки каждой категории персональных данных должен использоваться отдельный бумажный носитель.
3.3.3 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна проводиться таким образом, чтобы обеспечивать раздельное хранение персональных данных разных целей обработки.
3.3.4 Уничтожение бумажных носителей персональных данных производится после поступления от начальников отделов, обрабатывающих персональные данные, в постоянно действующую

экспертную комиссию перечня (в том числе в электронном виде) подлежащих уничтожению бумажных носителей персональных данных с указанием основания для их уничтожения.

3.3.5 Бумажные носители уничтожаются исполнителем в присутствии членов постоянно действующей экспертной комиссии с оформлением акта (форма акта об уничтожении бумажных носителей представлена в Приложении к настоящему Положению) по следующей процедуре:
- включение каждого отобранного к уничтожению документа (дела) отдельной
позицией в акт;
- оформление в акте итоговой записи с указанием количества
документов (дел), подписание итоговой записи членами постоянно действующей экспертной комиссии, составившими акт;
- письменное согласование акта с руководителями структурных подразделений [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], направившими запрос на уничтожение бумажных носителей;
- подписание акта членами постоянно действующей экспертной комиссии;
- утверждение акта [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].
3.3.6 Перед непосредственным уничтожением бумажных носителей персональных данных членами постоянно действующей экспертной комиссии должна быть осуществлена сверка носителей с описью, приведенной в акте уничтожения.

3.4 Обеспечение безопасности персональных данных
3.4.1 При обеспечении безопасности персональных данных работники [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] руководствуются настоящим Положением и Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]
3.4.2 Бумажные носители персональных данных уничтожаются в присутствии членов постоянно действующей экспертной комиссии в составе не менее 3 человек, принимавших участие в сверке (проверке) документов и дел, подлежащих уничтожению. После уничтожения документов члены постоянно действующей экспертной комиссии производят запись в акте об уничтожении, заверяют ее своими подписями.
3.4.3 Уничтожение документов производится путем сожжения, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в кусочки площадью не более 2,5 кв. мм.

4 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ, ОБРАБАТЫВАЕМЫМ В [ОРГАНИЗАЦИИ]

4.1 Доступ работников к персональным данным субъектов персональных данных, обрабатываемым в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]
4.1.1 Работники [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] получают доступ к персональным данным субъектов персональных данных исключительно в объеме, необходимом для выполнения своих должностных обязанностей.
4.1.2 Список работников [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], имеющих доступ к персональным данным субъектов персональных данных, утвержден Перечнем подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

4.1.3 Перечень подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.) постоянно действующей экспертной комиссией по информационной безопасности на основании заявок начальников отделов.

4.1.4 Работнику [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], должность которого не включена в Перечень подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], но которому необходим разовый или временный доступ к персональным данным субъектов персональных данных в связи с исполнением должностных обязанностей, приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] может быть предоставлен такой доступ на основании письменного мотивированного запроса непосредственного руководителя работника.

4.1.5 Работник [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] получает доступ к персональным данным субъектов персональных данных после:
- ознакомления и изучения требований настоящего Положения и иных внутренних нормативных документов [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] по защите персональных данных в части, его касающейся;
- прохождения инструктажа о соблюдении правил обработки персональных
данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ];
- ознакомления с видами ответственности за нарушение (невыполнение) норм
законодательства РФ в сфере обработки персональных данных.

4.1.6 Право на получение информации, касающейся обработки персональных данных, закрепляется за субъектом персональных данных с момента заключения договора с [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] и действует на протяжении всего срока обработки персональных данных (включая хранение), предусмотренного действующим законодательством РФ.

4.1.7 Перед началом обработки персональных данных [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] уведомляет субъекта (лично или посредством направления заказного письма) о целях и способах обработки, невозможности прекращения обработки (блокирования, уничтожения) персональных данных субъекта до истечения предусмотренного действующим законодательством Российской Федерации срока архивного хранения данных.

4.1.8 Субъект персональных данных (или его законный представитель) может ознакомиться с перечнем персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], на официальном сайте [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] или при направлении письменного запроса в адрес [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

4.1.9 Сведения о каждом работнике [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] (Ф.И.О., должность и рабочий телефон), который имеет доступ к персональным данным субъекта, могут быть получены субъектом исключительно при направлении им письменного запроса в адрес [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

4.1.10 Письменный запрос субъекта должен быть удостоверен следующими документами:

общегражданским паспортом – в случае непосредственного обращения субъекта персональных данных с запросом в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ];

электронной цифровой подписью – в случае направления в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] электронного запроса;

нотариально заверенной подписью – в случае направления в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] почтового запроса;

документом, подтверждающим полномочия законного представителя субъекта персональных данных, – в случае направления в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] запроса от законного представителя субъекта персональных данных. При этом непосредственно запрос должен быть удостоверен одним из вышеприведенных способов.

4.1.11 Правопреемники субъекта персональных данных вправе получить от [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] информацию об обработке и доступ к своим персональным данным, полученным [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] от субъекта персональных данных в соответствии с

федеральным законодательством, на основании подлинника или нотариально заверенной копии документа о смерти субъекта ПДн.
4.1.12 Все поступившие письменные и электронные запросы субъектов персональных данных (или их законных представителей) регистрируются секретариатом с докладом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ], а затем направляются компетентному работнику для подготовки ответа субъекту не позднее одного рабочего дня с момента их поступления в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].
4.1.13 Ответ в письменной форме на запрос субъекта должен быть сформирован компетентным работником, подписан [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ]] в течение шести рабочих дней с даты поступления в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] запроса от субъекта персональных данных и отправлен секретариатом в срок, не превышающий трех рабочих дней, в адрес субъекта через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись).

4.2 ДОСТУП ТРЕТЬИХ ЛИЦ К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

4.2.1 Третьи лица, заключившие с [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] договор об обработке персональных данных клиентов [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], получают доступ к персональным данным субъектов в соответствии с Регламентом обмена/выдачи информации.

5 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными работодатель вправе применять предусмотренные ТК РФ дисциплинарные взыскания.
5.2. В случае нарушения установленного федеральным законодательством порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрены административные штрафы.

ПРИЛОЖЕНИЕ Е

ТИПОВОЙ ОБРАЗЕЦ ПОЛОЖЕНИЯ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

УТВЕРЖДАЮ
[НАИМЕНОВАНИЕ
ДОЛЖНОСТИ РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]
[НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ]
[Ф.И.О. РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]
«____» _____ 201. г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
[НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

Санкт-Петербург 20[ ]

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение документа

1.1.1 Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.1.2 Настоящее Положение разработано в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в ИСПДн», приказом ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн", приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности" и «Положением об обработке персональных данных в ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.1.3 Цель Положения – регулирование работ по защите персональных данных и обеспечение функционирования ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] в соответствии с требованиями действующего федерального законодательства в области информационной безопасности.

1.2 Область действия документа

1.2.1 Действие Положения распространяется на ИСПДн [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], в которых осуществляется обработка персональных данных как с использованием средств автоматизации, так и без использования таковых.

1.2.2 Все работники [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], допущенные к работе с персональными данными, обрабатываемыми в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

1.3 Вступление в силу документа

1.3.1 Настоящее Положение вступает в силу с момента его утверждения [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] и действует бессрочно до замены его новым Положением.

1.3.2 Все изменения в Положение вносятся приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.4 Планирование работ по обеспечению безопасности персональных данных

1.4.1 В целях исполнения настоящего Положения и на основании Положения о постоянно действующей экспертной комиссии по информационной безопасности (далее – ПДЭК) ПДЭК ежегодно составляет и утверждает у [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] план работ по обеспечению безопасности персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.4.2 Проводимые в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] мероприятия по обеспечению безопасности персональных данных учитываются в Журнале учета мероприятий по защите персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ].

1.4.3 Выполнение работ по обеспечению безопасности персональных данных

1.4.4 В целях организации и проведения работ по обеспечению безопасности персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] Приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] назначаются:

- уполномоченное лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;
- администратор (-ы) информационной безопасности, ответственный (-ые) за установку, настройку и обслуживание средств защиты информации, применяемых для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными.

Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

- определение и описание информационных систем персональных данных;
- определение уровня защищенности персональных данных в информационных системах персональных данных;
- определение актуальных угроз безопасности персональных данных;

- проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;
- закупку, установку и настройку технических средств защиты информации;
- внедрение организационных мер и разработку соответствующих регламентов и положений;
- инструктаж и обучение лиц, которые будут использовать средства защиты информации.

1.4.5 Начальники отделов, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных и других установленных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] требований.

1.4.6 Для обеспечения безопасности персональных данных применяются следующие меры безопасности:

- организационные меры безопасности:
- инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;
- учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;
- мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;
- постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);
- меры физической безопасности:
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] устанавливается контролируемая зона [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ], вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

технические меры безопасности:
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- предотвращение внедрения в информационные системы вредоносных программ (программ - вирусов) и программных закладок. Ремонтно-восстановительные работы технических средств обработки информации проводятся под контролем администратора безопасности с привлечением работников IT подразделения. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

1.5 Контроль выполнения работ по обеспечению безопасности персональных данных

1.5.1 Контроль выполнения работ по обеспечению безопасности персональных данных в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

1.5.1 В рамках проведения контрольных мероприятий выполняются:
- проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;
- проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;
- проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;
- проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;
- инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

- проверка соответствия моделей угроз для ИСПДн условиям функционирования данных систем;
- проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

1.5.2 Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

1.5.3 Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и вне плана по решению руководителя организации и в случае возникновения инцидентов информационной безопасности.

1.5.4 Внутренние проверки в [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] в обязательном порядке проводятся в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- халатность и несоблюдение требований к обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

1.5.5 Задачами внутренней проверки являются:
- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

1.6 Совершенствование системы защиты персональных данных

1.6.1 Ежегодно ПДЭК направляет [НАИМЕНОВАНИЕ ДОЛЖНОСТИ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ] [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных, обрабатываемых в [НАИМЕНОВАНИЕ ВЫШЕСТОЯЩЕЙ ОРГАНИЗАЦИИ], вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

1.6.2 Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:
- результатами проведенных аудитов и контрольных мероприятий;

- изменениями федерального законодательства в области персональных данных;
- изменениями структуры процессов обработки персональных данных;
- результатами анализа инцидентов информационной безопасности;
- результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;
- жалобами и запросами субъектов персональных данных.

ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ
[НАИМЕНОВАНИЕ
ДОЛЖНОСТИ РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]
[НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ]
[Ф.И.О. РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]
«____» _____ 201. г.

ТИПОВАЯ ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Должностная инструкция ответственного за организацию обработки персональных данных (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", постановлением Правительства Российской Федерации 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", другими нормативными правовыми актами.

2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки персональных данных.

3. Ответственный за организацию обработки персональных данных отвечает за осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений работников соответствующих структурных подразделений положений законодательства Российской Федерации о персональных данных, правовых актов по вопросам обработки персональных данных, требований

к защите персональных данных, организации приема и обработки обращений и осуществлению контроля за приемом и обработкой таких обращений.

4. Ответственный за организацию обработки персональных данных обязан:

- определить 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;
- определять порядок и условия применения средств защиты информации;
- анализировать эффективность применения мер по обеспечению безопасности персональных данных;
- контролировать состояние учета машинных носителей персональных данных;
- проверять соблюдение правил доступа к персональным данным;
- контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

5. Ответственный за организацию обработки персональных данных имеет право:

- осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных;
- запрашивать у руководителя_____ информацию, необходимую для реализации полномочий;
- требовать от ответственных должностных лиц за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- применять меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить руководителю_____ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить руководителю_____ предложения о привлечении к дисциплинарной ответственности работников _____, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

ПРИЛОЖЕНИЕ 3

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО РАБОТНИКА, НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СЛУЧАЕ РАСТОРЖЕНИЯ С НИМ СЛУЖЕБНОГО КОНТРАКТА ПРЕКРАТИТЬ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ ЕМУ В СВЯЗИ С ИСПОЛНЕНИЕМ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ

Я,

_____,

(фамилия, имя, отчество полностью)

являясь работником_____,

_____,

(указать наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (трудового договора).

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ "___" _____ 201_ г.

(фамилия, инициалы) (подпись)

ПРИЛОЖЕНИЕ И

ТИПОВАЯ ФОРМА СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОГЛАСИЕ
на обработку персональных данных

Согласие на обработку персональных данных			
(информация о субъекте персональных данных)			
Я			
	(фамилия)	(имя)	(отчество)
(основной документ, удостоверяющий личность)		(номер основного документа, удостоверяющего личность)	
(сведения о дате выдачи указанного документа)		(сведения о выдавшем указанный документ органе)	
зарегистрированный по адресу:			
		(адрес)	
(информация о представителе субъекта персональных данных)			
Я			
	(фамилия)	(имя)	(отчество)
(основной документ, удостоверяющий личность)		(номер основного документа, удостоверяющего личность)	
(сведения о дате выдачи указанного документа)		(сведения о выдавшем указанный документ органе)	
зарегистрированный по адресу:			
		(адрес)	
наименование и реквизиты документа, подтверждающего полномочия представителя: >			

принимаю решение о предоставлении своих персональных данных в составе:
(перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)
(в случае обработки специальных категорий персональных данных работника)
сведения о состоянии здоровья сотрудника в объеме сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции
сведения о наличии судимости
(в случае обработки биометрических персональных данных)
личная подпись
фотография
и даю согласие на их обработку, включающую:
1. сбор
2. запись
3. систематизацию
4. накопление
5. хранение
6. уточнение (обновление)
7. уточнение (изменение)
8. извлечение
9. использование
10. передачу (предоставление)
11. передачу (доступ)
12. обезличивание
13. блокирование
14. удаление
15. уничтожение
(в случае обработки общедоступных персональных данных)
16. передачу (распространение)
персональных данных
(перечень действий с персональными данными, на совершение которых дается согласие)
способами, определяемыми (перечислить договоры, регламенты,

правила, инструкции и положения, которые определяют работу в ИСПДн и программных продуктах таких систем) или
(перечислить способы обработки и в каких информационных системах персональных данных производится обработка персональных данных)
(общее описание используемых оператором способов обработки персональных данных)
своей волей и в своем интересе (наименование оператора) расположенному по адресу:
с целью:
(цель или цели обработки персональных данных)
создания общедоступного источника персональных данных

на срок:	
	(срок, в течение которого действует согласие)

Порядок отзыва согласия:
Отзыв согласия подается в письменном виде лицом, указанным в согласии на обработку персональных данных, лично. Отзыв должен содержать: - номер основного документа, удостоверяющего личность субъекта персональных данных; - сведения о дате выдачи указанного документа и выдавшем его органе; - собственноручную подпись субъекта персональных данных; - сведения о согласии на обработку персональных данных (дата и адрес, по которому давалось согласие). При подаче лицом, осуществляющим прием такого отзыва, производится удостоверение личности подающего такой отзыв. Отзыв согласия осуществляется по адресу:
В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекращение обработки персональных данных и уничтожение персональных данных будет произведено в течение 30 дней с момента поступления
Порядок защиты субъектом персональных данных своих прав и законных интересов:
осуществляется в соответствии с требованиями Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ
(в случае если обязанность предоставления персональных данных установлена федеральным законом)

Юридические последствия отказа предоставить свои персональные данные, если обязанность предоставления персональных данных установлена федеральным законом:
(в случае исключительно автоматизированной обработки данных)
Порядок принятия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:
Возможные юридические последствия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:
Порядок защиты субъектом персональных данных своих прав и законных интересов
("я возражаю против решения исключительно автоматизированной обработки моих персональных данных" - заполняется собственноручно в случае такого возражения)
Наименование оператора, которому будут передаваться персональные данные
Адрес оператора, которому будут передаваться персональные данные
Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных
Срок, в течение которого действует согласие на передачу
(в случае обработки общедоступных персональных данных)
Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов
(в случае трансграничной передачи персональных данных)
Наименование оператора, которому будут передаваться персональные данные

Иностранные государства, которым будут передаваться персональные данные
Цель передачи персональных данных
Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных
Я подтверждаю, что предоставленные мною персональные данные являются полными, актуальными и достоверными
Я обязуюсь своевременно извещать об изменении предоставленных персональных данных

"		"		20		г.		
							(личная подпись)	(инициалы, фамилия)

Предоставленные данные соответствуют предъявленным документам, удостоверяющим личность

"		"		20		г.			
							(должность)	(личная подпись)	(инициалы, фамилия)

ПРИЛОЖЕНИЕ К

ТИПОВАЯ ФОРМА
РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ
ЮРИДИЧЕСКИХ
ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

РАЗЪЯСНЕНИЕ
субъекту персональных данных юридических последствий
отказа представить свои персональные данные
(для государственных служащих)

Мне,_____,
(фамилия, имя, отчество)
разъяснены юридические последствия отказа предоставить свои персональные данные
_____.

В соответствии со статьями 26, 42 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации", Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30.05.2005 № 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением или прохождением государственной гражданской службы.

Без представления субъектом персональных данных обязательных для заключения служебного контракта сведений служебный контракт не может быть заключен.

На основании пункта 11 части 1 статьи 33 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности гражданской службы.

_____

(дата) (Ф.И.О. полностью, подпись)

(для работников)

В соответствии со статьями 57, 65, 69 Трудового кодекса РФ субъект персональных данных, лицо, поступающее на работу или работающее обязано, представить определенный перечень информации о себе.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса РФ трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

_____

(дата) (Ф.И.О. полностью, подпись)

ПРИЛОЖЕНИЕ Л

ТИПОВАЯ ИНСТРУКЦИЯ О ПОРЯДКЕ ДОСТУПА РАБОТНИКОВ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Инструкция определяет порядок доступа в помещения, в которых ведется обработка персональных данных (далее - Инструкция), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в_____, и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящая Инструкция обязательна для применения и исполнения всеми работниками _____.

3. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранной сигнализацией.

4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш - карты) хранятся в металлических шкафах, оборудованных опечатывающими устройствами.

6. Помещения, в которых ведется обработка персональных данных, запираются на ключ, а в нерабочее время подключаются к охранной сигнализации.

7. Вскрытие и закрытие (опечатывание) помещений, в которых ведется обработка персональных данных, производится работниками, имеющими право доступа в данные помещения.

8. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть и опечатать шкафы;

отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

закрыть окна;

подключить охранную сигнализацию.

9. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:

провести внешний осмотр с целью установления целостности двери и замка;

открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

10. При обнаружении неисправности двери и запирающих устройств работники обязаны:

не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю;

в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

составить акт о выявленных нарушениях и передать его руководителю _____для организации служебного расследования.

11. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

13. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

14. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго, водо и теплоснабжения помещение, в котором ведется обработка персональных данных, вскрывается комиссией в составе не менее двух человек.

15. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей подразделений, обрабатывающих персональные данные.

ПРИЛОЖЕНИЕ М

ТИПОВОЕ ПОЛОЖЕНИЕ ОБ ОСОБЕННОСТЯХ И ПРАВИЛАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Обработка персональных данных, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.2 Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ.

2 ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.2 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3 Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных 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 _____.

2.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

2.4.1 типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование _____ и адрес _____, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых _____ способов обработки персональных данных;

2.4.2 типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

2.4.3 типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

2.5 При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение №__или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала должна быть предусмотрена актом _____, 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;

- копирование содержащейся в таких журналах информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

2.6 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, зачеркивание, стирание).

2.7 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1 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.

3.2 Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

3.3 При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом.

Лист ознакомления
с Положением об особенностях и правилах осуществления обработки персональных данных без использования средств автоматизации

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом

ПРИЛОЖЕНИЕ Н

УТВЕРЖДАЮ

_____

[НАИМЕНОВАНИЕ
ДОЛЖНОСТИ
РУКОВОДИТЕЛЯ
ОРГАНИЗАЦИИ]

« ___ » _____ 201. г.

ТИПОВОЙ ПЛАН

МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Санкт-Петербург 201.

1 Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.
План составлен на основании списка мер, методов и средств защиты, определенных в Концепции информационной безопасности и Политике информационной безопасности.
Выбор конкретных мероприятий осуществляется на основании анализа Отчета по результатам внутренней проверки и Модели угроз безопасности.
В План включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План включена следующая информация:

- Название мероприятия.
- Периодичность мероприятия (разовое/периодическое).
- Исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных Учреждения.

2 План мероприятий по обеспечению безопасности персональных данных

Мероприятия	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Первичная внутренняя проверка	Разовое срок до 01.01.201**.**	
Определение перечня ИСПДн	Разовое срок до	
Определение обрабатываемых ПДн и объектов защиты	**Разовое** **срок до**	
Определение круга лиц участвующих в обработке ПДн	**Разовое** **срок до**	
Определение ответственных лиц, участвующих в обработке	Разовое срок до	
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до	

Мероприятия	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Назначение ответственного за безопасность ПДн	Разовое срок до	
Введение режима защиты ПДн	Разовое срок до	
Утверждение Концепции информационной безопасности	Разовое срок до	
Утверждение Политики информационной безопасности	Разовое срок до	
Создание комиссии по определению уровня защищенности ПДн в ИСПДн	Разовое срок до	
Определение уровня защищенности всех выявленных ИСПДн	Разовое срок до	
Первичный анализ актуальности угроз безопасности ПДн	Разовое срок до	
Установление контролируемой зоны вокруг ИСПДн	Разовое срок до	
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц не допущенных к обработке ПДн	Разовое срок до	
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое срок до	
Организация порядка резервного копирования защищаемой информации на твердые носители	Разовое срок до	
Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн	Разовое срок до	
Введение в действие инструкции по порядку формирования, распределения и применения паролей	Разовое срок до	
Организация информирования и обучения сотрудников о порядке обработки ПДн	Разовое срок до	

Мероприятия	Периодичность	Исполнитель/ Ответственный
Организация информирования и обучения сотрудников о введенном режиме защиты ПДн	Разовое срок до	
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое срок до	
Разработка инструкций о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Разовое срок до	
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое срок до	
Разработка положения о внесении изменения в штатное программное обеспечение элементов ИСПДн	Разовое срок до	
Разработка положения о порядке внесения изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями. Положение должно включать в себя техническое задание на изменения, технический проект, приемо-сдаточные испытания, акт о введении в эксплуатацию.	Разовое срок до	
Организация журнала учета обращений субъектов ПДн	Разовое срок до	
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое срок до	
Физические мероприятия		
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до	
Внедрение технической системы контроля доступа в КЗ и помещения (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	

Мероприятия	Периодичность	Исполнитель/ Ответственный
Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	
Внедрение видеонаблюдения	Разовое срок до	
Установка дверей на входе в помещения с аппаратными средствами ИСПДн	Разовое срок до	
Установка замков на дверях в помещениях с аппаратными средствами ИСПДн	Разовое срок до	
Установка жалюзи на окнах	Разовое срок до	
Установка решеток на окнах первого и последнего этажа здания	Разовое срок до	
Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн	Разовое срок до	
Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн	Разовое срок до	
Установка систем бесперебойного питания на ключевые элементы ИСПДн	Разовое срок до	
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое срок до	
Технические (аппаратные и программные) мероприятия		
Внедрение единого хранилища зарегистрированных действий пользователей с ПДн	Разовое срок до	
Внедрение специальной подсистемы управления доступом, регистрации и учета (НАЗВАНИЕ)	Разовое срок до	
Внедрение антивирусной защиты (НАЗВАНИЕ)	Разовое срок до	

Внедрение межсетевого экранирования (НАЗВАНИЕ)	Разовое срок до	
Внедрение подсистемы анализа защищенности (НАЗВАНИЕ)	Разовое срок до	
Внедрение подсистемы обнаружения вторжений (НАЗВАНИЕ)	Разовое срок до	
Мероприятия	**Периодичность**	**Исполнитель/ Ответственный**
Внедрение криптографической защиты (НАЗВАНИЕ)	Разовое срок до	
Контролирующие мероприятия		
Создание журнал а внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно	
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Контроль над соблюдением режима защиты	Ежедневно	
Контроль над выполнением антивирусной защиты	Еженедельно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки ПДн	Ежегодно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии правовых актов и ОРД по защите персональных данных	Ежемесячно	

ПРИЛОЖЕНИЕ О. УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

_____

(полное и сокращенное наименования, фамилия, имя, отчество оператора)

_____

(адрес местонахождения и почтовый адрес оператора)

руководствуясь:

_____

(правовое основание обработки персональных данных)

_____

с целью:

_____

(цель обработки персональных данных)

_____

осуществляет обработку:

_____

(категории персональных данных)

_____

принадлежащих:

_____

(категории субъектов, персональные данные которых обрабатываются)

_____

Обработка вышеуказанных персональных данных будет осуществляться путем:

(перечень действий с персональными данными, общее описание используемых оператором способов

обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

(описание мер, предусмотренных ст. ст. 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ

“О персональных данных”, в т.ч. сведения о наличии шифровальных (криптографических)

средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование

юридического лица, ответственных за организацию обработки персональных данных,

и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных:

(при наличии трансграничной передачи персональных данных в процессе их обработки указывается перечень

иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных:

_____

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

_____

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных _____

(число, месяц, год)

Срок или условие прекращения обработки персональных данных:

_____

(число, месяц, год или основание (условие), наступление которого повлечет прекращение обработки

_____

персональных данных)

_____	_____	_____
(должность)	(подпись)	(расшифровка подписи)

«__» «_____» 201. г.

ПРИЛОЖЕНИЕ П

Перечень основных задач в области обеспечения защиты персональных данных и прогнозируемая оценка их трудоемкости без использования средств автоматизации

(Пример оценки для организации с числом АРМ и серверов до 1000)

№ п/п	Виды работ	Единица измерения	Без автоматизации		
			Норма на ед., (чел/час)	**Объем работы в год, в ед.**	**Трудозатраты в год, (чел/час)**
	Обеспечение безопасности ПДн				
	Учет лиц, допущенных к ПДн				
1.1	Определение лиц, которых надо допустить к работе с ПДн	Количество допускаемых лиц в год	0,02	100	1,67
1.2	Подготовка приказа на допуск лиц к работе с ПДн	Количество допускаемых лиц в год	0,08	100	8,33
1.3	Согласование приказа на допуск лиц к работе с ПДн	Количество выпускаемых приказов	0,08	100	8,33
	Учет обучения лиц, правилам защиты ПДн				
1.4	Учет лиц, прошедших обучение	Количество допускаемых лиц в год	0,02	100	1,67
1.5	Определение лиц, которые не прошли обучение	Количество допускаемых лиц в год	0,08	100	8,33
	Допуск лиц к СКЗИ				
1.6	Заполнение формы о лицах, допущенных к СКЗИ	Количество допускаемых к СКЗИ лиц в год	0,03	20	0,67

1.7	Отправка информации о допускаемых лицах в отдел ИБ	Количество допускаемых к СКЗИ лиц в год	0,02	20	0,33
1.8	Подготовка приказа на допуск к СКЗИ	Количество допускаемых к СКЗИ лиц в год	0,008	20	1,67
1.9	Заполнение формы о лицах, которым доступ к СКЗИ исключается	Количество лиц, которым допуск к СКЗИ убирается	0,02	20	0,33
1.10	Отправка информации об исключаемых лицах в отдел ИБ	Количество лиц, которым допуск к СКЗИ убирается	0,02	20	0,33
	Учет средств защиты				
1.11	Внесение данных о местах установки и составе средств защиты в журнал	Количество внедряемых СЗИ в год	0,07	200	13,33
1.12	Простановка отметки о снятии средства защиты в журнале	Количество снимаемых СЗИ в год	0,03	200	6,67
1.13	Предоставление данных о внедренных (снятых) СЗИ в отдел ИБ	Частота предоставления информации	0,07	400	26,67
	Определение требований к защите АРМ и серверов				
1.14	Заполнение формы сбора данных о характеристиках новых АРМ	Внедряемые АРМ в год	0,17	100	16,67
1.15	Заполнение формы сбора данных о характеристиках новых серверов	Внедряемые серверы в год	0,17	15	2,50

1.16	Отправка информации о характеристиках процессов на АРМ и серверах в отдел ИТ и отдел ИБ	Внедряемые АРМ и серверы в год	0,02	115	1,92
1.17	Предоставление отделом ИБ требований к безопасности АРМ и /или серверов	Внедряемые АРМ и серверы в год	0,17	115	19,17
	Документационное обеспечение внедрения СЗИ				
1.18	Подготовка заключения о готовности СЗИ к эксплуатации	Количество внедряемых СЗИ в год	0,5	200	100
1.19	Согласование заключения о готовности СЗИ к эксплуатации	Количество внедряемых СЗИ в год	0,17	200	33,33
1.20	Подготовка приказа на ввод СЗИ в эксплуатацию	Количество внедряемых СЗИ в год	0,08	200	16,67
1.21	Согласование приказа на ввод СЗИ в эксплуатацию	Количество внедряемых СЗИ в год	0,08	200	16,67
	Учет машинных носителей СЗИ				
1.22	Внесение данных об АРМ в журнал	Внедряемые АРМ в год	0,17	100	16,67
1.23	Внесение данных о серверах в журнал	Внедряемые серверы в год	0,17	15	2,50
1.24	Внесение данных о съемных носителях в журнал	Новые съемные носители в год			
	Учет эксплуатационной и технической документации к СЗИ				

1.25	Внесение данных о документации в журнал	Количество единиц документов в год	0,17	50	8,33
	Учет характеристик ИСПДн				
1.26	Заполнение формы сбора данных об изменениях и архитектуре ИС	Изменения в ИСПДн в год	0,17	150	25,0
1.27	Заполнение формы сбора данных об изменениях массивов, ПДн в них	Изменения состава ПДн в год	0,25	20	5,0
1.28	Отправка форм в отдел ИБ	Изменения ИСПДн и состава ПДн в год	0,03	170	5,67
	Контроль соответствия изменений в ИС требований к безопасности ПДн				
1.29	Проверка соответствия модели угроз изменениям в ИС	Изменения ИСПДн, состава ПДн, АРМ и серверов в год	0,25	305	76,25
1.30	Проверка соответствия описания системы защиты изменениям в ИС	Изменения ИСПДн, состава ПДн, АРМ и серверов в год	0,25	305	76,25
1.31	Проверка соответствия акта классификации ИСПДн изменениям в ИС	Изменения ИСПДн, состава ПДн, АРМ и серверов в год	0,08	305	25,42
1.32	Анализ новых активов на необходимость защиты ПДн на них	Внедряемые АРМ и серверы в год	0,17	115	19,17

	Управление документацией на систему защиты				
1.33	Подготовка акта классификации (уровня защищенности ПДн) ИСПДн	Количество изменений в ИСПДн	20,0	10	200,0
1.34	Подготовка модели угроз ИСПДн	Количество изменений в ИСПДн	40,0	20	800,0
1.35	Подготовка описания системы защиты	Количество изменений в ИСПДн	30,0	20	600,0
	Управление сертификатами на СЗИ				
1.36	Проверка сроков истечения сертификатов	Количество сертификатов на СЗИ	0,02	10	0,17
1.37	Выявление мест, где установлены СЗИ с истекшим сроком действия сертификата	Количество внедренных СЗИ	0,01	1200	10,0
1.38	Возобновление действия сертификата	Количество сертификатов с истекающим сроком в год	40,0	2	80,0
	Контроль эффективности системы защиты ПДн				
1.39	Подготовка приказа на проведение контроля эффективности	Частота контролей в год	0,25	32	8,0
1.40	Подготовка акта по результатам контроля эффективности	Частота контролей в год. количество проверяемых тСЗИ	0,42	320	133,33

1.41	Проверка истечения сроков очередного контроля эффективности	Количество ИСПДн	0,05	32	1,60
	Управление резервными копиями (РК)				
1.42	Контроль наличия резервных копий в ИСПДн	Количество новых ИСПДн в год	0,05	1	0,05
1.43	Учет наличия резервных копий в ИСПДн	Количество новых ИСПДн в год	0,05	1	0,05
1.44	Отправка информации о наличии РК в заинтересованные подразделения	Количество новых ИСПДн в год	0,05	1	0,05
	Управление помещениями, где осуществляется обработка ПДн				
1.45	Заполнение форм о помещениях, где осуществляется обработка ПДн	Количество новых помещений в год	0,17	100	16,67
1.46	Проверка данных о соответствии помещений требованиям	Количество новых помещений в год	0,17	100	16,67
1.47	Контроль выполнения требований к помещениям	Количество не соответствующих помещений в год	0,08	10	0,83
1.48	Подготовка приказа на обработку ПДн в помещении	Количество новых помещений в год	0,17	100	16,67
	Управление инцидентами в области ПДн				
1.49	Отработка журналов аудита СЗИ	Количество СЗИ	1,87	1200	2240,00

1.50	Проверка обнаруженных инцидентов	Количество инцидентов	0,17	200	33,33
1.51	Учет инцидентов	Количество инцидентов	0,08	200	16,67
1.52	Обработка инцидентов	Количество инцидентов	4,0	200	800,0
2	*Выполнение требований к процессам обработки ПДн*				
	Управление составом ПДн				
2.1	Заполнение форм о ПДн в бизнес-процессах	Количество изменений в ПДн в год	0,17	20	3,33
2.2	Отправка заполненной формы на заинтересованных лиц	Количество изменений в ПДн в год	0,05	20	1,0
2.3	Анализ необходимости изменения перечня ПДн	Количество изменений в ПДн в год	0,17	20	3,33
2.4	Анализ необходимости изменения «Уведомления об обработке ПДн» РКН	Количество изменений в ПДн в год	0,5	20	10,0
2.5	Анализ необходимости изменения «Модели угроз»	Количество изменений в ИСПДн в год	0,5	20	10,0
2.6	Правка «Перечня ПДн»	Количество изменений в ПДн в год	8,0	20	160,0
2.7	Правка «Уведомления об обработке ПДн» РКН	Количество изменений в ПДн в год	8,0	20	160,0
2.8	Правка «Модели угроз»	Количество изменений в ИСПДн в год	8,0	20	160,0

	Управление процессами обработки ПДн				
2.9	Сбор данных о процессах обработки ПДн (способы, третьи лица и т.п.)	Количество изменений процессов в год	0,17	20	3,33
2.10	Отправка заполненной формы на заинтересованных лиц	Количество изменений процессов в год	0,05	20	1,0
2.11	Контроль соответствия объема и характера ПДн, способов обработки - целям	Количество изменений процессов в год	0,17	20	3,33
2.12	Анализ необходимости изменекния «Уведомления об обработке ПДн» РКН	Количество изменений процессов в год	0,17	20	3,33
2.13	Правка «Уведомления об обработке ПДн» РКН	Количество изменений процессов в год	8.0	20	160,0
	Управление целями обработки ПДн				
2.14	Учет состава целей обработки ПДн	Количество новых целей в год	0,17	1	0,17
2.15	Контроль соответствия целей обработки ПДн заявленным	Количество новых целей в год	0,17	1	0,17
2.16	Анализ допустимости обработки ПДн в новых целях	Количество новых целей в год	0,17	1	0,17
2.17	Контроль баз данных на предмет отсутствия баз данных с несовместимыми целями	Количество изменений целей обработки ПДн. Количество баз ПДн	0,33	10	3,33

	Управление согласиями на обработку ПДн				
2.18	Определение юридических оснований, которые требуют сбора согласий	Количество изменений процессов в год	0,17	20	3,33
2.19	Определение ПДн, обрабатываемых при данных юридических тоснованиях	Количество изменений процессов в год	0,33	20	6,67
2.20	Определение списка субъектов ПДн, с которых требуется согласие на обработку	Количество изменений процессов в год. Количество баз ПДн	0,17	100	16,67
2.21	Генерация формы согласия на обработку ПДн для каждого субъекта ПДн	Количество субъектов ПДн, от которых требуется согласие в год	0,25	80	20,0
	Отработка запросов субъектов с указанием на неполные, неточные, недостоверные ПДн				
2.22	Учет запроса субъекта	Количество запросов в год	0,08	50	4,17
2.23	Отправка запроса в заинтересованные подразделения	Количество запросов в год	0,05	50	2,50
2.24	Проверка наличия данных субъектов ПДн в каждой базе данных	Количество запросов в год Количество баз данных	0,08	500	41,67
2.25	Внесение изменений в ПДн по каждой базе	Количество запросов в год	0,25	50	12,50
2.26	Контроль сроков подготовки ответа	Количество запросов в год	0,05	50	2,50

2.27	Подготовка ответа на запрс	Количество запросов в год	0,17	50	8,33
	Отработка запросов субъектов на устранение нарушений				
2.28	Учет запроса субъекта	Количество запросов в год	0,07	15	1,0
2.29	Отправка запроса в заинтересованные подразделения	Количество запросов в год	0,05	15	0,75
2.30	Принятие решений по запросу	Количество запросов в год	0,17	15	2,50
2.31	Отправка решения в ответственное подразделение	Количество запросов в год	0,05	15	0,75
2.32	Контроль сроков подготовки ответа	Количество запросов в год	0,05	15	0,75
2.33	Подготовка Уведомления о результатах рассмотрения запроса	Количество запросов в год	0,17	15	2,50
	Отработка запросов на предоставление информации о характере процессов обработки ПДн				
2.34	Учет запроса субъекта ПДн	Количество запросов в год	0,07	100	6,67
2.35	Отправка запросов в заинтересованные подразделения	Количество запросов в год	0,05	100	5,0
2.36	Проверка наличия данных субъектов ПДн в каждой базе при получении запроса	Количество запросов в год. Количество баз ПДн	0,07	1000	66,67

2.37	Предоставление информации о наличии данных субъекта ПДн в ответственное подразделение	Количество запросов в год	0,05	100	5,0
2.38	Контроль сроков подготовки ответа	Количество запросов в год	0,05	100	5,0
2.39	Подготовка формы Уведомления о характере процессов обработки ПДн	Количество запросов в год	0,17	100	16,67
	Подготовка Уведомлений субъектов ПДн л предполагаемой обработке их ПДн				
2.40	Определение состава баз, в которых ПДн получены от третьих лиц	Количество новых баз данных ПДн в год	0,17	20	3,33
2.41	Генерация списка субъектов ПДн для отправки уведомления	Количество списков в год	0,17	20	3,33
2.42	Отправка списка в заинтересованные подразделения	Количество списков в год	0,05	20	1,0
2.43	Контроль сроков подготовки ответа	Количество списков в год	0,05	20	1,0
2.44	Подготовка формы Уведомления о предполагаемой обработке ПДн	Количество новых субъектов ПДн в год	0,17	200	33,33
	Отработка отзывов субъектами ПДн согласий на обработку ПДн				
2.45	Учет отзыва согласия	Количество отзывов в год	0,08	50	4,17
2.46	Отправка отзыва в заинтересованные подразделения	Количество отзывов в год	0,05	50	2,50

2.47	Анализ правовых оснований для дальнейшей обработки ПДн	Количество отзывов в год	0,33	50	16,67
2.48	Контроль уничтожения ПДн при достижении целей обработки ПДн	Количество отзывов в год	0,33	50	16,67
	Уничтожение ПДн				
2.49	Ввод дат по каждой записи, позволяющих отслеживать сроки уничтожения ПДн	Количество записей в базах, по которым наствпили сроки уничтожения ПДн	0,01	5000	25,0
2.50	Определение состава лиц, цели обработки которых достигнуты (анализ достижения всех целей)	Частота удаления	0,17	2500	416,67
2.51	Уничтожение ПДн в базах ПДн	Частота удаления	0,08	1120	93,33
2.52	Контроль уничтожения ПДн	Частота контроля в год	3,0	40	120,0
Итого чел/год (с учетом коэффициента)			**7897**		
Стоимость чел/ч, руб			**417**		
Стоимость в год, руб			**3290375**		
Требуемая штатная численность			**4,4**		

Литература:

1. Государственный стандарт РФ ГОСТ Р5П41-98 «Делопроизводство и архивное дело. Термины и определения»;
2. Государственный стандарт РФ ГОСТ Р6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»;
3. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти (2000 г.);
4. Общероссийский классификатор управленческой документации (ОКУД) ОК 011-93 (1993 г., с изм.. и доп. 1999-2002 гг.);
5. Межотраслевые укрупненные нормативы времени на работы по документационному
обеспечению управления (1995 г.);
6. Основные правила работы архивов организаций (2002 г.);
7. Методические рекомендации ВНИИДАДФАС РФ «Унификация текстов управленческих документов» (1998 г.);
8. Методические рекомендации ВНИИДЛДФАС РФ «Организационно-распорядительная документация. Требования к оформлению документов» (2003 г.);
9. Методические рекомендации ВНИИДАД ФАС РФ «Ведение делопроизводства в
организации» (2004 г.).
10. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
11. П. Лучников «Персональные данные с точки зрения информационных технологий». Информационно-методический журнал «Защита информации, инсайд» № 2, 2012 год.
12. Катаржнов Учебное пособие «Обеспечение безопасности персональных данных» СПб, НИУ ИТМО, 2014 г.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

---

1. КАФЕДРА БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Кафедра «Безопасные информационные технологии» (БИТ) осуществляет подготовку специалистов по специальности 090103 «Организация и технология защиты информации», бакалавров и магистров по направлению 10.04.01 «Информационная безопасность». Широкий профиль подготовки, знание методов обеспечения информационной безопасности и средств защиты информации, практические навыки работы с современными техническими, программными и программно-аппаратными средствами защиты информации – все это позволяет выпускникам кафедры найти работу на производственных предприятиях, в подразделениях информационной безопасности, научно-исследовательских и инновационных организациях, а также в коммерческих структурах. Выпускники кафедры последних лет работают в Федеральной службе по техническому и экспортному контролю (ФСТЭК России), Лаборатории Касперского, компании Dr.Web, специализированных предприятиях в сфере разработки и применения комплексных систем защиты информации «ЭВРИКА», «ГазИнформСервис», ит.д. Партнерами кафедры являются ОАО «Воентелеком», Санкт-Петербургский институт информатики и автоматизации РАН, Военная академия Генерального штаба ВС РФ, Военно-космическая академия им. А.Ф. Можайского, Бостонский университет (США), Комитет по управлению городским имуществом администрации Санкт-Петербурга и другие научные организации и вузы.

Катаржнов Александр Демьянович

ОРГАНИЗАЦИОННО - РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ И ПРЕДПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел

Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49