Распоряжение Администрации Тверской области от 16 марта 2011 г. N 231-ра "Об отдельных вопросах обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных"

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных:

1. Утвердить Регламент обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Регламент) (приложение 1).

2. Утвердить Типовое положение о работе с персональными данными (приложение 2).

3. Руководителю аппарата Губернатора Тверской области, руководителям областных исполнительных органов государственной власти Тверской области при организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных обеспечить соблюдение Регламента.

4. Руководителю аппарата Губернатора Тверской области в срок до 01.05.2011 обеспечить подготовку проекта правового акта Губернатора Тверской области, утверждающего положение о работе с персональными данными в Администрации Тверской области.

5. Руководителям областных исполнительных органов государственной власти Тверской области в срок до 01.05.2011 подготовить и принять положение о работе с персональными данными областного исполнительного органа государственной власти Тверской области в соответствии с Типовым положением о работе с персональными данными, утвержденным настоящим распоряжением.

6. Рекомендовать органам местного самоуправления муниципальных образований Тверской области при организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных руководствоваться положениями Регламента.

7. Контроль за исполнением настоящего распоряжения возложить на заместителя Губернатора Тверской области Цеберганова Ю.В.

Отчет об исполнении пункта 3 распоряжения представлять ежегодно в срок до 30 декабря.

Отчет об исполнении пунктов 4, 5 распоряжения представить в срок до 01.06.2011.

8. Настоящее распоряжение вступает в силу со дня его подписания, подлежит официальному опубликованию и размещению на сайте управления региональной безопасности Тверской области в информационно-телекоммуникационной сети Интернет.

Губернатор области Д.В. Зеленин

Приложение 1
к распоряжению Администрации
Тверской области от 16 марта 2011 г. N 231-ра

Регламент обеспечения безопасности персональных данных при их обработке

в информационных системах персональных данных

1. Настоящий регламент определяет порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в Администрации Тверской области (аппарате Губернатора Тверской области) и областных исполнительных органах государственной власти Тверской области (далее также - операторы).

Настоящим Регламентом не регулируются вопросы обеспечения безопасности персональных данных, отнесенных в установленном федеральным законодательством порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

2. Для обеспечения безопасности персональных данных оператору необходимо:

а) до начала обработки персональных данных пройти процедуру регистрации в Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Тверской области (далее - Управление Роскомнадзора по Тверской области), за исключением случаев, предусмотренных федеральным законодательством. Порядок подачи и форма уведомления об обработке (о намерении осуществлять обработку) персональных данных, рекомендации по его заполнению представлены на сайте Управления Роскомнадзора по Тверской области в информационно-телекоммуникационной сети Интернет (www.69 rsoc.ru);

б) получить согласие субъектов персональных данных, за исключением случаев, предусмотренных федеральным законодательством;

в) присвоить соответствующий класс ИСПДн. Присвоение класса оформляется актом о классификации информационных систем персональных данных (приложение 1 к настоящему Регламенту), составленным в двух экземплярах. Второй экземпляр представляется в уполномоченный областной исполнительный орган государственной власти Тверской области в сфере защиты информации;

г) приказом руководителя назначить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности персональных данных, и определить перечень должностных лиц, допущенных к обработке персональных данных;

д) проверить соответствие организационно-технических мер защиты требованиям федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации;

е) разработать недостающую организационно-распорядительную документацию, описать систему защиты персональных данных (далее - СЗПДн);

ж) установить и ввести в эксплуатацию средства защиты информации;

з) проверить соответствие ИСПДн требованиям безопасности информации (специальные исследования);

и) провести аттестацию ИСПДн по требованиям безопасности информации (комплексные испытания, оценка результатов испытаний и выдача рекомендаций по обеспечению безопасности персональных данных на аттестованных объектах, оформление документов по результатам аттестационных испытаний и выдача аттестата соответствия ИСПДн требованиям по безопасности информации).

3. Выполнение установленных требований по обеспечению безопасности персональных данных достигается осуществлением алгоритма организации работ по обеспечению безопасности персональных данных при их обработке в ИСПДн в соответствии с пунктами 4-10 настоящего Регламента.

4. Алгоритм организации работ по обеспечению безопасности персональных данных при их обработке в ИСПДн включает в себя:

а) аудит информационной безопасности;

б) разработку типового пакета обязательных документов;

в) приобретение соответствующих средств защиты;

г) внедрение средств защиты;

д) аттестацию ИСПДн по требованиям безопасности информации;

е) периодический контроль соответствия ИСПДн требованиям безопасности информации.

5. Аудит информационной безопасности является способом получения количественных и качественных оценок текущего состояния информационной безопасности оператора, соответствия ИСПДн требованиям безопасности информации.

Аудит информационной безопасности необходим для подготовки исходных данных в целях последующей разработки обоснованных предложений по совершенствованию системы защиты информации от несанкционированного доступа (далее - НсД) в конкретных подсистемах автоматизированной системы (далее - АС) оператора.

В результате проведения аудита информационной безопасности оператор получает:

сводную таблицу характеристик АС оператора как объектов защиты;

классификацию ИСПДн, осуществляющих обработку персональных данных;

перечень персональных данных, обрабатываемых в ИСПДн;

список недостающих организационно-распорядительных документов по защите конфиденциальной информации, в том числе персональных данных;

рекомендуемые меры по формированию режима обеспечения безопасности персональных данных при их обработке в ИСПДн.

6. Разработка типового пакета обязательных документов включает в себя подготовку документов согласно таблице 1.

Таблица 1

1	Приказ об организации работы по защите информации	
1.1	Приложение 1	Перечень сведений конфиденциального характера
1.2	Приложение 2	Положение о порядке организации и проведения работ по защите конфиденциальной информации
2	Приказ об организации работы с персональными данными	
2.1	Приложение 1	Положение о работе с персональными данными
2.2	Приложение 2	Перечень помещений, в которых осуществляется обработка персональных данных с указанием лиц, имеющих допуск в данные помещения
2.3	Приложение 3	Список лиц, имеющих доступ к персональным данным
2.4	Приложение 4	Состав комиссии по классификации ИСПДн
3	Политика информационной безопасности (согласно ГОСТ Р ИСО/МЭК 17799-2005)	
4	Акт о классификации ИСПДн	

5	Модель угроз безопасности персональных данных при их обработке в ИСПДн
6	Описание технологического процесса обработки информации в ИСПДн
7	Техническое задание на создание системы защиты персональных данных
8	Технический проект системы защиты персональных данных
9	Журнал регистрации запросов субъектов персональных данных на предоставление доступа к своим персональным данным
10	Журнал учета электронных носителей персональных данных
11	Форма обязательства о неразглашении информации, содержащей персональные данные
12	Форма согласия субъекта персональных данных на обработку своих персональных данных

7. Приобретение средств защиты информации от НсД, средств межсетевого экранирования, антивирусной защиты и другого программного обеспечения позволяет выполнить обязательные требования по защите информации в соответствии с таблицей 2 в зависимости от класса ИСПДн.

Таблица 2

N п/п	Системы и требования к ним	Классы		
		К3	К2	К1
1	2	3	4	5
1	Для информационных систем при однопользовательском режиме обработки персональных данных			
1.1	Идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов	+	+	+
1.2	Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. (Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы)	+	+	+
1.3	Регистрация результата попытки входа (успешная или неуспешная)	-	-	+
1.4	Регистрация выдачи печатных (графических) документов на бумажный носитель. [В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа	-	-	+

	(наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства)]			
1.5	Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета	+	+	+
1.6	Дублирующий учет защищаемых носителей информации	-	-	+
1.7	Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. [Целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ]	+	+	+
1.8	Физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	+	+	+
1.9	Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
1.10	Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+
1.11	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации	-	-	+
2	Для информационных систем при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей			
2.1	Идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю	+	+	+

	условно-постоянного действия длиной не менее шести буквенно-цифровых символов			
2.2	Идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам)	-	-	+
2.3	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	-	-	+
2.4	Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. [Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная)]	+	+	-
2.5	Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. [Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа]	-	-	+
2.6	Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета	+	+	+
2.7	Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. [Целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации]	+	+	+
2.8	Физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в	+	+	+

	помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации			
2.9	Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
2.10	Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+
2.11	Регистрация выдачи печатных (графических) документов на бумажный носитель. [В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ]	-	-	+
2.12	Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. [В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)]	-	-	+
2.13	Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. [В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла]	-	-	+
2.14	Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). [В параметрах регистрации указываются дата и	-	-	+

	время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер)]			
2.15	Дублирующий учет защищаемых носителей информации	-	-	+
2.16	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации	-	-	+
3	Для информационных систем при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей			
3.1	Идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов	+	+	+
3.2	Идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам	-	-	+
3.3	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	-	-	+
3.4	Контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа	-	-	+
3.5	Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. [Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа]	+	+	+
3.6	Регистрация выдачи печатных (графических) документов на бумажный носитель. [В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ]	-	-	+
3.7	Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных	-	-	+

	для обработки персональных данных. [В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)]			
3.8	Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. [В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла]	-	-	+
3.9	Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). [В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер)]	-	-	+
3.10	Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)	+	+	+
3.11	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей	-	-	+
3.12	Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. [Целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации]	+	+	+
3.13	Физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в	+	+	+

	помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации			
3.14	Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
3.15	Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+
4	Безопасное межсетевое взаимодействие для информационных систем при их подключении к сетям международного информационного обмена			
4.1	Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)	+	+	+
4.2	Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия	+	+	+
4.3	Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)	+	+	+
4.4	Контроль целостности своей программной и информационной части	+	+	+
4.5	Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств	+	+	+
4.6	Восстановление свойств межсетевого экрана после сбоев и отказов оборудования	+	+	+
4.7	Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и	+	+	+

	информационной части, процедуры восстановления			
4.8	Фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов	-	+	+
4.9	Фильтрация с учетом любых значимых полей сетевых пакетов	-	+	+
4.10	Фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя	-	-	+
4.11	Фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя	-	-	+
4.12	Фильтрация с учетом даты и времени	-	-	+
4.13	Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети	-	-	+
4.14	Регистрация и учет запросов на установление виртуальных соединений	-	-	+
4.15	Локальная сигнализация попыток нарушения правил фильтрации	-	-	+
4.16	Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)	-	+	+
4.17	Регистрация запуска программ и процессов (заданий, задач)	-	+	+
4.18	Предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась	-	-	+
4.19	Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации	-	-	+
4.20	Идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации	-	-	+

8. Внедрение средств защиты осуществляется при наличии у оператора лицензии федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, на осуществление деятельности по технической защите конфиденциальной информации.

К проведению данных мероприятий по решению оператора могут привлекаться организации, имеющие соответствующие лицензии.

9. ИСПДн Администрации Тверской области (аппарата Губернатора Тверской области), областных исполнительных органов государственной власти Тверской

области проходят обязательную аттестацию по требованиям безопасности информации.

Аттестация проводится органами по аттестации, имеющими право проведения аттестации.

10. Периодический контроль соответствия ИСПДн требованиям безопасности информации проводится оператором не реже одного раза в год в случае наличия у него лицензии федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, на осуществление деятельности по технической защите конфиденциальной информации.

К проведению данных мероприятий по решению оператора могут привлекаться организации, имеющие соответствующие лицензии.

11. Обработка персональных данных без использования средств автоматизации осуществляется на бумажных носителях и в электронном виде.

Обработка персональных данных без использования средств автоматизации в электронном виде осуществляется на внешних электронных носителях информации.

Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных (приложение 2 к настоящему Регламенту).

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

12. Должностные лица оператора, виновные в нарушении законодательства в области обеспечения безопасности персональных данных, привлекаются к ответственности в порядке, установленном федеральным законодательством.

Приложение 1
к Регламенту обеспечения безопасности
персональных данных при их обработке
в информационных системах персональных данных

Утверждаю

_____
(должность, фамилия и инициалы)
"___"_____ 20__ г.

Акт
о классификации информационных систем
персональных данных
в _____
(наименование исполнительного органа
государственной власти Тверской области)

В соответствии с требованиями Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17.11.2007 N 781, приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" (далее - Порядок) комиссия, назначенная приказом _____ (должность руководителя) _____ (наименование исполнительного органа

государственной власти Тверской области) от _____ N ____ , в составе:

председателя -
членов комиссии -

рассмотрев исходные данные на информационные системы персональных данных (далее - ИСПДн) _____
(наименование исполнительного органа государственной власти Тверской области)
решила присвоить ИСПДн _____
(наименование исполнительного органа государственной власти Тверской области) следующие классы:

N п/п	Наименование ИСПДн	Структура ИСПДн	Наличие подключения к сетям	Режим обработки	Разграничение доступа	Нахождение ИСПДн	Класс ИСПДн	Примечание
1	2	3	4	5	6	7	8	9

Примечания:
В графе 3 отражается структура ИСПДн согласно пункту 9 Порядка.
В графе 4 отражается наличие подключения к сетям согласно пункту 10 Порядка.
В графе 5 отражается режим обработки персональных данных согласно пункту 11 Порядка.
В графе 6 отражается разграничение доступа согласно пункту 12 Порядка.
В графе 7 отражается нахождение ИСПДн согласно пункту 13 Порядка.
В графе 8 отражается класс ИСПДн согласно пункту 15 Порядка.
В графе 9 указывается дополнительная информация об ИСПДн, которую оператор считает необходимым включить в акт.

Председатель комиссии:

Члены комиссии:

Приложение 2
к Регламенту обеспечения безопасности
персональных данных при их обработке
в информационных системах персональных данных

Утверждаю
_____
(должность, фамилия и инициалы)
"___"_____ 20__ г.

Начат "___"_____ 20__ г.

Окончен "___"_____ 20__ г.
На _____ листах

Журнал
учета электронных носителей персональных данных

Учетный номер	Дата постановки на учет	Вид электронного носителя, место его хранения (размещения)	Ответственный за использование и хранение		
			Ф.И.О.	подпись	дата
1	2	3	4	5	6

Приложение 2
к распоряжению Администрации
Тверской области
от 16 марта 2011 г. N 231-ра

Типовое положение о работе с персональными данными

Раздел I. Общие положения

1. Настоящее Положение устанавливает порядок обработки документов, содержащих сведения, отнесенные к персональным данным, с использованием средств автоматизации или без использования таких средств, а также исследования и оценки информационных систем персональных данных (далее - ИСПДн) и систем защиты персональных данных (далее - СЗПДн), на которых будет происходить обработка персональных данных в _____.(наименование исполнительного органа государственной власти Тверской области (далее - оператор)

2. Обработка персональных данных физических лиц осуществляется должностными лицами оператора в соответствии с полномочиями, определенными их должностными регламентами.

3. Должностные лица оператора осуществляют обработку персональных данных следующих категорий субъектов персональных данных:

а) государственные гражданские служащие, служащие и работники оператора;

б) физические лица, обращающиеся к оператору с письменными предложениями, заявлениями или жалобами, а также устными обращениями;

в) руководители, уполномоченные представители юридических лиц, а также физические лица, состоящие в гражданско-правовых отношениях с оператором;

г) иные физические лица, сведения о персональных данных которых имеются у оператора в связи реализацией им своих полномочий.

4. Категории субъектов персональных данных, чьи персональные данные обрабатываются в структурных подразделениях оператора, определяются исходя из решаемых структурным подразделением оператора задач и полномочий, установленных соответствующими положениями о структурных подразделениях оператора и должностными регламентами сотрудников структурных подразделений оператора.

5. Объем обрабатываемых персональных данных вышеуказанных категорий субъектов персональных данных определяется оператором самостоятельно, исходя из решаемых задач и полномочий в соответствии с законодательством и нормативными

правовыми актами, регулирующими его деятельность.

Раздел II. Принципы обработки персональных данных

6. Обработка персональных данных должна осуществляться на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки; персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

8. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи оператору своих персональных данных.

9. Держателем персональных данных является оператор, которому субъект персональных данных добровольно передает во владение свои персональные данные. Оператор выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

10. Право доступа к персональным данным субъекта персональных данных имеют лица, уполномоченные оператором.

11. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или оператору за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

12. Получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъектам персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъектов персональных данных, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Раздел III. Обработка и хранение персональных данных

13. Условием обработки персональных данных субъекта персональных данных является его согласие, оформляемое согласно приложению 1 к настоящему Положению. Субъект персональных данных принимает решение о предоставлении

своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных пунктом 14 настоящего Положения. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных при необходимости дается в письменной форме одним из его наследников, если такое согласие не было дано работником при его жизни.

14. Согласие субъекта персональных данных на обработку его персональных данных не требуется в следующих случаях:

а) если обработка персональных данных осуществляется на основании соответствующего федерального закона;

б) если обработка персональных данных осуществляется на основании исполнения трудового, гражданско-правового договора между субъектом персональных данных и оператором;

в) если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

г) если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия при данных обстоятельствах невозможно;

д) если обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

е) если осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

15. Не допускается получение и обработка персональных данных субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных пунктом 16 настоящего Положения.

16. Обработка указанных в пункте 15 настоящего Положения персональных данных допускается, в случаях если:

а) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

б) персональные данные являются общедоступными;

в) персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов его или других лиц, и получение согласия субъекта персональных данных в данный момент невозможно;

г) в иных случаях, предусмотренных законодательством Российской Федерации.

17. Обработка персональных данных о судимости осуществляется в соответствии с федеральными законами.

18. Обработка персональных данных, перечисленных в пункте 15 настоящего Положения, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

19. Сведения, которые характеризуют физиологические особенности человека и на основе которых устанавливается его личность (биометрические персональные данные), обрабатываются только при наличии согласия субъекта персональных данных в письменной форме, за исключением случаев, предусмотренных пунктом 20

настоящего Положения.

20. Обработка биометрических персональных данных осуществляется без согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации, в частности законодательством о государственной службе.

21. Документы, содержащие персональные данные субъекта персональных данных, составляют его личное дело. Личное дело хранится уполномоченным лицом на бумажных носителях, а помимо этого может храниться в виде электронных документов. Личное дело пополняется на протяжении всей трудовой деятельности субъекта персональных данных. Письменные доказательства получения оператором согласия субъекта персональных данных на обработку его персональных данных хранятся в личном деле субъекта персональных данных.

22. При обработке персональных данных субъектов персональных данных оператор определяет способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

Раздел IV. Организация разрешительной системы доступа пользователей к обрабатываемой в информационных системах персональных данных информации

23. К требованиям при регистрации пользователей ИСПДн относятся:

а) получение сведений о персональных данных субъекта персональных данных из следующих документов:

паспорт или иной документ, удостоверяющий личность;

трудовая книжка;

страховое свидетельство государственного пенсионного страхования;

документы воинского учета;

документ об образовании, о квалификации или наличии специальных знаний;

анкета, заполняемая субъектом персональных данных при приеме на работу;

иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, в процессе работы, при обращении субъекта персональных данных к оператору;

б) получение персональных данных лично от субъекта персональных данных. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от субъекта персональных данных документы, проверяет их полноту и правильность указываемых сведений. В случае невозможности получения персональных данных от субъекта персональных данных лично получение возможно от третьих лиц при условии уведомления субъекта персональных данных за 3 календарных дня и получения от него письменного согласия о передаче своих персональных данных третьим лицам;

в) оператор должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

24. Внутренний доступ к персональным данным субъекта персональных данных имеют сотрудники структурных подразделений оператора, которым эти данные необходимы для выполнения должностных обязанностей на основании Регламента разграничения прав доступа (приложение 2 к настоящему Положению).

25. Пользователь персональных данных имеет доступ к своим персональным

данным на основании разрешительной системы допуска на объект вычислительной техники "Автоматизированное рабочее место на базе автономной персональной электронной вычислительной машины (инв. N_____) _____ (наименование оператора)" (приложение 3 к настоящему Положению).

Раздел V. Конфиденциальность персональных данных

26. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных пунктом 27 настоящего Положения.

27. Обеспечение конфиденциальности персональных данных не требуется:

а) в случае обезличивания персональных данных;

б) в отношении общедоступных персональных данных.

Раздел VI. Общедоступные источники персональных данных

28. С целью информационного обеспечения деятельности могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

29. Сведения о субъекте персональных данных исключаются в любое время из общедоступных источников персональных данных по его требованию, либо по решению оператора, либо суда или иных уполномоченных государственных органов.

Раздел VII. Права и обязанности сторон в области обеспечения безопасности персональных данных

Информация об изменениях:

Распоряжением Правительства Тверской области от 7 сентября 2011 г. N 34-рп в пункт 30 раздела VII настоящего положения внесены изменения, вступающие в силу со дня подписания названного распоряжения

См. текст пункта в предыдущей редакции

30. Субъект персональных данных:

а) передает оператору или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и иные сведения;

б) своевременно сообщает оператору об изменении своих персональных данных;

в) получает полную информацию о своих персональных данных;

г) имеет свободный без взимания платы доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

д) имеет возможность получения относящихся к нему медицинских данных у выбранного им медицинского специалиста;

е) получает сведения об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных;

ж) требует от оператора уточнения своих персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

з) получает информацию, касающуюся обработки его персональных данных, в том числе содержащую подтверждение факта обработки персональных данных оператором, а также цель такой обработки; способы обработки персональных данных, применяемые оператором; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных;

и) при отказе оператора исключить или исправить персональные данные субъекта персональных данных он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия.

Сведения о наличии персональных данных предоставляются субъекту персональных данных в доступной форме, не содержащей персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его представителю оператором при личном обращении либо при получении запроса.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его представителя. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

31. Право субъекта персональных данных на доступ к своим персональным данным ограничивается, в случае если:

а) обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) предоставление персональных данных нарушает конституционные права и свободы других лиц;

в) в иных случаях, предусмотренных законодательством Российской Федерации.

32. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных пунктом 33 настоящего Положения.

33. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, принимается на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия субъекта персональных данных в письменной форме или в случаях, предусмотренных федеральными законами.

34. Оператор разъясняет субъекту персональных данных порядок принятия

решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставляет возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Оператор рассматривает возражение субъекта персональных данных в течение 7 рабочих дней со дня его получения и уведомляет его о результатах рассмотрения такого возражения.

35. Если обязанность предоставления персональных данных субъектом персональных данных установлена федеральным законом, оператор разъясняет субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

36. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

а) наименование и адрес оператора или его представителя;

б) цель обработки персональных данных и ее правовое основание;

в) предполагаемые пользователи персональных данных;

г) права субъекта персональных данных в области защиты персональных данных.

37. Оператор безвозмездно предоставляет субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также вносит в них необходимые изменения, уничтожает или блокирует соответствующие персональные данные по предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта персональных данных были переданы.

38. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператор осуществляет блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных оператор на основании соответствующих документов уточняет персональные данные и снимает их блокирование.

В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий 3 рабочих дней с даты такого выявления, устраняет допущенные нарушения.

В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор уведомляет субъекта персональных данных.

39. В случае достижения цели обработки персональных данных оператор незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий 3 рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомляет об этом субъекта персональных данных.

40. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор прекращает обработку персональных данных и

уничтожает персональные данные в срок, не превышающий 3 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон. Об уничтожении персональных данных оператор уведомляет субъекта персональных данных.

Раздел VIII. Доступ к персональным данным и их передача

41. Внутренний доступ к персональным данным субъекта персональных данных имеют уполномоченные сотрудники структурных подразделений оператора, которым эти данные необходимы для выполнения должностных обязанностей.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

42. После увольнения субъекта персональных данных документы, содержащие его персональные данные, хранятся у оператора в течение сроков, установленных законодательством.

43. Внешний доступ со стороны третьих лиц к персональным данным субъекта персональных данных осуществляется только с письменного согласия субъекта персональных данных, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта персональных данных или других лиц, и иных случаев, установленных законодательством.

44. Оператор обязан сообщать персональные данные субъекта персональных данных по надлежаще оформленным запросам суда, прокуратуры, правоохранительных органов.

45. При передаче персональных данных субъекта персональных данных внешнему потребителю оператор передает минимальный объем персональных данных и только в целях выполнения задач, соответствующих объективной причине сбора этих данных. Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

46. Доступ к персональным данным субъектов персональных данных, обрабатываемых оператором, разрешается только специально уполномоченным лицам (внутреннему потребителю).

Внутренние потребители персональных данных в обязательном порядке под подпись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные (приложение 4 к настоящему Положению).

47. Регламентация доступа сотрудников оператора к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации. Для защиты персональных данных субъектов персональных данных оператор:

а) ограничивает и регламентирует состав сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

б) избирательно и обоснованно распределяет документы и информацию между сотрудниками;

в) рационально размещает рабочие места сотрудников, исключая бесконтрольное использование защищаемой информации;

г) обеспечивает ознакомление сотрудников с требованиями документов по защите персональных данных;

д) обеспечивает соответствие необходимых условий в помещении для работы с

конфиденциальными документами и базами данных;

е) определяет и регламентирует состав сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

ж) организует порядок уничтожения информации;

з) своевременно выявляет нарушения требований разрешительной системы доступа сотрудниками структурных подразделений, допущенными к обработке персональных данных;

и) обеспечивает воспитательную и разъяснительную работу с сотрудниками по предупреждению утраты сведений при работе с конфиденциальными документами.

Раздел IX. Безопасность персональных данных

48. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

49. Использование и хранение биометрических персональных данных вне ИСПДн осуществляются только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

50. Организация работ по обеспечению безопасности персональных данных осуществляется в соответствии с установленной руководителем оператора схемой организации работ по обеспечению безопасности персональных данных (приложение 5 к настоящему Положению).

Раздел X. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

51. Каждый сотрудник оператора, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

52. Нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных влечет ответственность граждан и юридических лиц в соответствии с законодательством Российской Федерации.

Раздел XI. Порядок классификации информационных систем персональных данных

53. Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

54. Проведение классификации ИСПДн состоит из:

а) сбора и анализа исходных данных по ИСПДн;

б) присвоения ИСПДн соответствующего класса и его документального

оформления.

55. При проведении классификации ИСПДн учитываются:

а) категория обрабатываемых в ИСПДн персональных данных - Хпд;

б) объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн) - Хнпд;

в) заданные оператором характеристики безопасности персональных данных, обрабатываемых в ИСПДн;

г) структура ИСПДн;

д) наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

е) режим обработки персональных данных;

ж) режим разграничения прав доступа пользователей ИСПДн;

з) местонахождение технических средств ИСПДн.

56. Определяются следующие категории обрабатываемых в ИСПДн персональных данных (Хпд):

а) категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

в) категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

г) категория 4 - обезличенные и (или) общедоступные персональные данные.

57. Объем обрабатываемых персональных данных (Хнпд) может принимать следующие значения:

а) 1 - в ИСПДн одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах Тверской области;

б) 2 - в ИСПДн одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти (государственном органе) Тверской области, проживающих в пределах муниципального образования Тверской области;

в) 3 - в ИСПДн одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

58. Оператор определяет ИСПДн как типовую информационную систему ИСПДн, в которой требуется обеспечение только конфиденциальности персональных данных, и как специальную информационную систему ИСПДн, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

59. По результатам анализа исходных данных типовой ИСПДн присваивается один из следующих классов:

а) класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных

данных;

б) класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

в) класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

г) класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

60. Класс типовой информационной системы ИСПДн определяется в соответствии с нижеприведенной таблицей.

Хпд \ Хнпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

61. В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

62. Результаты классификации ИСПДн оформляются соответствующим актом оператора.

63. Класс ИСПДн пересматривается:

а) по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

б) по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Раздел XII. Порядок разработки, ввода в действие и эксплуатацию системы защиты персональных данных

64. Порядок предпроектного обследования ИСПДн включает:

а) определение перечня персональных данных обрабатываемых в ИСПДн;

б) определение перечня персональных данных, подлежащих защите от несанкционированного доступа (далее - НсД);

в) определение условий расположения ИСПДн относительно границ контролируемой зоны;

г) определение конфигурации и топологии ИСПДн в целом и ее отдельных компонентов; физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

д) определение технических средств и систем, предполагаемых к использованию в разрабатываемой ИСПДн, условия их расположения; общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

е) определение режимов обработки персональных данных в ИСПДн в целом и в

отдельных компонентах;

ж) определение класса ИСПДн;

з) уточнение степени участия должностных лиц в обработке персональных данных, характер их взаимодействия между собой;

и) определение (уточнение) угроз безопасности персональным данным применительно к конкретным условиям функционирования ИСПДн.

65. По результатам предпроектного обследования на основе документа с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности персональных данных, включаемые в техническое задание на разработку СЗПДн. Разработка технического задания на создание СЗПДн включает:

а) обоснование разработки СЗПДн;

б) исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

в) класс ИСПДн;

г) требования федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

д) перечень предполагаемых к использованию сертифицированных средств защиты информации;

е) обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

ж) состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

66. Проектирование и реализация СЗПДн включает:

а) разработку задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

б) выполнение работ в соответствии с проектной документацией;

в) закупку обоснованной совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;

г) разработку мероприятий по защите информации в соответствии с предъявляемыми требованиями;

д) закупку обоснованной совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

е) проведение сертификации по требованиям безопасности информации технических, программных и программно-технических средств защиты информации, в случае когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

ж) разработку и реализацию разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

з) определение структурных подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности персональных данных;

и) разработку эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации;

к) выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности персональных данных.

67. Ввод в действие СЗПДн включает:

а) выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

б) опытную эксплуатацию средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

в) приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

г) организацию охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

д) оценку соответствия ИСПДн требованиям безопасности персональных данных.

Раздел XIII. Порядок контроля за обеспечением уровня безопасности персональных данных и оценки соответствия информационных систем персональных данных

68. Порядок обследования защищенности персональных данных включает:

а) выделение информационных ресурсов, содержащих в себе персональные данные, а также технические средства, позволяющие осуществлять обработку персональных данных, из всей совокупности обрабатываемой информации;

б) определение соответствия действующей системы обработки персональных данных требованиям, установленным федеральным законодательством;

в) классификация информационных систем персональных данных.

69. По итогам обследования оператор получает:

а) аналитический отчет о предпроектном обследовании и текущей защищенности персональных данных;

б) акт классификации ИСПДн.

70. Подготовка ИСПДн к проведению оценки соответствия ИСПДн требованиям безопасности персональных данных и созданию СЗПДн осуществляется путем:

а) анализа информационных ресурсов (определения перечня всех существующих ИСПДн; определения состава и структуры каждой ИСПДн; определения перечня и местонахождения персональных данных, подлежащих защите; категорирования персональных данных; определения режима обработки персональных в целом и отдельных компонентах);

б) анализа уязвимых звеньев и возможных угроз безопасности персональных данных (оценки возможности физического доступа к ИСПДн;

выявления возможных каналов утечки информации, в том числе технических; анализа возможностей программно-математического воздействия на ИСПДн; анализа возможностей электромагнитного воздействия на ИСПДн);

в) оценки ущерба от реализации угроз безопасности персональных данных (оценки непосредственного и опосредованного ущерба от реализации угроз безопасности персональных данных);

г) анализа имеющихся в распоряжении мер и средств защиты персональных данных (от физического доступа; от утечки по техническим каналам; от НсД; от программно-математического воздействия; от электромагнитных воздействий).

71. Обоснование требований по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, включает:

а) разработку модели угроз безопасности персональных данных;

б) разработку модели нарушителя безопасности персональных данных;

в) составление перечня и проведение оценки актуальных угроз безопасности персональных данных;

г) определение класса ИСПДн.

72. Проведение работ по организации обеспечения безопасности персональных данных при их обработке в ИСПДн включает:

а) разработку и согласование с уполномоченными службами требований к СЗПДн и формулирование задач по защите персональных данных (разработка перечня мероприятий по защите персональных данных в соответствии с выбранным классом ИСПДн);

б) выбор способов, мер и средств защиты персональных данных в соответствии с мероприятиями по защите;

в) разработку технического задания на СЗПДн;

г) разработку документов, регламентирующих вопросы организации обеспечения безопасности персональных данных и эксплуатации СЗПДн в ИСПДн;

д) развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

е) доработку СЗПДн по результатам опытной эксплуатации;

ж) проведение работ по аттестации ИСПДн по требованиям безопасности информации.

Приложение 1
к Типовому положению
о работе с персональными данными

Согласие
на обработку персональных данных

г. _____ "___"_____ 20__г.

Я, _____ (Ф.И.О), _____ (вид документа, удостоверяющего личность) серия _____ N _____ выдан _____ (когда и кем), проживающий (ая) по адресу: _____, настоящим даю свое согласие на обработку _____ (наименование и адрес оператора) моих персональных данных и подтверждаю, что, давая такое согласие, я действую осознанно и в своих интересах.

Согласие дается мною с целью _____ (цель обработки персональных данных) и распространяется на следующую информацию:

_____
_____
_____
_____
(перечень персональных данных).

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с федеральным законодательством.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с "__" _____ 20___ г. по "__" ____ 20___ г.

_____
(Ф.И.О., подпись лица, давшего согласие)

Приложение 2
к Типовому положению
о работе с персональными данными

Утверждаю
_____
(должность, фамилия и инициалы)
"___"_____ 20__ г.

Регламент разграничения прав доступа

N п/п	Ф.И.О. сотрудника	Структурное подразделение	Должность	Информационные системы персональных данных, к которым разрешен доступ

Ответственный за обеспечение безопасности
персональных данных _____ (фамилия и инициалы)

"____" _____ 20 __ г.

Приложение 3
к Типовому положению
о работе с персональными данными

Утверждаю
_____
(должность, фамилия и инициалы)
"___"_____ 20__ г.

Разрешительная система
допуска на объект вычислительной техники
"Автоматизированное рабочее место

на базе автономной персональной электронной вычислительной машины (инв. N_____)

_____ "

(наименование оператора)

1. Перечень лиц, имеющих самостоятельный доступ к штатным средствам объекта вычислительной техники (субъектов доступа):

Ф.И.О.	Уровень полномочий (Администратор/ Пользователь)	Имя в системе	Вид выполняемых функций

2. Перечень защищаемых информационных ресурсов объекта вычислительной техники (объектов доступа):

Место хранения защищаемого ресурса	Категория защищаемого ресурса	Содержание ресурса

3. Матрица разграничения доступа к защищаемым ресурсам автоматизированной системы (месту хранения и используемым техническим средствам):

Тип ресурса (информационный/ аппаратный)	Название ресурса	Имя пользователя и полномочия *	
		Администратор	Пользователи

Примечание*
"+"- полные права на доступ;
"-"- отсутствуют права на доступ;
"Ч"- читать файлы (массивы информации);
"З"- записывать: добавлять (создавать) файлы (массивы информации), вносить изменения, удалять файлы (массивы информации), сохранять (записывать) на учтенные магнитные носители, распечатывать на принтере файлы (массивы информации).

Ответственный за обеспечение безопасности
персональных данных _____ (фамилия и инициалы)
"____" _____ 20 __ г.

Приложение 4
к Типовому положению
о работе с персональными данными

Обязательство
о неразглашении информации, содержащей персональные данные

Я,_____, (Ф.И.О. сотрудника оператора) исполняющий (ая) должностные обязанности по замещаемой должности

_____, (должность, наименование структурного подразделения оператора) предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать об этом непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

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

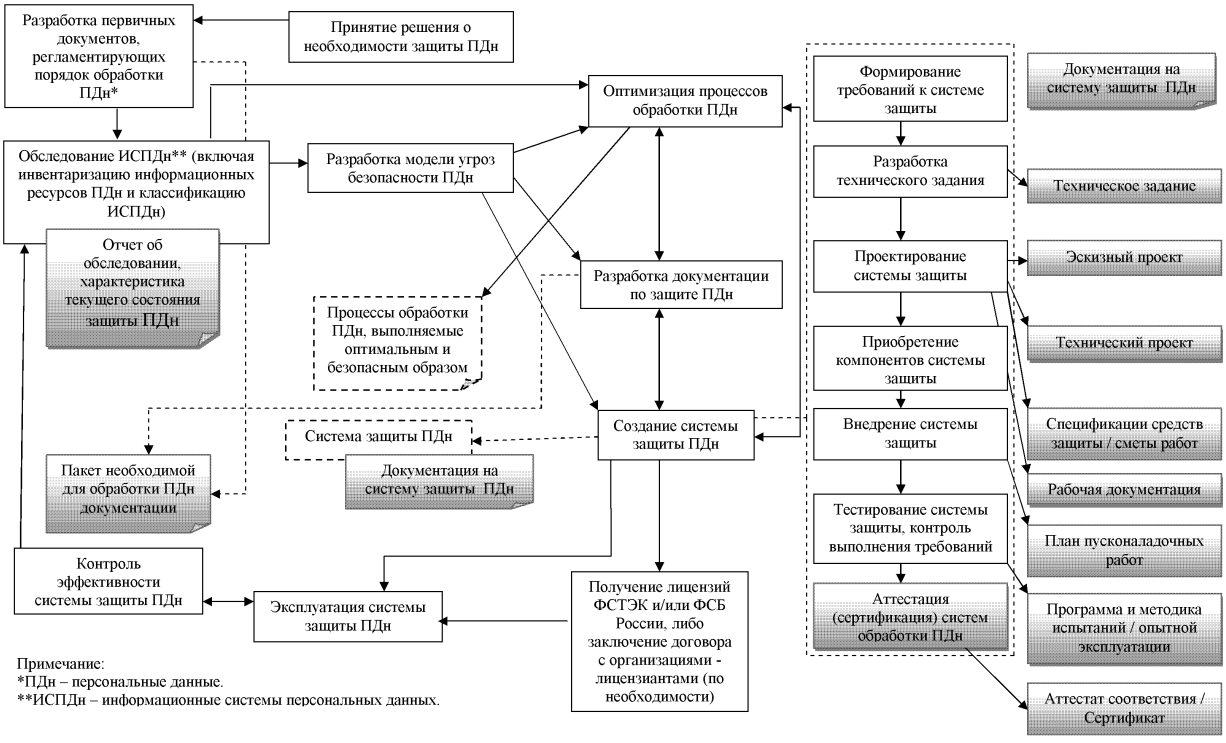
_____ _____ (Ф.И.О.) (подпись)

"_____"_____ 20___г.

Приложение 5
к Типовому положению
о работе с персональными данными

Схема организации работ
по обеспечению безопасности персональных данных

Схема организации работ по обеспечению безопасности персональных данных



Примечание:
*ПДн – персональные данные.
**ИСПДн – информационные системы персональных данных.