ПРАВИТЕЛЬСТВО ВОРОНЕЖСКОЙ ОБЛАСТИ

КОМИССИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРИ ГУБЕРНАТОРЕ ВОРОНЕЖСКОЙ ОБЛАСТИ

Серия «Библиотека государственного гражданского служащего Воронежской области»

Основана в 2014 году

Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и органах местного самоуправления

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Под редакцией В.А. Мещерякова

ВОРОНЕЖ
2016

УДК 004.912
ББК 32.973.202
П27

Коллектив авторов:

В.А. Мещеряков, В.П. Железняк, А.О. Бондарь,
К.Я. Ряполов, С.А. Вялых

П27 **Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и органах местного самоуправления** : учебно-методическое пособие / В.А. Мещеряков [и др.]; под ред. В.А. Мещерякова. – Воронеж: Правительство Воронежской области, 2016. – 208 с. (Библиотека государственного гражданского служащего Воронежской области).

В настоящем пособии на основе требований действующего законодательства в сфере персональных данных, а также с учётом практических особенностей реализации основных мероприятий по защите информации изложена технология организации обработки и обеспечения безопасности персональных данных в органах государственной власти и местного самоуправления.

Данное учебно-методическое пособие может быть полезно для специалистов в области защиты информации, а также государственных и муниципальных служащих, занимающихся организацией обработки и обеспечением безопасности персональных данных.

УДК 004.912
ББК 32.973.202

ВВЕДЕНИЕ

В последнее время все большее внимание уделяется вопросам обеспечения безопасности персональных данных. Вступивший в силу с 2007 года Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» в 2011 – 2014 годах был в значительной степени детализирован сразу несколькими подзаконными актами всех основных регуляторов в данной сфере: Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

К сожалению, появившиеся нормативные правовые акты далеко не всегда согласованы между собой. Это вызывает значительные трудности у специалистов органов государственной власти и органов местного самоуправления занимающихся организацией обработки и обеспечением безопасности персональных данных.

Представленное учебно-методическое пособие содержит как системный взгляд на сам технологический процесс организации обработки и защиты персональных данных, обрабатываемых в информационных системах органов государственной власти и органов местного самоуправления, так и достаточно подробный анализ каждого из выделенных этапов.

Изложение материала сопровождается значительным количеством практических примеров заполнения типовых организационно-распорядительных и технологических документов, отражающих порядок создания и эксплуатации систем защиты персональных данных на всех основных этапах её жизненного цикла. При этом все возможные ситуации, возникающие в органах государственной власти и органах местного самоуправления, типизировались применительно к трём основным уровням:

- орган местного самоуправления сельского поселения с 1 – 2 сотрудниками, работающими с персональными данными и 1 – 2 информационными системами персональных данных;
- орган местного самоуправления муниципального района с 3 – 7 сотрудниками, работающими с персональными данными и 3 – 10 информационными системами, объединенными в рамках административного центра муниципального района;
- орган государственной власти субъекта Российской Федерации с 5 – 10 сотрудниками, работающими с персональными данными и более чем 3 – 5 информационными системами с наличием широкополосного доступа в сеть Интернет.

1. ПОНЯТИЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЕЁ НОРМАТИВНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Конституция Российской Федерации 1993 года в качестве высшей ценности провозгласила человека, его права и свободы. При этом признание, соблюдение и защита прав и свобод человека и гражданина объявлено важнейшей обязанностью государства.

Последовательная реализация данных конституционных принципов привела к разработке и принятию федеральных законов в сфере информационных прав человека и гражданина, где особое место занимает Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»[1].

В соответствии с данным законом персональные данные определяются как «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

Следует отметить, что приведенное определение приобрело свой нынешний вид после внесения изменений в базовый закон о персональных данных[2]. К сожалению, это лишь усугубило ситуацию с неопределенностью понимания того, что же собой представляют персональные данные. До этого момента законодатель уточнял, что персональными данными человека являются его фамилия, имя, отчество, год, месяц, число и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Еще одно действующее в настоящее время нормативное определение персональных данных содержится в Указе Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»[3]. В соответствии с названным нормативным правовым актом под персональными данными понимаются сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Таким образом, отсутствие исчерпывающего списка или иным образом строго определенного перечня сведений, относящихся к категории персональных данных, вынуждает обращаться к цели принятия Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», закрепленной в статье 2. В соответствии с данной статьёй целью названного закона является обеспечение защиты прав и свобод человека и гражданина при обра-

---

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451.

[2] Федеральный закон от 25 июля 2011 года № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства Российской Федерации, 01 августа 2011 года № 31, ст. 4701.

[3] Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации, 10 марта 1997 года № 10, ст. 1127.

ботке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайны.

Следовательно, решая вопрос о принадлежности каких-либо сведений о физическом лице к персональным данным, необходимо в первую очередь оценить, затрагивают ли эти сведения права и свободы человека и гражданина и затронут ли частную жизнь человека нарушения режима конфиденциальности этих сведений.

Приведенная точка зрения полностью согласуется с распространенным в мировой практике и считающимся чуть ли не каноническим критерием «чувствительности» сведений о человеке как индикаторе их принадлежности к персональным данным. Считается, что все сведения о человеке можно условно разделить на «нейтральные», к распространению которых человек относится равнодушно, и «чувствительные», распространение и раскрытие которых стремится не допустить. При этом именно последние сведения и образуют то, что мы объединяем понятием персональные данные[4].

Подобный подход является во многом субъективным, поскольку сильно зависит от личности каждого субъекта персональных данных и, на наш взгляд, может быть эффективно использован только при рассмотрении различного рода инцидентов и судебных споров, т.е. ситуаций, когда факт раскрытия или распространения персональных данных уже имел место. Его использование в целях организации систем защиты персональных данных и предотвращение фактов их раскрытия и распространения будет менее эффективно.

В рамках определения категории персональных данных действующим законодательством выделяются отдельные группы сведений, для которых установлены особые режимы обработки[5]:

- **Специальные категории персональных данных**, отражающие национальную принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и интимную жизнь субъекта персональных данных.
- **Биометрические персональные данные**, отражающие физиологические и биологические особенности человека, на основании которых можно установить его личность.
- **Общедоступные персональные данные**, отражающие сведения о субъекте персональных данных, полученные из общедоступных источников. В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите ин-

---

[4] WakesRaymond. Protection of Privacy. London: Sweet&Maxwell, 1980. P. 31.

[5] Статьи 10 и 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451; Часть 5 Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.

формации» общедоступной считается информация, доступ к которой не ограничен. К числу таких общедоступных источников персональных данных можно отнести различные справочники, адресные книги, энциклопедии, издаваемые в печатном или электронном виде либо размещаемые в сети Интернет, либо накапливаемые в библиотеках, архивах, органах государственной власти и органах местного самоуправления.

- **Иные категории персональных данных –** персональные данные, не относящиеся к категории специальных, биометрических и общедоступных персональных данных.

Анализ массива действующего законодательства в сфере информационного права, персональных данных, а также доступных источников специальной литературы и сети Интернет показал, что сведения, относимые к категории персональных данных, могут быть условно разделены на восемь основных групп и определены следующим образом.

Личные данные: фамилия, имя, отчество и сведения об их изменении; место, число, месяц и год рождения; фотографическое изображение человека; семейное положение; сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, номер контактного телефона).

Учётные данные государственных органов: паспортные данные; адрес регистрации и фактического проживания; гражданство; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета застрахованного лица; номер страхового свидетельства государственного пенсионного страхования; данные страхового медицинского полиса; сведения о государственных наградах и поощрениях; сведения о воинском учете (военно-учётная специальность); сведения об исправительных работах.

Данные трудовых отношений: сведения о месте работы (должность, структурное подразделение, категория квалификации, сведения об испытательном сроке работника, период работы, стаж, сведения об аттестации, табельный номер); сведения о поощрениях и взысканиях; сведения о предыдущих местах работы и особенностях трудовой деятельности; основание прекращения трудового договора (увольнения); сведения об отпуске и командировках; сведения о временной нетрудоспособности.

Квалификационные данные: образование (наименование учебного заведения, место и год окончания, присвоенная квалификация); сведения о повышении квалификации и профессиональной переподготовке; сведения о профессиональной пригодности; сведения о наличии специальных знаний в определенных сферах; сведения о знании иностранных языков; сведения о наличии учёной степени и учёного звания.

Коммуникационные данные: номера контактных телефонов, адреса электронной почты, учётные имена в социальных сетях, почтовый адрес.

Медицинские данные: сведения о состоянии здоровья, фактах и результатах прохождения профессиональных медицинских осмотров; сведения об инвалидности.

Финансово-экономические данные: доходы; сведения об удержаниях из заработной платы; сведения о выданных подотчетных суммах; сведения о лицевом счёте в банке; сведения о выданных банковских картах, займах, кредитах; сведения о выплачиваемых алиментах.

Политические, религиозные и иные данные: национальная принадлежность, вероисповедание, принадлежность к какой-либо политической партии, членстве в общественных объединениях и профсоюзах; сексуальная ориентация.

Следует помнить, что все перечисленные сведения важны лишь в тесной взаимосвязи с личностью конкретного человека. Контекст использования этих сведений должен прямо и однозначно указывать на вполне определённого субъекта персональных данных. Если такое однозначное соответствие установить невозможно, то это означает, что мы имеем дело с одной из форм обезличенных персональных данных.

2. ВИДЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Существует два основных вида обработки персональных данных: автоматизированный и неавтоматизированный.

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» автоматизированная обработка определяется как «обработка персональных данных с помощью средств вычислительной техники».

Определение неавтоматизированной обработки персональных данных дано в постановлении Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». В соответствии с пунктами 1 и 2 названного постановления обработка персональных данных, содержащихся в информационной системе персональных данных 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. При этом обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из неё.

Таким образом, обработка персональных данных является неавтоматизированной, если осуществляется при непосредственном участии человека. Примером неавтоматизированной обработки персональных данных может служить выдача одноразового бумажного пропуска на территорию организации.

Однако сразу следует предостеречь от ошибок, связанных с неправильной трактовкой приведенных определений. Почти все операции с персональными данными осуществляет человек, но это не означает, что обработка неавтоматизированная. Достаточно сохранить информацию в виде электронного документа на компьютере, и обработка станет автоматизированной.

Более детальное определение содержания автоматизированной обработки персональных данных приведено в Конвенции от 28 января 1981 года «О защите физических лиц при автоматизированной обработке персональных данных»[6]. Этим актом вводится понятие «автоматизированный файл», определяемое как любой набор данных, подвергающийся автоматизированной обработке и, соответственно, «автоматизированная обработка» включает в себя все операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических

[6] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Официальный интернет-портал правовой информации – http://www.pravo.gov.ru, 11.10.2013 (дата обращения 30.03.2014).

и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение.

Повышенное внимание к вопросам автоматизации обработки персональных данных вызвано необходимостью выполнения специальных норм законодательства, касающихся использования информационных технологий, к тому же в настоящее время нормативно-правовая база может толковаться весьма неоднозначно, особенно в части предъявления требований к информационным системам.

Так, в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», информационная система персональных данных определена как совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Приведенное определение является составным, поскольку основывается на совокупности понятий, введенных целым рядом федеральных законов и нормативных актов Правительства Российской Федерации.

В соответствии с Гражданским кодексом Российской Федерации под базой данных понимается представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)»[7].

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[8] информационные технологии определены как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются 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 тому подобное), средства защиты информации, применяемые в информационных системах.

---

[7] Пункт 2 статьи 1260 Гражданского кодекса Российской Федерации (часть четвертая) от 18 декабря 2006 года № 230-ФЗ // Собрание законодательства Российской Федерации, 25.12.2006, № 52 (1 ч.), ст. 5496.

[8] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.

Таким образом, в состав технических средств входят и копировальные устройства, и программное обеспечение, однако ключевым в определении информационной системы персональных данных является понятие «база данных». Из этого определения следует, что обработка базы данных осуществляется с помощью компьютера. Если же обработка ведется без использования средств информатизации и связи, а также базы данных, то формально информационная система отсутствует. Кроме того, без технических средств, позволяющих осуществлять обработку персональных данных, база данных также не может быть признана информационной системой.

Исходя из вышеизложенного, можно сделать однозначный вывод о наличии автоматизированной обработки персональных данных в информационных системах в каждом органе государственной власти и органе местного самоуправления, поэтому далее будем рассматривать только автоматизированную обработку персональных данных в информационных системах персональных данных.

3. ТЕХНОЛОГИЯ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ

Формирование технологии решения задачи организации обработки и обеспечения безопасности персональных данных в органах государственной власти и органах местного самоуправления представляется самостоятельным и достаточно сложным вопросом по целому ряду причин.

Во-первых, сфера защиты персональных данных и конфиденциальной информации вообще при её обработке в информационных системах регулируется значительным количеством нормативных правовых актов разного уровня (от федеральных законов и постановлений Правительства Российской Федерации до ведомственных приказов и стандартов) и различных ведомств (Роскомнадзор, ФСБ России, ФСТЭК России). При этом терминология, подходы в ряде случаев созвучны по названиям, но существенно различаются по содержанию, что приводит к определенной путанице.

Во-вторых, бездумное выполнение требований всего массива нормативных актов в сфере персональных данных приводит к необходимости разработки огромного количества документов (до нескольких десятков), которые специалисты органов государственной власти и особенно органов местного самоуправления зачастую не могут подготовить самостоятельно. Существующие в настоящее время варианты подобных документов грешат размытостью содержания и многократным дублированием норм действующего законодательства. В связи с этим, как нам представляется, вполне уместен творческий подход к формированию необходимого пакета документов, обеспечивающий их предельную лаконичность и функциональную направленность, при безусловном выполнении всех требований действующего законодательства.

Последовательность решения задач организации обработки персональных данных и обеспечения их безопасности в информационных системах органов государственной власти и органов местного самоуправления представлена на рис. 1.

Начальным этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления является назначение должностных лиц, ответственных за организацию обработки персональных данных и за обеспечение их безопасности. Эти сотрудники организуют всю дальнейшую работу и в большинстве случаев осуществляют контроль эффективности проводимых мероприятий. Одновременно с назначением указанных ответственных лиц разрабатываются и утверждаются их должностные инструкции.

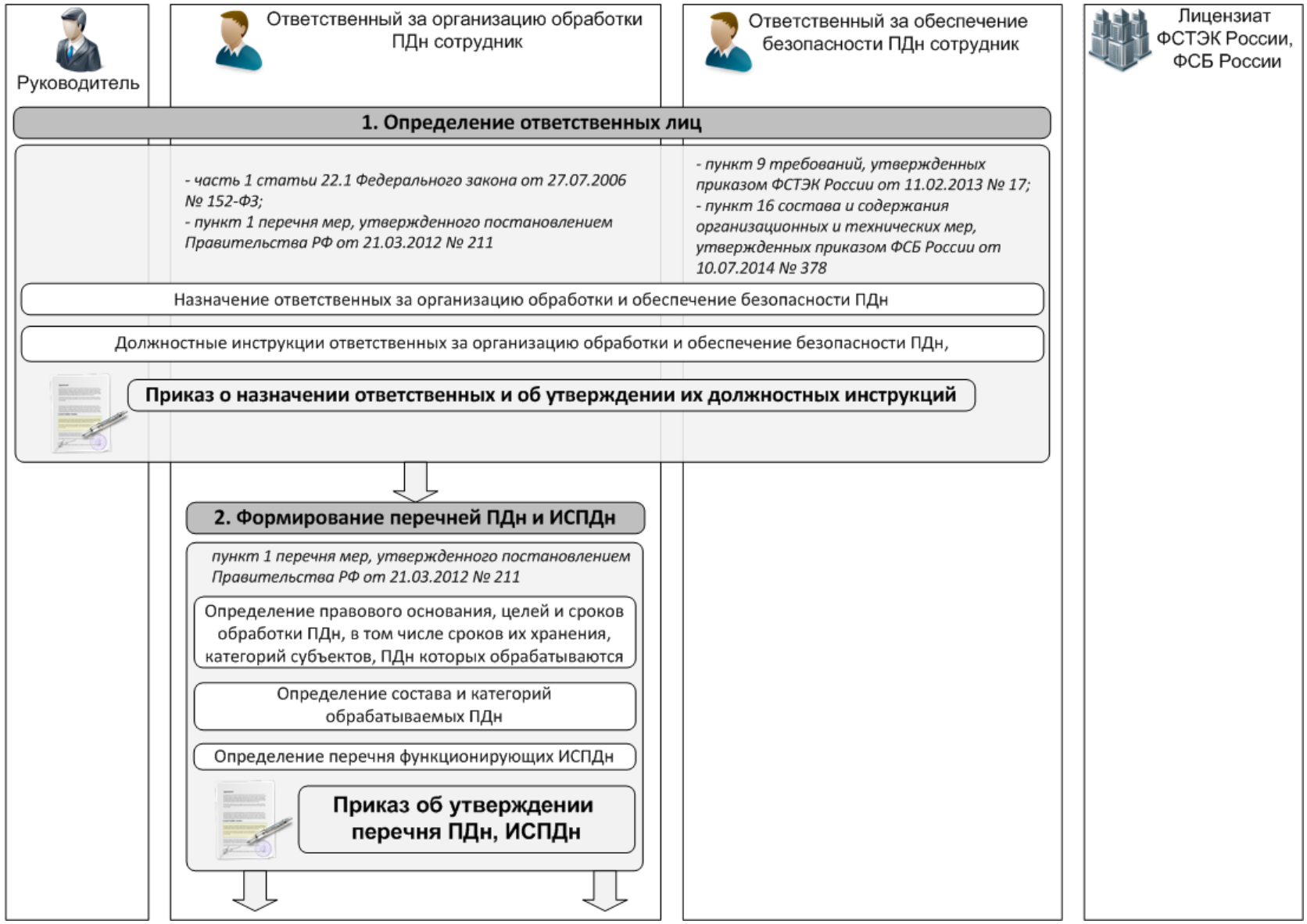
Руководитель
Ответственный за организацию обработки ПДн сотрудник
Ответственный за обеспечение безопасности ПДн сотрудник
Лицензиат ФСТЭК России, ФСБ России
1. Определение ответственных лиц
- часть 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ;
- пункт 1 перечня мер, утвержденного постановлением Правительства РФ от 21.03.2012 № 211
- пункт 9 требований, утвержденных приказом ФСТЭК России от 11.02.2013 № 17;
- пункт 16 состава и содержания организационных и технических мер, утвержденных приказом ФСБ России от 10.07.2014 № 378
Назначение ответственных за организацию обработки и обеспечение безопасности ПДн
Должностные инструкции ответственных за организацию обработки и обеспечение безопасности ПДн,
Приказ о назначении ответственных и об утверждении их должностных инструкций
2. Формирование перечней ПДн и ИСПДн
пункт 1 перечня мер, утвержденного постановлением Правительства РФ от 21.03.2012 № 211
Определение правового основания, целей и сроков обработки ПДн, в том числе сроков их хранения, категорий субъектов, ПДн которых обрабатываются
Определение состава и категорий обрабатываемых ПДн
Определение перечня функционирующих ИСПДн
Приказ об утверждении перечня ПДн, ИСПДн

Рис.1. Технологическая схема организации обработки и обеспечения безопасности персональных данных в органах государственной власти и местного самоуправления

Руководитель

Ответственный за организацию обработки ПДн сотрудник

5. Формирование политики обработки ПДн

- пункт 1 перечня мер, утвержденного постановлением Правительства РФ от 21.03.2012 № 211;
- подпункты «а» и «в» пункта 5 состава и содержания организационных и технических мер, утвержденных приказом ФСБ России от 10.07.2014 № 378

Разработка, правил обработки ПДн, рассмотрения запросов субъектов ПДп или их представителей, осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, порядка доступа в помещения в которых ведется обработка ПДн в рабочее и нерабочее время, а также в нештатных ситуациях, типовой формы согласия на обработку ПДн, типовой формы разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн, утверждение списка лиц, допущенных к содержанию электронного журнала сообщений

- пункт 5 части 2 статья 19 Федерального закона от 27.07.2006 № 152-ФЗ;
- пункт 13 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 г. РФ № 1119;
- подпункт «б» пункта 5 состава и содержания организационных и технических мер, утвержденных приказом ФСБ России от 10.07.2014 № 378

Организация учета, хранения и уничтожения машинных носителей ПДн

Приказ об утверждении документов

Ответственный за обеспечение безопасности ПДн сотрудник

7. Формирование облика и внедрение системы защиты ПДн в ИСПДн

- пункт 2 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ;
- пункт 13 требований, утвержденных приказом ФСТЭК России от 11.02.2013 № 17;
- подпункты «а» и «г» пункта 5 состава и содержания организационных и технических мер, утвержденных приказом ФСБ России от 10.07.2014 № 378

Требования к системе защиты ПДн в ИСПДн

Лицензиат ФСТЭК России, ФСБ России

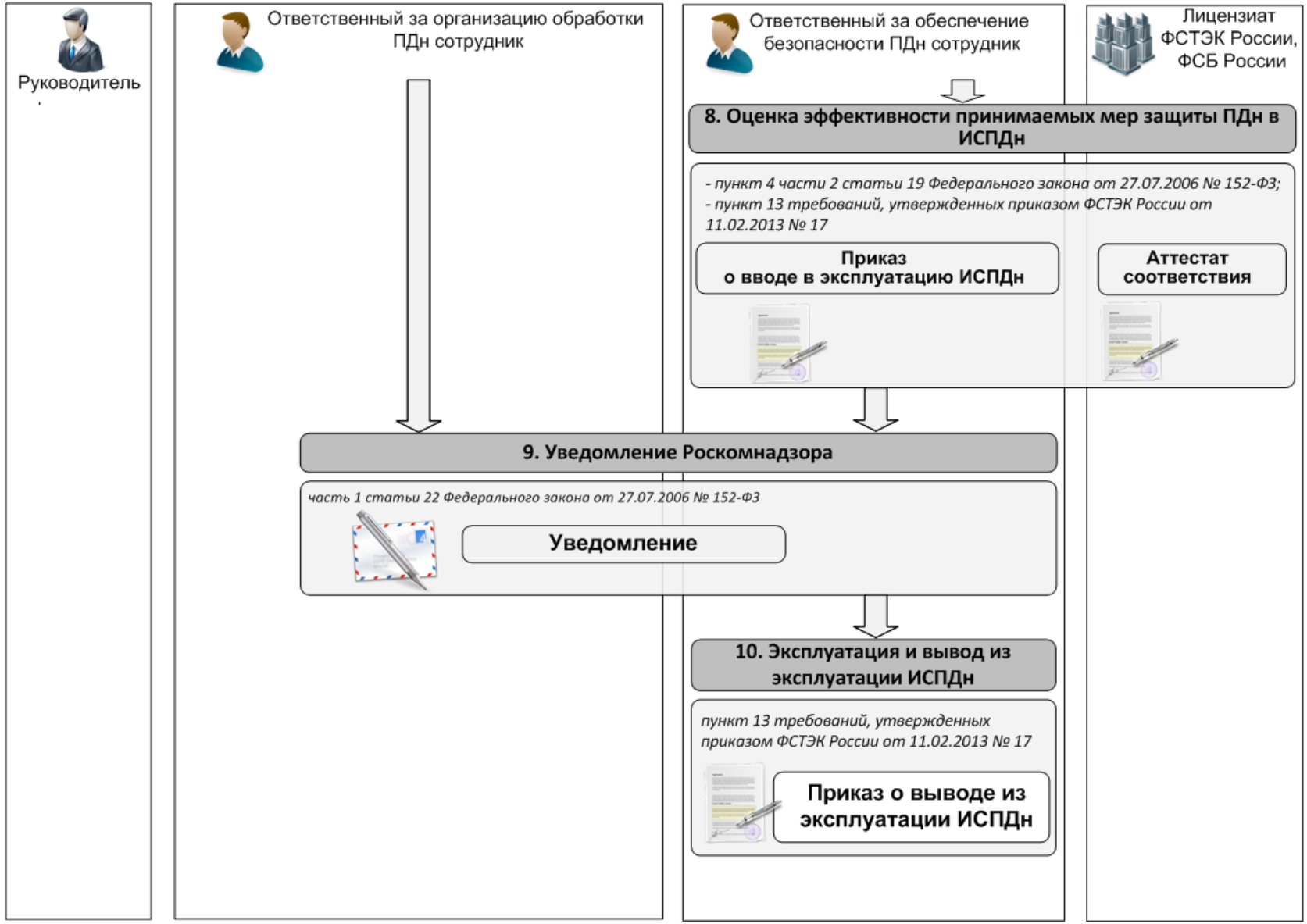

Рис. 1. Технологическая схема организации обработки и обеспечения безопасности персональных данных в органах государственной власти и местного самоуправления (продолжение)

Результатом работы на данном этапе является правовой акт о назначении ответственных, а также их должностные инструкции, юридически оформленные в виде приложения к этому акту. Кроме этого, готовятся необходимые изменения в должностные регламенты вновь назначенных ответственных сотрудников или изменения в положения о соответствующих подразделениях.

В случае использования информационных систем персональных данных, требующих обеспечения 1-го уровня защищенности персональных данных в соответствии с требованиями «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378, необходимо назначить ответственного за периодический контроль ведения электронного журнала безопасности. Данные полномочия целесообразнее всего возложить на ответственного за обеспечение безопасности персональных данных с отражением соответствующих обязанностей в его должностной инструкции.

Следует отметить, что определение уровня защищенности информационных систем осуществляется на третьем этапе технологической схемы организации обработки и обеспечения безопасности персональных данных, поэтому необходимость назначения данного ответственного на первом этапе трудно предусмотреть.

Следующим этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления является определение правового основания, целей и сроков обработки персональных данных, в том числе сроков их хранения, категорий субъектов, персональные данные которых подлежат обработке, а также определение перечня функционирующих информационных систем персональных данных.

Исходными данными для выполнения работ являются действующие нормативные правовые акты, организующие работу органа государственной власти или органа местного самоуправления. Основным исполнителем данного этапа является сотрудник, ответственный за организацию обработки персональных данных.

Результатом работы на рассматриваемом этапе является издание приказа (распоряжения) об утверждении перечней обрабатываемых персональных данных и используемых информационных систем персональных данных.

Третьим этапом технологии организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления является определение уровня защищённости персональных данных, типа и класса защищённости информационных систем персональных данных.

Исходные данные для выполнения работ получаются по итогам выполнения второго этапа технологической схемы. Реализация всех мероприятий осуществляется совместно сотрудниками, ответственными за организацию обработки и обеспечение безопасности персональных данных. Рекомендация о привлечении именно двух исполнителей для выполнения данной работы далеко не случайна. В рамках рассматриваемых мероприятий ответственный за обеспечение безопасности персональных данных совершенно обоснованно постарается максимально завысить требования и установит наиболее жёсткие условия для использования информационной системы персональных данных, поскольку именно в таких условиях возможно обеспечить требуемый уровень безопасности. Естественно, что это повлечёт за собой необходимость выделения ощутимых финансовых, организационных и технических средств. В то же время, как было отмечено ранее, сотрудник, ответственный за организацию обработки персональных данных, обычно является руководителем (как минимум среднего звена) в сфере ответственности которого кроме персональных данных достаточно много иных направлений. В связи с этим он может взвесить важность и актуальность каждого из направлений деятельности органа государственной власти или органа местного самоуправления и реально определить объём сил и средств, которые следует выделить в данный момент времени для решения задач обеспечения безопасности персональных данных.

Результатом работы на данном этапе является акт классификации информационной системы персональных данных, утверждённый руководителем органа государственной власти или органом местного самоуправления. В случае наличия в органе государственной власти (органе местного самоуправления) нескольких информационных систем персональных данных, для каждой из них разрабатывается и утверждается отдельный акт классификации.

На четвёртом этапе работы необходимо определить перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных, либо доступ к ним.

Исходными данными для выполнения работ являются результаты выполнения второго этапа технологической схемы. Основным исполнителем данного этапа является сотрудник, ответственный за организацию обработки персональных данных.

Исходя из сформированного перечня должностей, определяется список сотрудников, допущенных к обработке персональных данных в информационных системах, и назначается сотрудник, ответственный за проведение мероприятий по обезличиванию персональных данных. Вместе с проведением названных мероприятий разрабатывается типовое обязательство сотрудника, допущенного к обработке персональных данных прекратить их обработку в случаях, предусмотренных действующим законодательством.

Результатом работы на данном этапе будет приказ (распоряжение) руководителя органа государственной власти (органа местного самоуправления), утверждающий соответствующие перечни должностей и сотрудников,

допущенных к обработке персональных данных, а также типовое обязательство прекратить обработку персональных данных.

Пятым этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления является разработка политики безопасности персональных данных, включающей формирование правил их обработки, рассмотрения запросов субъектов персональных данных или их представителей, осуществления внутреннего контроля соответствия обработки персональных данных требованиям по их защите, порядка доступа в помещения, в которых ведется обработка персональных данных, типовых форм согласия на обработку персональных данных и разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональных данные.

Кроме этого, на рассматриваемом этапе разрабатывается политика учёта и хранения машинных носителей персональных данных. Основным исполнителем данного этапа является лицо, ответственное за организацию обработки персональных данных.

Результатом работы на данном этапе будет приказ (распоряжение) руководителя органа государственной власти (органа местного самоуправления),утверждающий правила обработки персональных данных и регламент учёта, хранения и уничтожения машинных носителей персональных данных. Отдельно следует отметить, что в соответствии с требованиями действующего законодательства документы, разработанные на данном этапе и определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте органа государственной власти или органа местного самоуправления в течение 10 дней после их утверждения.

Шестым этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти или органов местного самоуправления будет определение угроз и нарушителей безопасности персональных данных при их обработке в информационных системах.

Информационной основой для решения этих задач будут полученные на третьем этапе оценки уровня исходной защищённости персональных данных и класса защищённости информационной системы.

Результатом работы на данном этапе будет сформированная модель угроз безопасности персональных данных при их обработке в информационной системе. Данная модель утверждается руководителем органа государственной власти или органа местного самоуправления. Основным исполнителем названных работ является сотрудник, назначенный ответственным за обеспечение безопасности персональных данных. В случае необходимости, а также при наличии организационных и финансовых возможностей для решения данной задачи могут привлекаться иные сотрудники органа власти или органа местного самоуправления (в первую очередь системный администратор и сотрудники, осуществляющие техническое обслуживание информаци-

онных систем персональных данных), а также внешние исполнители – лицензиаты ФСБ России и ФСТЭК России.

Наиболее сложным и неоднозначным с точки зрения реализации задач является седьмой этап технологии – формирование облика и внедрение системы защиты персональных данных.

В зависимости от сложности эксплуатирующихся в органах государственной власти и органах местного самоуправления информационных систем этот этап может быть как исключительно сложным, так и предельно простым.

В первом случае на основе сформированной и утвержденной на шестом этапе модели угроз безопасности персональных данных, в соответствии с действующими стандартами на создание технических систем, готовится техническое задание на разработку системы защиты персональных данных. В связи с поэтапным введением с 1 января 2014 года в действие Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» все дальнейшие действия связаны с проведением предусмотренных действующим законодательством конкурсных процедур, и их продолжительность растягивается на весьма продолжительное время.

В результате завершения всех работ на основании сформированного технического задания определяется облик всей системы, комплектуются необходимые средства защиты, а также осуществляется их внедрение и настройка в информационной системе персональных данных.

Во втором, простейшем, случае формирование облика системы защиты персональных данных фактически сводится к выбору одного из имеющихся на рынке готовых средств защиты информации, его приобретению и установке в информационную систему персональных данных.

Следующим этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти или органов местного самоуправления является проверка эффективности принимаемых мер по защите персональных данных.

Содержанием данной деятельности является анализ особенностей обработки и защиты информации в реальной информационной системе, проведение внутренних тестовых испытаний применяемых средств защиты информации на соответствие установленным требованиям по безопасности персональных данных. Выполнение этой работы требует наличия специальной квалификации и, зачастую, соответствующего оборудования. В связи с этим в соответствии с требованиями действующего законодательства эта деятельность осуществляется организациями-лицензиатами основных регуляторов в сфере защиты информации.

Результатом проведения аттестационных испытаний является выданный «Аттестат соответствия», подтверждающий, что информационная система персональных данных соответствует установленным требованиям по обеспечению безопасности персональных данных.

Предпоследним этапом рассматриваемой технологии является ввод в эксплуатацию информационной системы персональных данных, который юридически оформляется соответствующим приказом (распоряжением) руководителя органа государственной власти (органа местного самоуправления). Основным исполнителем работ данного этапа является сотрудник, ответственный за обеспечение безопасности персональных данных.

Завершающим этапом организации обработки и обеспечения безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления является уведомление территориального органа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Такое позиционирование названного этапа обусловлено тем, что в соответствии с установленными требованиями по содержанию уведомления оно должно содержать описание предпринимаемых мер по обеспечению безопасности персональных данных и используемых средствах защиты информации.

Значительная часть работы по обеспечению безопасности персональных данных в информационных системах органов государственной власти и органов местного самоуправления проводится в ходе эксплуатации созданной в результате выполнения всех перечисленных ранее этапов информационной системы с системой защиты информации.

В период эксплуатации в постоянном режиме осуществляется выявление инцидентов информационной безопасности, и принимаются адекватные меры реагирования. Проводится контроль за обеспечением установленного уровня защищённости персональных данных и в необходимых случаях осуществляется администрирование конфигурации информационной системы и её системы защиты информации.

Основным исполнителем работ данного этапа является сотрудник, ответственный за обеспечение безопасности персональных данных.

Каждый из названных выше этапов имеет свою специфику и особенности, которые подробно рассмотрены в следующей части данного пособия.

4. ОСНОВНЫЕ ЭТАПЫ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ

4.1. Определение ответственных за организацию обработки персональных данных и обеспечение безопасности персональных данных

В соответствии с требованиями части 1 статьи 22.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» каждый орган государственной власти или орган местного самоуправления, а также каждое государственное или муниципальное учреждение, являющиеся самостоятельным юридическим лицом, осуществляющие обработку персональных данных, обязано назначить ответственного за организацию обработки персональных данных. Юридически данное решение оформляется в виде соответствующего приказа или распоряжения руководителя.

Поскольку основной задачей назначенного должностного лица будет организация обработки персональных данных, то данный сотрудник должен обладать необходимыми организационными полномочиями. Как показывает практика, наиболее подходящей кандидатурой для выполнения указанных функций является заместитель руководителя органа исполнительной власти или органа местного самоуправления, отвечающий за организационную и кадровую работу. Назначение нескольких ответственных за организацию обработки персональных данных представляется неоправданным, поскольку требует чёткого разграничения их сфер ответственности и увеличивает нагрузку на руководителя, который в данном случае вынужден брать на себя ответственность за обеспечение безопасности персональных данных, а также координировать деятельность всех назначенных ответственных.

В случае, если орган власти имеет сложную организационную структуру, многочисленный штат сотрудников, а, самое главное, большое число информационных систем, обрабатывающих персональные данные, то задачи по обеспечению их защиты могут быть возложены на соответствующее структурное подразделение (например, отдел информационной безопасности), а ответственным должностным лицом может быть назначен руководитель данного подразделения.

Следует обратить внимание, что задачи внедрения и эксплуатации информационных технологий и обеспечение информационной безопасности персональных данных принципиально отличаются друг от друга, поэтому подходить к возложению функций обеспечения информационной безопасности на отдел информационных технологий необходимо с большой осторожностью. Поясним данную ситуацию более подробно.

Основной целью подразделения, отвечающего за эксплуатацию информационных технологий, является обеспечение постоянной работоспособности, доступности и удобства работы сотрудников организации со всеми имеющимися информационными ресурсами и системами. В то же время вы-

полнение требования по обеспечению безопасности персональных данных может снижать доступность определённых ресурсов и удобство работы в тех информационных системах, где обрабатываются персональные данные. Вполне закономерно, что подобная ситуация приводит к соблазну отключить имеющиеся средства защиты информации или минимизировать их использование. При этом если функции эксплуатации информационных технологий и обеспечения информационной безопасности персональных данных сосредоточены в одних руках, то этот соблазн многократно возрастает. Факт назначения ответственным за обеспечение безопасности персональных данных внешнего по отношению к отделу информационных технологий руководителя (например, заместителя руководителя организации, отвечающего за организационную и кадровую работу) существенно положение дел не меняет. Это связано с тем, что данный руководитель, с одной стороны, нагружен собственной работой и не имеет необходимого объёма времени, чтобы вникнуть в технические детали организации обработки информации, а с другой стороны, как правило, не имеет необходимого образования и специальной подготовки в сфере информационных технологий.

На наш взгляд оптимальным решением вопроса будет создание специального подразделения, отвечающего не только за защиту персональных данных, но и за информационную безопасность в целом. При этом такое подразделение должно быть подчинено заместителю руководителя организации отвечающего за организационную и кадровую работу или непосредственно самому руководителю организации. Это подразделение может быть очень малочисленно (вплоть до 2 человек), выполнять дополнительные задачи, но оно не должно быть подчинено руководителю одела информационных технологий.

Следуя логике организации государственного управления, для каждого из назначаемых ответственных сотрудников требуется разработка соответствующих должностных инструкций. Вместе с тем (как показывает практика) увеличение количества различного рода регламентов, инструкций, правил и прочих правовых актов, принимаемых для регулирования служебной деятельности сотрудника, приводит к снижению эффективности его работы. Как нам представляется, идеальным вариантом в подобной ситуации является наличие одного единственного документа – должностного регламента государственного или муниципального служащего, особенно учитывая, что он обязательно должен соответствовать требованиям Федерального закона от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе» и подавляющему большинству законов субъектов Российской Федерации, регламентирующих вопросы организации муниципальной службы[9].

Вполне логичным могло бы быть использование этого же подхода и для регламентирования прав и обязанностей ответственного за организацию

---

[9] См. Закон Воронежской области от 27 декабря 2007 года № 175-ОЗ «О муниципальной службе в Воронежской области» // Собрание законодательства Воронежской области, 28.01.2008, № 12, ст. 434.

обработки персональных данных. Однако часть 10 подпункта б) пункта 1 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, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, прямо устанавливает требование существования самостоятельной должностной инструкции для ответственного за обработку персональных данных.

В связи с этим вполне логичным будет создание двух самостоятельных инструкций для рассматриваемых категорий ответственных лиц. При этом в их должностные регламенты вносится указание на обязанность выполнения требований, установленных в соответствующих инструкциях.

Пример формулировки положения, включаемого в соответствующий должностной регламент, может выглядеть следующим образом.

Исполняет обязанности по организации обработки персональных данных в <*наименование органа государственной власти или местного самоуправления*> в соответствии с требованиями должностной инструкции ответственного за организацию обработки персональных данных, а также действующих нормативных правовых актов Роскомнадзора, ФСТЭК России и ФСБ России.

Примерный образец приказа о назначении ответственных за организацию обработки и обеспечение безопасности персональных данных в органе государственной власти и утверждении их должностных инструкций приведен в приложении № 1 к настоящему пособию.

В органах местного самоуправления муниципального района все названные выше задачи, как правило, входят в сферу ответственности руководителя аппарата администрации. Идеальной является ситуация, когда руководитель аппарата администрации муниципального района (городского округа) одновременно является заместителем главы администрации. В этом случае лучшей кандидатуры для назначения ответственного за организацию обработки персональных данных, на наш взгляд, просто не найти.

В администрациях маленьких сельских поселений, где численность всех муниципальных служащих, как правило, не превышает 3 – 5 человек, наиболее подходящей кандидатурой является главный бухгалтер администрации.

Собственно говоря, выбор в данной ситуации практически отсутствует. Глава администрации сельского поселения, исходя из смысла частей 2 и 3 статьи 22.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», таким должностным лицом быть не может. Кроме главы администрации и главного бухгалтера есть только сотрудники, которые ведут информационную систему сельского поселения (например, электронный вариант похозяйственной книги), т.е. фактически занимаются обработкой пер-

сональных данных. Поэтому возлагать на них функции организации обработки и контроля эффективности защиты персональных данных вместе с самой их обработкой было бы методически неверно.

Аргументом в пользу назначения ответственным главного бухгалтера становится ещё и то, что данный сотрудник является муниципальным служащим и, следовательно, не может выполнять только бухгалтерские функции. Примером таких дополнительных функций как раз и может выступать рассматриваемая нами деятельность.

4.2. Формирование перечней обрабатываемых персональных данных и информационных систем персональных данных

Следующим этапом технологии организации обработки и обеспечения безопасности персональных данных является определение перечня персональных данных, обрабатываемых в органе государственной власти или органе местного самоуправления.

Перечень обрабатываемых персональных данных представляет собой максимально подробный и чётко структурированный документ, содержащий информацию обо всех категориях и видах персональных данных, обрабатываемых оператором, как с применением средств автоматизации, так и без таковых. Он составляется с привлечением самого широкого круга должностных лиц, что позволяет провести анализ всех сторон деятельности органа государственной власти или органа местного самоуправления и выявить все обрабатываемые персональные данные, определить основные условия обработки, а также сроки обработки и хранения для различных их категорий.

В соответствии с частью 7 подпункта б) пункта 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утверждённого постановлением Правительства Российской Федерации от 21 марта 20012 года № 211, предусматривается всего три основания для обработки персональных данных в органах государственной власти:

- в связи с реализацией трудовых отношений;
- в связи с оказанием государственных или муниципальных услуг;
- в связи с осуществлением государственных или муниципальных функций.

Вполне очевидно, что каждая из указанных сфер обязательно присутствует в деятельности каждого органа государственной власти и органа местного самоуправления. Поэтому при формировании перечня персональных данных необходимо обязательно проанализировать все нормативные правовые акты, регламентирующие деятельность государственного или муниципального органа в каждой из этих сфер деятельности.

Перечень персональных данных, обрабатываемых в связи с реализацией трудовых отношений, касается, в основном, сотрудников государственно-

го или муниципального органа и определяется из анализа следующих нормативных правовых актов:

- Трудовой Кодекс Российской Федерации от 30 декабря 2001 года № 197-ФЗ[10];
- Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации»[11];
- Указ Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Каждый орган государственной власти или орган местного самоуправления оказывает как минимум одну государственную услугу, реализующую конституционное право граждан на обращение в эти органы. В зависимости от профиля деятельности рассматриваемого органа формируется реестр его государственных или муниципальных услуг, который в соответствии с требованиями Федерального закона от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» утверждается соответствующим нормативным правым актом высшего исполнительного органа государственной власти (для государственных услуг субъекта Российской Федерации) или решением местной администрации (для муниципальных услуг).

Для каждой государственной или муниципальной услуги разрабатывается соответствующий регламент её оказания, который содержит все исчерпывающие сведения о необходимых персональных данных.

Таким образом, перечень персональных данных, обрабатываемых в связи с оказанием государственных или муниципальных услуг, определяется исходя из анализа следующих нормативных правовых актов:

- Федеральный закон от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращения граждан»;
- Федеральный закон от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- нормативный правовой акт высшего должностного лица или высшего исполнительного органа государственной власти субъекта Российской Федерации устанавливающий исчерпывающий перечень государственных услуг и органов государственной власти субъекта Российской Федерации их оказывающих12 (норма-

[10] Трудовой кодекс Российской Федерации от 30 декабря 2001 года № 197-ФЗ // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 3.

[11] Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» // Собрание законодательства РФ, 02.08.2004, № 31, ст. 3215.

[12] Например, в Воронежской области таким нормативным правовым актом является Указ губернатора Воронежской области от 27 мая 2011 г. № 214-у «Об утверждении перечня государ-

тивный правовой акт администрации муниципального образования, устанавливающий исчерпывающий перечень муниципальных услуг, оказываемых муниципальными органами);

- нормативные правые акты органа государственной власти, утверждающие регламенты оказания соответствующих государственных услуг[13] (нормативные правовые акты муниципальных органов, утверждающие регламенты оказания соответствующих муниципальных услуг).

Кроме оказания государственных или муниципальных услуг каждый орган государственной власти или орган местного самоуправления исполняет ряд государственных или муниципальных функций. В соответствии с концепцией административной реформы в Российской Федерации в 2006 – 2010 годах[14] в каждом субъекте Российской Федерации сформирован исчерпывающий список государственных функций, оказываемых органами государственной власти субъекта Российской Федерации, и для каждой из выявленных функций разработан регламент их исполнения. Аналогичные перечни и регламенты исполнения муниципальных функций разработаны на уровне местного самоуправления.

Таким образом, перечень персональных данных, обрабатываемых в связи с исполнением государственных или муниципальных функций, определяется исходя из анализа следующих нормативных правовых актов:

- нормативный правовой акт высшего должностного лица или высшего исполнительного органа государственной власти субъекта Российской Федерации, устанавливающий исчерпывающий перечень государственных функций органов государственной власти субъекта Российской Федерации[15] (нормативный правовой акт администрации муниципального образования, устанавливающий исчерпывающий перечень муниципальных функций);
- нормативные правые акты высшего должностного лица или высшего исполнительного органа государственной власти субъекта Российской Федерации органа государственной власти, утверждающие регламенты исполнения государственных функций ор-

---

ственных услуг исполнительных органов государственной власти Воронежской области» // Молодой коммунар, № 60, 07.06.2011.

[13] В качестве примера подобного нормативного правового акта можно привести приказ департамента связи и массовых коммуникаций Воронежской области от 23 августа 2012 года № 01-06/124 «Об утверждении административного регламента по предоставлению государственной услуги «Согласование режима работы объектов почтовой связи организаций федеральной почтовой связи на территории Воронежской области» // Собрание законодательства Воронежской области, № 26, 2012, ст. 885.

[14] Концепция административной реформы в Российской Федерации в 2006 - 2010 годах, утверждена распоряжением Правительства Российской Федерации от 25 октября 2005 года № 1789-р // Собрание законодательства Российской Федерации, 14.11.2005, № 46, ст. 4720.

[15] Указ губернатора Воронежской области от 19 февраля 2009 года № 81-у «Об утверждении реестра государственных функций исполнительных органов государственной власти Воронежской области» // Собрание законодательства Воронежской области, № 2, ст. 34.

ганами государственной власти субъекта Российской Федерации[16] (нормативные правовые акты администрации муниципального образования, утверждающие регламенты исполнения соответствующих муниципальных функций).

Следует обратить особое внимание на обоснование сроков обработки и хранения всех категорий персональных данных. В соответствии с частью 2 статьи 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» хранение информации должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Проведенный таким образом анализ правовых оснований обработки персональных данных позволяет сформировать обоснованный состав персональных данных, оценить их категорию и выявить перечень информационных систем, в которых осуществляется их обработка. Результаты этой работы в соответствии с частью 7 подпункта "б" пункта 1 перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных названным выше федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21 марта 20012 года № 211, утверждаются правовым актом руководителя органа государственной власти или органа местного самоуправления.

Примерный образец распоряжения об утверждении перечней обрабатываемых персональных данных и информационных систем персональных данных в органе местного самоуправления приведен в приложении № 2 к настоящему пособию.

4.3. Определение уровня защищённости персональных данных и классификация информационных систем персональных данных

Классификация информационных систем персональных данных включает в себя определение требуемого уровня защищенности персональных данных в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и определение требуемого класса защищенности информационной системы в соответствии с приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не со-

[16] Постановление Правительства Воронежской области от 21 июля 2010 года № 611 «Об утверждении административного регламента Правительства воронежской области по исполнению государственной функции «осуществление мер по реализации, обеспечению и защите прав и свобод человека и гражданина, охране собственности и общественного порядка, противодействию терроризму и экстремизму, борьбе с преступностью» // Собрание законодательства воронежской области, № 7, ст. 458.

ставляющей государственную тайну, содержащейся в государственных информационных системах».

Реализация данных процессов является достаточно сложной задачей. Это обусловлено наличием созвучной терминологии для различных понятий обеспечения безопасности информации и противоречивыми требованиями нормативных правовых актов регулирующих данную сферу[17]. Следует отметить, что предпринятая Вторым Управлением ФСТЭК попытка как-то снять имеющиеся разночтения[18] лишь добавила трудностей, которые и без того были непреодолимы для исполнителей уровня муниципального района и сельского поселения. В связи с этим данный вопрос требует детального рассмотрения.

Правовую основу необходимости классификации информационных систем образуют положения статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», которая устанавливает, что оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры по их защите от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

При этом частями 2 – 4 названной статьи устанавливается конкретный перечень мер, которыми достигается обеспечение безопасности персональных данных, и Правительство Российской Федерации наделяется правом установить уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных.

Реализуя предоставленное законом право, Правительство Российской Федерации приняло постановление от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в котором установило требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

---

[17] Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257; Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.

[18] Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 июля 2013 года № 240/22/2637 // http://fstec.ru/component/attachments/download/574 (дата обращения 30.032014 года).

Казалось бы, все просто, логично и понятно. Однако следует помнить о двух весьма значимых юридических фактах:

1. Персональные данные относятся к категории конфиденциальной информации (Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»[19]) со всеми вытекающими обязанностями по их защите.

2. Информационная система персональных данных в органах государственной власти и органах местного самоуправления (с учетом положения части 1 статьи 13 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[20]) является государственной (муниципальной) информационной системой и для неё обязательны мероприятия по защите обрабатываемой информации.

Таким образом, выстраивается вторая цепочка рассуждений, приводящая к необходимости проведения классификации информационных систем персональных данных по требованиям защиты информации.

Правовую основу деятельности по второй цепочке рассуждений (защите конфиденциальной информации в государственных (муниципальных) информационных системах) образует Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 16 которого устанавливает обязанность операторов информационных систем к выполнению ряда организационных и технических мер по защите обрабатываемой в них информации. Требования по защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Реализуя предоставленное названным законом полномочие, ФСТЭК России как федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, издала приказ от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В соответствии с названными требованиями (пункт 14) установлена необходимость классификации информационной системы по требованиям защиты информации. Более того, перечень обязательных мероприятий по обеспечению безопасности информации основывается на установленном классе защищённости.

---

[19] Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации, 10.03.1997, № 10, ст. 1127.

[20] Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.

Анализ правовых оснований необходимости проведения двух классификаций показывает, что они юридически абсолютно равнопрочны (и та, и другая основаны на требованиях федеральных законов), однако законодательные нормы соотносятся, как «общее и частное (специальное)». В нашем случае, при решении вопросов обеспечения безопасности персональных данных Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержит общие нормы, а Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» содержит специальные нормы.

В соответствии с принятым в юриспруденции подходом при равной юридической силе нормативных правовых актов приоритетом пользуется специальная норма. Однако общая норма продолжает действовать в части, не противоречащей специальной.

Таким образом, мы имеем по сути две основанные на требованиях действующего законодательства классификации и две итоговые оценки, получаемые по различным методикам. С одной стороны, определение класса защищённости информационной системы, с другой стороны, определение уровня защищённости персональных данных.

В сложившейся ситуации вполне закономерным является вопрос о соотношении этих классификаций.

Абзац 2 пункта 14.2 приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливает эквивалентность понятий «класс защищённости информационной системы» и «уровень защищённости информации».

Вместе с тем даже поверхностный анализ последующих действий (основанных и во многом определяемых результатами классификации) по обеспечению безопасности информации показывает, что существуют значимые различия в содержании этих понятий. Справедливость данного утверждения подтверждается информационным сообщением ФСТЭК России от 15 июля 2013 года № 240/22/2637[21], в пункте 2 которого допускаются случаи несовпадения полученных в установленном порядке оценок уровней защищённости персональных данных и класса защищённости государственной информационной системы. Более того, даются рекомендации о повышении класса защищённости информационной системы до уровня защищённости персональных данных.

---

[21] Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 июля 2013 года № 240/22/2637 // http://fstec.ru/component/attachments/download/574 (дата обращения 30.032014 года).

Подводя итог всему изложенному выше, следует сделать вывод о необходимости проведения двух классификаций. Единственным упрощением, возможным в данной ситуации, является разработка единого документа, отражающего результаты классификационной работы по двум рассмотренным направлениям, – акта классификации.

Классификация информационных систем по требованиям защиты информации производится в соответствии с положениями части 14 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказа ФСТЭК России от 11 февраля 2013 года № 17.

Исходя из содержания данного этапа работы, её выполнение должно быть возложено на ответственного за организацию обработки персональных данных.

В том случае, если он не может взять на себя ответственность за правильное проведение классификации, в органе государственной власти или органе местного самоуправления может быть создан временный коллегиальный орган – комиссия по определению уровней защищённости персональных данных, обрабатываемых в информационных системах персональных данных, и их классификации.

Пример оформления приказа о создании такой комиссии приведён в приложении № 3 к настоящему пособию.

После выполнения возложенной на комиссию функции она может не прекращать свою деятельность и решать аналогичные задачи для вновь создаваемых информационных систем персональных данных, а также в случае необходимости пересмотра класса защищённости информационной системы или уровня защищённости персональных данных.

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» логика определения уровней защищённости персональных данных выстроена следующим образом.

1. Определение типа актуальности угроз безопасности персональных данных. В зависимости от наличия угроз, обусловленных недокументированными (недекларированными) возможностями в системном и прикладном программном обеспечении, устанавливается тип актуальности угроз безопасности персональных данных.

Недекларированные возможности — это функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Интегрированное представление процесса определения типа актуальности угроз безопасности персональных данных, установленного пунктом 6 требований, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119, представлено в таблице 1.

Таблица 1

Актуальность угроз, связанных с наличием недокументированных (недекларированных) возможностей в программном обеспечении		Тип актуальных угроз безопасности персональных данных
Системное программное обеспечение	Прикладное программное обеспечение	
Есть (1)	Есть (1)	1
Есть (1)	Нет (0)	1
Нет (0)	Есть (1)	2
Нет (0)	Нет (0)	3

Фактически, если вероятность существования недекларированных возможностей в системном и (или) прикладном программном обеспечении информационной системы достаточно высока, то будет необходимо обеспечить высокий уровень защищённости персональных данных. В свою очередь это потребует значительных финансовых, технологических и организационных ресурсов. Низкая вероятность присутствия недекларированных возможностей влечёт допустимость низкого уровня защищённости, что весьма существенно упрощает набор требований по защите информации и как следствие ощутимую экономию средств, выделяемых на обеспечение информационной безопасности.

Не секрет, что практически все программное и аппаратное обеспечение, используемое для создания информационных систем, использующихся в органах государственной власти, разработано и произведено за рубежом. Его объемы (размер программного кода) и разнообразие настолько велики, а его анализ на предмет наличия недекларированных возможностей настолько сложен и трудоёмок, что рассчитывать на получение каких-либо обоснованных оценок вероятности существования недекларированных возможностей (не говоря уже об однозначном ответе) в ближайшее время не приходится.

Использование программного обеспечения, прошедшего специальную проверку, к сожалению, серьезных гарантий отсутствия недекларированных возможностей также не даёт. Это связано с тем, что соответствующий сертификат выдается на фиксированную сборку программного продукта и малейшее изменение (обновление) любой его части лишает программное обеспечение сертификата. Вместе с тем очень часто мы сталкиваемся с ситуациями, когда в уже сертифицированном программном обеспечении находятся дыры безопасности, которые признаются самим производителем. В качестве реакции на найденные дефекты разработчик выпускает так называемые «патчи» – небольшие программы, вносящие необходимые изменения в исходный код программного продукта, что неминуемо лишает его соответствующего сертификата.

В результате получается парадоксальная ситуация. С одной стороны, программный продукт сертифицирован, но в нём есть изъяны информационной безопасности, и этот факт официально признаётся разработчиком. С другой стороны, дефект программного продукта ликвидирован (внесено необходимое изменение в программный код), но сертификат аннулирован, поскольку содержимое программного кода изменено.

Таким образом, значимых гарантий того, что в используемом для создания информационной системы персональных данных программном обеспечении отсутствуют недекларируемые возможности нет.

Другое дело — оценка актуальности угроз информационной безопасности, которые могут быть реализованы с использованием существующих недекларированных возможностей. На наш взгляд, актуальность таких угроз в первую очередь связана с оценкой потенциального ущерба и возможностями (квалификацией и техническим оснащением) потенциального нарушителя безопасности информационных систем.

Использование недекларированных возможностей программного обеспечения для получения каких-либо значимых результатов (несанкционированного доступа, уничтожения или блокирования доступа к персональным данным) весьма затратно, требует высочайшей квалификации злоумышленника и наличия специализированного аппаратного и программного обеспечения. Поэтому трудно представить, чтобы для получения несанкционированного доступа к информационной системе сельского поселения с 200 жителями привлекались специалисты уровня экспертов АНБ США или ФСБ России с использованием недекларированных (и до сих пор не обнаруженных сообществом пользователей) возможностей операционной системы Microsoft Windows 8.1.

2. Определение категории обрабатываемых персональных данных. Решение этой задачи уже было предусмотрено предыдущим этапом технологической схемы организации обработки и обеспечения безопасности персональных данных (формирование перечня персональных данных), и теперь лишь используется полученное ранее значение, закрепленное в приложении к соответствующему приказу (распоряжению) руководителя органа государственной власти или органа местного самоуправления.

3. Уточнение субъектов, персональные данные которых обрабатываются в информационных системах. В данном случае речь идёт о простом уточнении, являются ли субъекты персональных данных сотрудниками органа государственной власти или органа местного самоуправления или они не состоят с ним в трудовых отношениях.

4. Оценка объёма обрабатываемых в информационной системе персональных данных. Для данной оценки предусмотрено всего лишь два возможных решения: менее 100 тыс. субъектов персональных данных и более 100 тыс. субъектов.

5. Определение уровня защищённости персональных данных. Обобщенное представление порядка определения уровня защищённости персональных данных, установленного пунктами 9 – 12 требований, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119, представлено в таблице 2.

Таблица 2

Категории персональных данных	Категории субъектов	Количество субъектов (тыс.)	Тип актуальных угроз		
			1 тип	2 тип	3 тип
Специальные	Не сотрудники	Более 100	**УЗ 1**	**УЗ 1**	**УЗ 2**
		Менее 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
	Сотрудники	Более 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
		Менее 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
Биометрические	Не сотрудники	Более 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
		Менее 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
	Сотрудники	Более 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
		Менее 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
Иные категории	Не сотрудники	Более 100	**УЗ 1**	**УЗ 2**	**УЗ 3**
		Менее 100	**УЗ 1**	**УЗ 3**	**УЗ 4**
	Сотрудники	Более 100	**УЗ 1**	**УЗ 3**	**УЗ 4**
		Менее 100	**УЗ 1**	**УЗ 3**	**УЗ 4**
Общедоступные	Не сотрудники	Более 100	**УЗ 2**	**УЗ 2**	**УЗ 4**
		Менее 100	**УЗ 2**	**УЗ 3**	**УЗ 4**
	Сотрудники	Более 100	**УЗ 2**	**УЗ 3**	**УЗ 4**
		Менее 100	**УЗ 2**	**УЗ 3**	**УЗ 4**

В результате мы получаем оценку уровня защищённости персональных данных, для которой в соответствии с мерами, утверждёнными приказом ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», можно определить весь пакет необходимых мер обеспечения их безопасности.

Однако кроме определения уровня защищённости персональных данных, обрабатываемых в информационной системе, в соответствии с требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, предусмотрено определение класса защищённости данной информационной системы. В соответствии с названным нормативным актом последовательность действий по определению класса защищённости выглядит следующим образом.

1. Определение уровня значимости персональных данных.

В зависимости от степени возможного ущерба для обладателя информации, вследствие нарушения конфиденциальности, целостности или доступности персональных данных, определяется уровень значимости информации, обрабатываемой в анализируемой информационной системе. Названный уровень значимости может быть оценен как высокий, средний, низкий и минимальный.

Информации присваивается высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации определена высокая степень ущерба.

Информации присваивается средний уровень значимости (УЗ 2), если

хотя бы для одного из свойств безопасности информации определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информации присваивается низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации определены низкие степени ущерба.

Информации присваивается минимальный уровень значимости (УЗ 4), если обладателем информации/заказчиком и/или оператором степень ущерба от нарушения свойств безопасности информации не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

В соответствии со статьями 7 и 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» информация, содержащая персональные данные, является конфиденциальной, и операторы информационных систем обязаны принимать необходимые правовые, организационные и технические меры по её защите. Таким образом, наименьший уровень значимости информации для персональных данных не может быть ниже УЗ 4.

Попутно следует отметить, что оценка степени ущерба от нарушения свойств безопасности информации носит субъективный характер и во многом зависит от отношения к этому вопросу самого субъекта персональных данных. Так, исследования, проведённые зарубежными специалистами, показали, что далеко не все субъекты персональных данных трепетно относятся к их безопасности. Например, большинство клиентов операторов связи готовы делиться сведениями о себе, своей семье, своём текущем местонахождении и даже профилями в социальных сетях. При этом 36% клиентов готовы передавать эти сведения совершенно бесплатно, 38 – 39% готовы передавать их за некоторые эксклюзивные предложения предоставляемых услуг и программ лояльности. Если же оператор готов предложить наличные деньги (льготные тарифные планы) или же улучшенные параметры услуг связи (приоритетное обслуживание, увеличенную скорость канала связи), то число клиентов готовых предоставить свои персональные данные, в том числе и для передачи третьим лицам, вырастает от 54 – 61% до 65%[22].

Учитывая приведенные результаты исследования зарубежной аудитории, а также российскую ментальность и оставшееся пока доверие россиян к органам государственной власти и органам местного самоуправления (особенно в сельской местности) следует предостеречь от завышения уровня значимости персональных данных, поскольку это влечет за собой неоправданные затраты на создание и эксплуатацию сложной и дорогостоящей системы защиты информации. Однако данная рекомендация не означает призыва к пренебрежению мероприятиями по информационной безопасности и игнорированию установленных требований. Залогом к успеху в данной ситуации

[22] Новая валюта телекома // Computerworld Россия, 23 июля 2013 года С.25.

будет вдумчивый, обоснованный и, в то же время, творческий подход к решению стоящих задач.

2. Определение масштаба информационной системы.

Определение масштаба информационной системы осуществляется из диапазона установленных значений: федеральный, региональный и объектовый.

В соответствии с приложением 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 года № 17 информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации в пределах федерального округа и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и/или организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и/или подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и/или организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

В качестве примера следует отметить, что подавляющее большинство существующих в настоящее время информационных систем персональных данных на территории Воронежской области относится к категории объектовых.

3. Формирование оценки класса защищённости информационной системы.

Итоговая оценка класса защищённости информационной системы определяется в соответствии с таблицей 3.

Таблица 3

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Результаты всей проделанной работы по определению уровня защищённости персональных данных, обрабатываемых в информационной системе, и её классификации в соответствии с требованиями части 14.2 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17, оформляются актом

классификации, примерный образец которого для органа государственной власти приведён в приложении № 4 к настоящему пособию.

4.4. Формирование перечня должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных

Выполнение мероприятий следующего этапа технологии организации обработки и обеспечения безопасности персональных данных связано с формированием перечня должностей в органах государственной власти и органах местного самоуправления, замещение которых предусматривает осуществление обработки либо доступа к персональным данным, а также должностей ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

Юридическое закрепление сформированных перечней осуществляется в форме приказа (распоряжения) руководителя органа государственной власти или органа местного самоуправления. Необходимость выполнения данных действий установлена требованиями подпункта "б" пункта 1 «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», утверждённого постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и подпункта "в" пункта 13 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утверждённых постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119.

Исходными данными для выполнения этого этапа будут штатное расписание, штатное замещение должностей и должностные регламенты каждого из сотрудников органа государственной власти или органа местного самоуправления. На основе этих документов формирование названных выше перечней затруднений вызывать не должно.

Учитывая, что численность сотрудников органа государственной власти или органа местного самоуправления всегда ограничена, то вполне логично было бы возложить функции по обезличиванию на ответственного за организацию обработки персональных данных.

Для того, чтобы уменьшить количество нормативных актов, издаваемых в органе государственной власти или органе местного самоуправления по вопросам организации обработки и обеспечения безопасности персональных данных, полагаем возможным и целесообразным одновременно с рассматриваемыми перечнями утвердить типовую форму обязательства прекратить обработку персональных данных.

Примерный образец итогового приказа об утверждении перечня должностей сотрудников органа государственной власти, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, ответственных за проведение

мероприятий по обезличиванию обрабатываемых персональных данных и лиц, их занимающих, типовой формы обязательства прекратить обработку персональных данных приведён в приложении № 5 к настоящему пособию.

4.5. Формирование политики в отношении обработки персональных данных

Важнейшим документом, устанавливающим порядок работы с персональными данными, процедуры, направленные на выявление и предотвращение нарушений действующего законодательства в сфере персональных данных, являются правила обработки персональных данных.

Необходимость и обязательность разработки данного документа установлена подпунктом "б" пункта 1 «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», утверждённого постановлением Правительства Российской Федерации от 21 марта 2012 года № 211.

Названной нормой установлено, что правила обработки персональных данных должны:

- устанавливать процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- определять содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований для каждой цели обработки персональных данных.

Кроме приведённого перечня требований названной нормой предусмотрена разработка ещё целого ряда мероприятий и процедур обеспечения безопасности персональных данных, закрепляемых правовым актом руководителя органа государственной власти и органа местного самоуправления.

Буквальное и поверхностное толкование текста данной нормы подразумевает принятие 12 отдельных документов. Однако внимательный анализ их содержания показывает, что для значительного их числа предписываемые действия охватываются понятием «обработка персональных данных» и, следовательно, могут оформляться не самостоятельным документом, а в виде части общего документа «правил обработки персональных данных».

Рассмотрим содержание таких случаев подробнее, принимая во внимание, что в соответствии с пунктом 3 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» под обработкой персональных данных понимается любое действие (операция) или совокупность действия (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.

Правила рассмотрения запросов субъектов персональных данных или их представителей и уполномоченного органа.

В соответствии со статьёй 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» субъект персональных данных или его законный представитель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о сотрудниках, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

6) сроки обработки персональных данных, в том числе сроки их хранения.

Предоставление названных сведений раскрывает содержание работы с запросами и обращениями субъектов персональных данных или их законных представителей и по своей сути фактически является обработкой персональных данных заявителя.

Исходя из этого и с целью сокращения количества разрабатываемых документов, нам представляется возможным включить правила рассмотрения запросов субъектов персональных данных или их представителей в качестве раздела правил обработки персональных данных.

Правила работы с обезличенными данными.

В соответствии с положениями статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» под обезличиванием персональных данных понимаются «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных».

Обезличивание персональных данных – это эффективный способ обеспечения их безопасности, так как для обезличенных персональных данных не требуется обеспечение их конфиденциальности. Осуществление таких мероприятий приводит к тому, что защите будет подлежать лишь справочник, позволяющий произвести обратное преобразование обезличенной информации.

Порядок организации обезличивания персональных данных устанавливается правилами работы с обезличенными данными, основную и во многом

определяющую часть содержания которых составляют цели и используемые способы обезличивания.

Основные методы обезличивания персональных данных, обрабатываемых в информационных системах органов государственной власти и органов местного самоуправления, достаточно подробно регламентированы требованиями, утверждёнными приказом Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»[23], а их методология приведена в методических рекомендациях Роскомнадзора от 13 декабря 2013 г.[24] по применению данного приказа.

Поскольку способы обезличивания не могут быть определены без указания непосредственных действий (операций) с персональными данными, а в свою очередь регламентация действий (операций) с персональными данными охватывается понятием обработки персональных данных, следовательно, может быть оформлена в виде раздела правил обработки персональных данных. Кроме этого, прямое указание на включение обезличивания в категорию обработки персональных данных содержится в пункте 3 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Правила работы с обезличенными персональными данными в органе государственной власти или органе местного самоуправления должны в обязательном порядке определять ответственного за принятие решения о необходимости обезличивания персональных данных, а также способы их обезличивания, считаем, что это должен быть руководитель (глава) органа государственной власти или органа местного самоуправления.

В то же время сотрудник, ответственный за организацию обработки персональных данных в органе власти, готовит предложения по обезличиванию персональных данных, обрабатываемых в информационных системах, обоснованию такой необходимости и способам обезличивания.

Основными и наиболее употребительными способами обезличивания персональных данных являются:

- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- деление сведений на части и обработка в разных информационных системах.

Необходимо отметить, что введение процедуры обезличивания персональных данных инициируется только владельцем информационной системы персональных данных (в случае распределённой информационной системы – владельцем центрального узла информационной системы персональных данных), поскольку достижение необходимого результата применения процеду-

---

[23] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета, № 208, 18.09.2013

[24] Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // СПС Консультант Плюс

ры обезличивания – существенное снижение требований по защите обрабатываемых персональных данных – возможно только в случае, когда механизм обезличивания персональных данных охватывает все узлы информационной системы. В случае, если орган государственной власти или орган местного самоуправления – владелец информационной системы персональных данных – осуществляет правомерную передачу персональных данных третьей стороне, то применение процедуры обезличивания возможно только в случае внедрения аналогичного способа обезличивания у третьей стороны.

Поскольку способы обезличивания персональных данных предполагают наличие полной базы персональных данных (справочника, позволяющего выполнить обратное преобразование обезличенной информации) на одном из узлов информационной системы, для информационных систем персональных данных, состоящих из одного рабочего места, применение процедуры обезличивания является экономически нецелесообразным.

Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведётся обработка персональных данных.

Доступ в помещения, где ведётся обработка персональных данных, является одним из первых и необходимых этапов (действий) осуществления доступа к персональным данным. В свою очередь в соответствии с определением, введённым пунктом 3 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», доступ является частным случаем (формой осуществления) передачи и охватывается понятием «обработка персональных данных».

В связи с этим логично предложить оформление порядка доступа в помещения, где ведётся обработка персональных данных, в виде раздела правил обработки персональных данных.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Правила обработки персональных данных в соответствии с «Перечнем 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», утверждённого постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, утверждаются актом руководителя органа государственной власти или органа местного самоуправления.

Классическим правилом юридической техники при формировании приказов, устанавливающих какие-либо обязательные для исполнения требования, является назначение (одним из последних пунктов приказа) лиц, ответственных за осуществление контроля исполнения вводимых правил, а также определение форм, сроков и порядка докладов руководителю о результатах контроля.

Кроме этого, контроль соответствия обработки персональных данных установленным требованиям к защите персональных данных является эле-

ментом мероприятий, направленных на выявление и предотвращение нарушений законодательства в сфере персональных данных. Эти мероприятия в свою очередь в соответствии с подпунктом "б" пункта 1 «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», утверждённого постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, являются неотъемлемой частью правил обработки персональных данных.

Таким образом, правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных могут быть оформлены в виде раздела общего документа – правила обработки персональных данных.

Также необходимо обратить внимание на наличие плана проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, который ежегодно утверждается руководителем (главой) органа государственной власти или органа местного самоуправления.

С целью обеспечения выполнения требований пункта 5 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и пункта 13 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утверждённых постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, в каждом органе государственной власти или органе местного самоуправления разрабатывается регламент учёта, хранения и уничтожения машинных носителей персональных данных (далее – Регламент).

Данный Регламент определяет и содержит достаточно подробный порядок учёта, хранения и уничтожения машинных носителей персональных данных, а также ответственное лицо за его исполнение. Рекомендуем обязанности по учёту и хранению машинных носителей персональных данных возложить на ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

Отметим, что в органе государственной власти или органе местного самоуправления должны быть созданы надлежащие условия, обеспечивающие физическую сохранность машинных носителей персональных данных с возможностью их хранения в надёжно запираемых шкафах (сейфах).

Все машинные носители информации (стационарные и внешние жёсткие диски, флеш-накопители, оптические диски и т.д.), используемые для хранения, обработки и (или) передачи персональных данных, подлежат обязательному учёту. Учёт носителей информации осуществляется перед записью на них персональных данных ответственным лицом в журнале с проставлением на носителях регистрационных данных.

Журнал учёта машинных носителей персональных данных вносится в номенклатуру дел и журналов органа государственной власти или органа

местного самоуправления с постановкой на инвентарный учёт. Листы журнала нумеруются, прошиваются и опечатываются. Форма журнала приведена в приложении № 6 к настоящему пособию.

Машинные носители персональных данных могут выдаваться только сотрудникам, допущенным к обработке персональных данных под личную роспись. Допускается пересылка машинных носителей персональных данных в сторонние организации с сопроводительным письмом заказным почтовым отправлением.

Следует обратить внимание на то, что в соответствии с требованиями, утверждёнными приказом ФСТЭК России от 11 февраля 2013 года № 17, при выводе из эксплуатации машинных носителей персональных данных осуществляется физическое уничтожение этих машинных носителей информации. Строгое выполнение данного требования фактически не допускает даже возможности какого-либо ремонта повреждённых машинных носителей информации. В соответствии с пунктом 19.2 названных выше требований перед передачей машинного носителя информации в сторонние организации для ремонта или технического обслуживания вся информация и остаточные данные с него должны быть уничтожены. Однако выполнить гарантированное уничтожение информации на технически неисправном машинном носителе, как правило, не представляется возможным. В связи с этим единственным вариантом вывода машинного носителя персональных данных из эксплуатации является его физическое уничтожение с оформлением соответствующего акта.

Контроль за соблюдением порядка учёта, хранения и уничтожения машинных носителей персональных данных осуществляет сотрудник, ответственный за организацию обработки персональных данных в органе власти в рамках внутреннего контроля соответствия обработки персональных данных, установленным требованиям к защите персональных данных в органе власти.

Примерный образец приказа об утверждении правил обработки персональных данных и регламента учёта, хранения и уничтожения машинных носителей персональных данных в органе государственной власти приведен в приложении № 6 к настоящему пособию.

4.6. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Правовым основанием разработки модели угроз безопасности персональных данных является пункт 1 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и пункт 14 требований, утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приведённые нормы прямо предусматривают наличие отдельного документа – модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных (далее – Модель угроз),

однако детальных требований к его структуре и содержанию не устанавливают.

Важную роль в составе Модели угроз играет описание состава, структуры, особенностей построения и эксплуатации информационных систем персональных данных в органах государственной власти и органах местного самоуправления, поскольку на основании этих данных формируется перечень актуальных угроз безопасности персональных данных. Неправильное указание характеристик информационных систем или параметров их эксплуатации может привести либо к значительному перерасходу средств выделяемых на организацию защиты персональных данных, либо приведёт к формированию облика системы защиты, не отвечающей всем необходимым требованиям.

Особое внимание в рамках описания информационных систем следует уделить установленной системе разграничения доступа сотрудников к компьютерам, их операционным системам и непосредственно самим информационным системам. Если мы определим, что все сотрудники имеют права администраторов (т.е. могут изменять конфигурацию технических средств, устанавливать/удалять любое программное обеспечение), то в такой ситуации построить адекватную систему защиты персональных данных будет либо вообще невозможно, либо построение системы защиты потребует существенных материальных затрат.

Вместе с тем, применение организационных мер, обеспечивающих возложение обязанностей администратора информационных систем на одного из сотрудников и наделение всех остальных только правами пользователей, сильно меняет дело. Правда, в этой ситуации с позиции обычной логики трудно объяснить, почему, например, права доступа к ресурсам информационной системы у главы сельского поселения будут меньше, чем у назначенного им же специалиста (системного администратора).

Методической основой построения подобной модели является Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных[25] (далее – Базовая модель) и Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных[26] (далее – Методика определения актуальных угроз) разработанные ФСТЭК России, а также требования, установленные ФСБ России[27]

---

[25] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК 15 февраля 2008 года // http://fstec.ru/component/attachments/download/289 (дата обращения 30.03.2014).

[26] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК 14 февраля 2008 года // http://fstec.ru/component/attachments/download/290 (дата обращения 30.03.2014).

[27] Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 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 выпол-

При этом требования ФСБ России ориентированы на случаи использования криптографической защиты информации. Для защиты персональных данных такие средства используются не всегда, поэтому Модель угроз зачастую может строиться с использованием только документов ФСТЭК России.

Базовая модель содержит типовые модели угроз для различных объектов информатизации, типизированных в зависимости от количества рабочих мест (автономное рабочее место, локальная компьютерная сеть, распределенная компьютерная сеть) и степени их информационной открытости (с выходом в сети общего пользования и (или) сеть Интернет или без такового).

Таким образом, определив по предложенным критериям вид объекта информатизации, создаваемого в органе государственной власти или органе местного самоуправления, мы получаем перечень всех угроз, которые необходимо рассматривать при создании его системы защиты информации.

При этом следует помнить, что далеко не все угрозы из приведённого в Базовой модели перечня являются актуальными для конкретных условий эксплуатации рассматриваемой информационной системы персональных данных. Все выявленные на основании Базовой модели угрозы должны пройти оценку их актуальности на основании Методики определения актуальных угроз. Результатом этой работы будет перечень только актуальных угроз, которые в дальнейшем используются в качестве исходных данных для формирования облика системы защиты информации для рассматриваемой информационной системы персональных данных.

Возможность реализации той или иной угрозы оценивается в зависимости от уровня исходной защищённости информационной системы и вероятности[28] реализации каждой из выявленных на предыдущем этапе угроз.

Уровень исходной защищённости определяется исходя из технических и эксплуатационных характеристик информационной системы в соответствии со схемой, представленной в таблице 4. При этом каждому значению характеристики присваивается числовой коэффициент Y_1 равный 0 – для значения уровня защищённости «высокий», 5 – для значения уровня защищённости «средний» и 10 – для значения уровня защищённости «низкий».

нения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

[28] Для характеристики возможности реализации каждой из угроз в тексте Методики определения актуальных угроз использована такая категория как «частота (вероятность)». Внимательное рассмотрение показывает, что, скорее всего, авторы Методики определения актуальных угроз имели в виду не «частоту», а «частость», поскольку в теории вероятности вероятность наступления произвольного события определяется как частость наступления этого события в бесконечной (достаточно длинной) серии испытаний. Учитывая, что категория «частость» в основном применяется в математической статистике, где исследуются закономерности наступающих событий в серии экспериментов, то в нашем случае (предварительной работы без проведения каких-либо испытаний) оценки защищенности информационных систем персональных данных, речь можно вести только о категории «вероятность».

Таблица 4

Технические и эксплуатационные характеристики	Уровень защищённости		
	Высокий (0 баллов)	Средний (5 баллов)	Низкий (10 баллов)
1. По территориальному размещению			
Распределённая информационная система, которая охватывает несколько областей, краев, округов или государство в целом	–	–	✓
Городская информационная система, охватывающая не более одного населенного пункта (города, поселка)	–	–	✓
Корпоративная распределённая информационная система, охватывающая многие подразделения одной организации	–	✓	–
Локальная (кампусная) информационная система, развёрнутая в пределах нескольких близко расположенных зданий	–	✓	–
Локальная информационная система, развёрнутая в пределах одного здания	✓	–	–
2. По наличию соединения с сетями общего пользования			
Информационная система, имеющая многоточечный выход в сеть общего пользования	–	–	✓
Информационная система, имеющая одноточечный выход в сеть общего пользования	–	✓	–
Информационная система, физически отделённая от сети общего пользования	✓	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных			
Чтение, поиск	✓	–	–
Запись, удаление, сортировка	–	✓	–
Модификация, передача	–	–	✓
4. По разграничению доступа к персональным данным			
Информационная система, к которой имеют доступ определённые перечнем сотрудники организации, являющейся её владельцем, либо субъект персональных данных	–	✓	–
Информационная система, к которой имеют доступ все сотрудники организации, являющейся её владельцем	–	–	✓
Информационная система с открытым доступом	–	–	✓
5. По наличию соединений с другими базами персональных данных иных информационных систем			
Интегрированная информационная система персональных данных (организация использует несколько баз персональных данных в информационных системах, при этом организация не является владельцем всех используемых баз);	–	–	✓
Информационная система, в которой используется одна база персональных данных, принадлежащая организации – владельцу данной информационной системы	✓	–	–

Технические и эксплуатационные характеристики	Уровень защищённости		
	Высокий (0 баллов)	Средний (5 баллов)	Низкий (10 баллов)
6. По уровню обобщения (обезличивания) персональных данных			
Информационная система персональных данных, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	✓	–	–
Информационная система персональных данных, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–	✓	–
Информационная система персональных данных, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных)	–	–	✓
7. По объему персональных данных, которые предоставляются сторонним пользователям информационных систем без предварительной обработки			
Информационная система, предоставляющая всю базу данных с персональными данными	–	–	✓
Информационная система, предоставляющая часть персональных данных	–	✓	–
Информационная система, не предоставляющая никакой информации	✓	–	–

Поученные качественные оценки уровня защищённости сворачиваются в значения «высокий», «средний» и «низкий».

Установлено, что информационная система персональных данных имеет **высокий уровень** защищённости, если не менее 70% (т.е. не менее 14 значений «✓») характеристик имеют значение «высокий», а остальные «✓» (6 или менее значений) размещены в столбце «средний». Соответственно, в столбце «низкий» не должно быть ни одного значения.

Информационная система персональных данных имеет **средний уровень** защищённости, если предыдущие условия не выполняются и при этом не менее 70% характеристик соответствуют уровню не ниже «средний» (т.е. не менее 14 значений «✓» размещено за пределами столбца «низкий»).

Если оба приведённые выше условия не выполняются, то считается, что информационная система персональных данных имеет **низкий уровень** защищённости.

Вероятность реализации каждой угрозы определяется экспертным путём, исходя из особенностей конкретной информационной системы персональных данных в складывающихся условиях её эксплуатации. Для количественной оценки вероятности реализации угрозы вводятся четыре вербальных градации, которым устанавливаются числовые значения коэффициента Y_2:

- **маловероятно** (0 баллов) – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информа-

ции лицами, не имеющими легального доступа в помещение, где последние хранятся);

- **низкая вероятность** (2 балла) – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (например, использованы соответствующие средства защиты информации);
- **средняя вероятность** (5 баллов) – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности персональных данных недостаточны;
- **высокая вероятность** (10 баллов) – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности персональных данных не приняты.

Таким образом, итоговый коэффициент реализуемости конкретной угрозы будет определяться по формуле:

$$Y = (Y_1 + Y_2)/20.$$

На основании полученного числового значения коэффициента Y формируется его вербальная интерпретация. Возможность реализации угрозы признается:

- **низкой**, если $0 \leq Y \leq 0{,}3$;
- **средней**, если $0{,}3 < Y \leq 0{,}6$;
- **высокой**, если $0{,}6 < Y \leq 0{,}8$;
- **очень высокой**, если $Y > 0{,}8$.

Далее экспертным путём определяется показатель опасности каждой из выявленных угроз. В соответствии с Методикой определения актуальных угроз этот показатель имеет три значения:

- **низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- **средняя опасность** – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- **высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Итоговое решение о признании той или иной угрозы актуальной принимается по схеме, представленной в таблице 5.

Таблица 5

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	Актуальная	актуальная	актуальная
Очень высокая	Актуальная	актуальная	актуальная

Повторяя рассмотренную процедуру для каждой из угроз, представленных в исходном перечне, полученном на основе Базовой модели, формируется перечень только актуальных угроз для рассматриваемой нами конкретной информационной системы персональных данных в конкретных условиях её эксплуатации. Полученный итоговый перечень образует набор исходных данных для определения рационального облика системы защиты персональных данных, обрабатываемых в информационных системах органов государственной власти и органов местного самоуправления.

Сформированный описанным выше способом перечень актуальных угроз и набор всех промежуточных сведений, приводящий к получению итогового результата, образуют Модель угроз для конкретной информационной системы.

При необходимости применения требований, утверждённых приказом ФСБ России от 10 июня 2014 года № 378, орган власти формирует совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учётом типа актуальных угроз требуемого класса средств криптографической защиты информации (СКЗИ). Под этой замысловатой формулировкой скрывается построение ничего иного как модели нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных (далее – Модель нарушителя).

Порядок и структура построения данной модели регулятором не определены. В рамках данного пособия предлагается построение Модели нарушителя осуществлять в составе Модели угроз в качестве отдельного раздела, в котором описываются меры, содержащие СКЗИ и применяемые для нейтрализации атак, и, соответственно, актуальность данных атак.

В зависимости от уровня защищенности и типа актуальных угроз в требованиях, утвержденных приказом ФСБ России от 10 июня 2014 года № 378, установлены минимальные классы СКЗИ (таблица 6).

Таблица 6

Уровень защищенности ПДн	**4 УЗ**		**3 УЗ**		**2 УЗ**		**1 УЗ**	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

С учётом установленного минимального класса СКЗИ и на основании определённых актуальных атак, вероятность реализации которых определя-

ется экспертным путём, исходя из особенностей конкретной информационной системы персональных данных, орган власти определяет требуемый класс СКЗИ, необходимый для нейтрализации данных атак.

Пример реализации рассмотренной выше технологии и разработанной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных с учётом построения Модели нарушителя на примере информационной системы органа местного самоуправления приведён в приложении № 7 к настоящему пособию.

Завершая рассмотрение данного этапа технологии организации обработки и обеспечения безопасности персональных данных, следует отметить, что в соответствии с рекомендациями Методики определения актуальных угроз опасность каждой из них, как и вероятность её реализации, оценивается исключительно экспертным путём. При этом, каких-либо требований к уровню подготовки, квалификации, наличию практического опыта экспертов, а также их количеству (при рекомендуемом проведении опроса) не предъявляется. Учитывая этот факт, а также реальные финансовые и организационные возможности органов местного самоуправления сельских поселений и муниципальных районов по привлечению внешних специалистов в области информационной безопасности, с высокой долей уверенности можно считать, что в роли основных экспертов по информационной безопасности, будут выступать сами муниципальные и государственные служащие, ответственные за организацию обработки и обеспечение безопасности персональных данных, обрабатываемых в информационных системах.

В этих условиях значительно возрастает роль обучения и постоянного повышения квалификации государственных и муниципальных служащих в сфере информационной безопасности и защиты персональных данных.

4.7. Формирование облика и внедрение системы защиты персональных данных в информационных системах персональных данных

Нормативной основой формирования системы защиты информации в информационных системах персональных данных является 13 пункт «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17, устанавливающий, что для обеспечения защиты информации (в том числе персональных данных), содержащейся в информационной системе, должны проводиться мероприятия, связанные с формированием требований к защите информации, разработкой и внедрением системы защиты информационной системы. Каждое из названных мероприятий относительно подробно урегулировано в пунктах 14 – 16 названных выше требований ФСТЭК России.

Основные сложности этого этапа связаны с отсутствием необходимой нормативной базы и методической нестыковкой подходов февральских приказов ФСТЭК России 2013 года, с одной стороны, и содержанием Базовой

модели угроз безопасности персональных данных при их обработке в информационных системах, с другой стороны.

В соответствии с названными приказами ФСТЭК России облик системы защиты персональных данных в органах государственной власти и органах местного самоуправления должен формироваться на основе определённых в соответствии с установленной методикой уровней защищённости персональных данных (классов защищённости информационной системы). При этом полученные оценки уровней/классов, в основном, зависят от свойств и характеристик информационных систем персональных данных и абсолютно не учитывают типы, возможности, а также техническое оснащение наиболее вероятных нарушителей информационной безопасности.

В связи с этим строгой юридически обоснованной и нормативно закрепленной необходимости использования результатов построения частной модели угроз безопасности персональных данных в конкретных информационных системах с учётом их назначения, условий и особенностей функционирования на сегодняшний день нет.

Поэтому, формально следуя принципам февральских приказов ФСТЭК России, определив уровень защищённости персональных данных (класс защищённости информационной системы), мы получим необходимый набор организационных и технических мер по обеспечению безопасности персональных данных в информационной системе.

Все эти меры, объединённые в рамках системы защиты информации, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищённости информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, её средств, систем связи и передачи данных.

Практически каждая из перечисленных мер (или даже целая их совокупность) реализуется благодаря использованию какого-либо технического (аппаратного) программного или программно-аппаратного средства защиты информации. В соответствии с принятой терминологией средство защиты информации определяется как техническое, программное средство, вещество

и/или материал, предназначенные или используемые для защиты информации[29].

Согласно пунктам 19 и 22 «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378, для обеспечения 2-го и выше уровня защищённости персональных данных при их обработке в информационных системах в соответствии с требованиями «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378:

- утвержден список лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;
- информационные системы обеспечены автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;
- информационные системы имеют в своем составе автоматизированные средства, исключающие доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем списке лиц, допущенных к содержанию электронного журнала сообщений.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах в соответствии с требованиями «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378, информационные системы обеспечены автоматизированными средствами, позволяющими автоматически реги-

[29] Средство защиты информации. Национальный стандарт Российской Федерации. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения – Москва. Стандартинформ, 2006.

стрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.

Согласно положениям пункта 4 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и пункта 13 требований, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для обеспечения безопасности персональных данных в информационных системах применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия.

На основании пункта 11 требований, утверждённых приказом от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», применяемые средства защиты информации проходят оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Сертификацию средств защиты информации осуществляют федеральные органы по сертификации – ФСТЭК России и ФСБ России.

Список сертифицированных ФСТЭК России средств защиты информации доступен в Государственном реестре сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 на сайте ФСТЭК России[30].

Образец сертификата соответствия средства защиты информации ФСТЭК России приведен в приложении № 8 к настоящему пособию.

Список сертифицированных ФСБ России средств защиты информации доступен на официальном сайте[31]. Образец сертификата соответствия средства защиты информации ФСБ России приведен в приложении № 9 к настоящему пособию.

Большинство современных средств защиты информации представляют достаточно сложные программно-аппаратные системы, которые позволяют реализовать широкий спектр необходимых мероприятий и установленных мер. Если какое-то из необходимых мероприятий оказывается нереализованным в рамках использования одного выбранного средства защиты информации, то подбирается второе (при необходимости – третье и т.п.), обеспечивающее полное выполнение комплекса мер, соответствующих установленному

---

[30] ФСТЭК России. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 // http://fstec.ru/component/attachments/download/489 (дата обращения 30.03.2014).

[31] Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. Перечень средств защиты информации, сертифицированных ФСБ России // http://clsz.fsb.ru/certification.htm (дата обращения 30.03.2014).

уровню защищенности персональных данных (классу защищённости информационной системы).

Теоретически в рамках подобного подхода возможна постановка оптимизационной задачи выбора оптимального по соответствующему критерию (стоимости, наименьшей дополнительной нагрузки на вычислительную систему, простоте эксплуатации и т.п.) комплекса средств защиты. Однако на практике из-за реально сложившейся ситуации на рынке средств защиты всё достаточно просто и может быть решено простым перебором двух-трёх доступных вариантов.

Хотя и здесь есть серьёзные подводные камни. Например, ни в одном из описаний средств защиты информации[32] мы не найдём указаний на то, что то или иное средство защиты позволяет обеспечить реализацию таких-то и таких-то мер по обеспечению безопасности персональных данных. Более того, большинство сертификатов ФСТЭК России, выданных на средства защиты информации, в своем описании содержат формулировку – «может использоваться в автоматизированных системах до класса … включительно и в информационных системах персональных данных до … класса включительно».

Разницу между «**обеспечивает реализацию** мер по обеспечению безопасности, предусмотренную … классом защищенности информационной системы» и «**может использоваться** в автоматизированных системах до класса …» чувствуете? В любом случае, что бы не приобрёл и не установил у себя на компьютере оператор информационной системы персональных данных (подразумевая, что все он сделал идеально правильно), юридической гарантии, что он реализовал все требуемые меры, нет. Причем такой гарантии не может быть даже теоретически, поскольку количественных критериев или даже метрик близости имеющегося состояния уровня безопасности от требуемого в пространстве признаков в котором функционируют средства защиты информации насколько нам известно не существует[33].

В таком случае, как же сегодня в органах государственной власти и органах местного самоуправления на практике решается задача формирования рационального облика средств защиты персональных данных для конкретной информационной системы? Выясняется, что все очень просто, и необходимое решение лежит вне плоскости технических проблем. Всего лишь надо пригласить для решения требуемой задачи внешнюю организацию, обладающую соответствующей лицензией контролирующего органа. Тогда при проверке можно будет предъявить копию соответствующей лицензии организации-разработчика системы защиты персональных данных и комплект документов, подтверждающих, что именно она выполняла все необходимые работы. Ар-

---

[32] Например, СЗИ от НСД Secret Net // http://www.securitycode.ru/products/secret_net/sertificates/ (дата обращения 30.03.2014); Система защиты информации от несанкционированного доступа Dallas Lock // http://www.dallaslock.ru/sertifikaty-i-liczenzii.html (дата обращения 30.03.2014).

[33] По крайней мере внимательный анализ доступной специальной литературы и источников в сети Интернет, а также расспросы специалистов в данной сфере не позволил выявить даже косвенные следы их существования.

гумент «железобетонный»: систему защиты создавали сведущие люди (наличие лицензии это подтверждает), они знали, почему все надо сделать так, а не иначе.

При этом методики проверки качества решения задачи создания системы защиты персональных данных для конкретного заказчика с учётом особенностей его информационных систем и условий эксплуатации не существует. Хотя следует сразу же оговориться, что речь не идёт об оценке эффективности защиты персональных данных от утечки по побочным электромагнитным излучениям (ПЭМИН). В случае с ПЭМИН мы имеем дело с классической радиофизикой, и здесь все понятно. Иное дело – оценка эффективности защиты персональных данных от несанкционированного доступа.

Вместе с тем, отступая от сухого формального следования букве нормативного правового акта и сложившейся сомнительной практики, мы понимаем, что наличие разработанной модели угроз безопасности персональных данных обрабатываемых в конкретной информационной системе в конкретном органе государственной власти или органе местного самоуправления позволяет нам сузить (в отдельных случаях весьма значительно) перечень необходимых мер по обеспечению безопасности персональных данных. Как следствие, экономия всех выделяемых на решение задач обеспечения информационной безопасности персональных данных ресурсов: финансовых, вычислительных, организационных.

Например, в соответствии с требованиями ФСТЭК России необходимые меры обеспечения безопасности, связанные с защитой среды виртуализации, предусмотрены абсолютно для всех уровней защищённости персональных данных. Их реализация требует использования определённых средств защиты, которые стоят денег и используют вычислительные ресурсы компьютера, на котором развернута информационная система персональных данных.

Однако в муниципальных образованиях сельских поселений, как правило, среда виртуализации не используется. В этом случае логично было бы использовать результаты построения Модели угроз для соответствующего «прореживания» используемых мер обеспечения безопасности персональных данных.

С этой целью предлагается разработанная нами матрица соответствия мер по обеспечению безопасности персональных данных, приведенных в требованиях, утверждённых 17 и 21 приказами ФСТЭК России 2013 года, угрозам безопасности персональных данных при их обработке в информационных системах персональных данных из Базовой модели (далее – Матрица соответствия). Матрица соответствия приведена в приложении № 10 к настоящему пособию.

Опираясь на построенную Матрицу соответствия, органы государственной власти и органы местного самоуправления имеют возможность в конечном итоге выполнять только те меры по обеспечению безопасности персональных данных, которые соответствуют актуальным угрозам их безопасности согласно разработанной Модели угроз.

Подобная логика рассуждений давно обсуждается в среде специалистов по информационной безопасности и нашла свое отражение в методическом документе «Меры защиты информации в государственных информационных системах ФСТЭК России»[34]. В соответствии с методическим документом класс защищённости информационной системы определяет только «базовый набор» мер защиты информации. Учёт структурно-функциональных характеристик информационной системы, информационной технологии и особенностей их функционирования позволяет сформировать «адаптированный базовый набор» мер защиты информации. Учёт угроз безопасности информации, включенных в Модель угроз, определит «уточнённый адаптированный базовый набор» мер защиты информации. И, наконец, необходимость учёта требований иных (в том числе ведомственных и локальных) нормативных актов по вопросам обеспечения информационной безопасности персональных данных позволит сформировать «дополнительный уточнённый адаптированный базовый набор» мер защиты информации.

При этом совсем не обязательно, что полученный в конце всей работы набор мер защиты информации будет меньше по объёму, чем базовый.

Однако, даже принимая во внимание рекомендации о привлечении внешнего квалифицированного исполнителя для формирования облика системы защиты персональных данных, руководитель (глава) органа государственной власти или органа местного самоуправления, а также сотрудники, ответственные за организацию обработки и обеспечение безопасности персональных данных в информационных системах, выполняя роль заказчика разрабатываемой системы, должны знать, какие работы должны проводиться и какие измеримые результаты будут получаться в итоге проделанной работы.

В ряде случаев, когда мы сталкиваемся с уже существующей и давно использующейся в практической деятельности информационной системой персональных данных, то вместо названных выше технических заданий могут быть разработаны требования к системе защиты персональных данных в информационной системе органа государственной власти или органа местного самоуправления.

Пример таких требований к системе защиты персональных данных информационной системы с уровнем защищённости персональных данных – 4 и классом защищённости – К4 приведён в приложении № 11 к настоящему пособию.

Выработанные требования к системе защиты персональных данных информационной системы содержат набор организационных и технических мер, реализуемых с применением сертифицированных средств защиты информации.

---

[34] Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 года // http://fstec.ru/component/attachments/download/675 (дата обращения 30.03.2014).

4.8. Оценка эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных

Правовым основанием проведения работ по оценке эффективности реализуемых мер защиты информации в информационных системах персональных данных являются положения пункта 4 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и пункта 13 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17, в котором указано, что информационная система (в том числе и персональных данных) подлежит аттестации по требованиям защиты информации.

Содержанием данной деятельности является анализ особенностей обработки и обеспечения безопасности персональных данных в информационной системе, проведение комплекса внутренних организационных и технических мероприятий (испытаний) реализованной системы защиты информации на соответствие установленным требованиям в области безопасности персональных данных в соответствии с утверждённой программой и методикой аттестационных испытаний информационной системы.

В соответствии с частью 5 пункта 1 статьи 12 Федерального закона от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности» данная деятельность осуществляется только лицензиатами (организациями, имеющими лицензию на соответствующую деятельность) лицензирующего органа (ФСТЭК России).

Выдаваемые лицензии содержат следующие основные сведения:

- наименование лицензирующего органа;
- наименование организации-лицензиата, адрес места нахождения;
- регистрационный номер, дата выдачи и срок действия;
- перечень видов работ и услуг, на которые она распространяется.

Согласно постановлению Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» перечень видов работ и услуг в сфере технической защиты конфиденциальной информации, лицензируемых ФСТЭК России, включает:

- контроль защищённости конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;
- технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещённых в помещениях, где она обрабатывается, помещениях со средствами (системами), подлежащими защите, помещениях, предназначенных для ведения конфиденциальных переговоров;

- контроль защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации;
- сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищённых технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищённых программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищённости информации);
- аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений;
- проектирование в защищённом исполнении средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений;
- установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищённых программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищённости информации).

Реестр лицензий, выданных ФСТЭК России предприятиям и организациям на деятельность по технической защите конфиденциальной информации, доступен в сети Интернет[35]. Поэтому начиная обсуждать вопрос об оценке эффективности реализуемых мер по защите персональных данных, всегда можно проверить обладает ли потенциальный исполнитель работ необходимой квалификацией и лицензией в данной сфере деятельности.

В связи с тем, что при получении лицензий ФСТЭК России каждая из организаций самостоятельно выбирает свой перечень лицензируемой деятельности, далеко не все организации, получившие лицензию, обладают необходимым набором полномочий для решения задач аттестации информационных систем персональных данных в органах государственной власти и органах местного самоуправления.

[35] ФСТЭК России. Реестр лицензий на деятельность по технической защите конфиденциальной информации // http://fstec.ru/component/attachments/download/138 (дата обращения 16.05.2016).

В нашем случае организация (лицензиат ФСТЭК России) – потенциальный исполнитель работ по проведению аттестации информационной системы персональных данных по требованиям защиты информации обязательно должна иметь лицензию на деятельность по технической защите конфиденциальной информации, включающую следующие виды работ и услуг:

- контроль защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации;
- аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации.

Образец лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации приведён в приложении № 12 к настоящему пособию.

В качестве исходных данных, необходимых для проведения аттестации информационной системы персональных данных в органе государственной власти или органе местного самоуправления, используются:

- перечень технических и программных средств информационной системы;
- акт классификации информационной системы;
- модель угроз безопасности персональных данных, обрабатываемых в информационной системе;
- требования к системе защиты информации информационной системы;
- техническое задание на создание информационной системы (для вновь создаваемых информационных систем) или техническое задание на создание системы защиты информации информационной системы;
- эксплуатационная документация и сертификаты соответствия по требованиям безопасности информации на применяемые средства защиты информации информационной системы;
- акты установки средств защиты информации информационной системы;
- организационно-распорядительные документы, регламентирующие обработку и обеспечение безопасности персональных данных;
- иные документы, разрабатываемые в органах государственной власти и органах местного самоуправления в соответствии с требованиями действующего законодательства.

Непосредственное осуществление аттестационных испытаний информационной системы персональных данных включает следующую совокупность действий:

- предварительное ознакомление с составом, структурой и организацией эксплуатации информационной системы;

- проверку правильности классификации информационной системы;
- проверку информационной системы на соответствие организационно-техническим требованиям по защите информации;
- проведение испытаний информационной системы на соответствие требованиям по защите информации от несанкционированного доступа;
- проведение комплексных испытаний с целью оценки соответствия реализуемых мер и средств защиты требуемому уровню безопасности информации;
- подготовку отчётной документации и оценка результатов испытаний информационной системы.

После проведения аттестационных испытаний готовится целый пакет документов, основными из которых являются «Протокол аттестационных испытаний информационной системы персональных данных» и «Заключение по результатам аттестационных испытаний информационной системы персональных данных».

Протокол аттестационных испытаний информационной системы персональных данных должен содержать:

- наименование аттестуемой информационной системы и дату проведения испытаний;
- цель испытаний;
- перечень используемых нормативных документов и методик испытаний;
- результаты испытаний.

На основании полученных данных разрабатывается заключение по результатам аттестационных испытаний информационной системы персональных данных, включающее:

- оценку соответствия информационной системы установленным требованиям в области безопасности персональных данных;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности (невозможности) выдачи аттестата соответствия требованиям по безопасности информации.

На основании названного протокола и заключения организацией-лицензиатом принимается решение о выдаче аттестата соответствия требованиям по безопасности информации, в котором отражается:

- наименование организации-лицензиата;
- номер, дата выдачи и срок действия лицензии ФСТЭК России на осуществление технической защиты конфиденциальной информации;
- наименование информационной системы, адрес её размещения;
- класс информационной системы;

- состав технических средств информационной системы;
- состав средств защиты информации информационной системы;
- планы размещения технических средств, схемы прокладки линий и коммуникаций информационной системы.

В соответствии с установленными требованиями ФСТЭК России максимальный срок действия аттестата соответствия составляет – три года. В течение этого срока должна быть обеспечена неизменность условий функционирования информационной системы, состава её технических средств и технологии обработки персональных данных, которые могут повлиять на характеристики их защищённости.

По истечении срока действия аттестата соответствия или при нарушении исходных характеристик защищённости информационная система персональных данных подлежит обязательной переаттестации. В противном случае обработка персональных данных в информационной системе запрещается и она выводится из эксплуатации.

В соответствии с положениями пункта 17.3 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17, допускается аттестация всей информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации. При этом распространение аттестата соответствия на другие сегменты информационной системы осуществляется при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания.

Сегмент считается соответствующим сегменту информационной системы, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищённости, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и её системе защиты информации.

Такой подход целесообразно применять для информационных систем персональных данных, состоящих из большого количества (5 и более) однотипных узлов (наборов технических средств, автоматизированных рабочих мест) и использующих единый технологический процесс для обработки персональных данных, что позволяет существенно снизить затраты на проведение аттестационных испытаний такой информационной системы.

Поскольку аттестационные испытания по требованиям защиты информации выполняются, как правило, на договорной основе и занимают достаточно длительный промежуток времени (2-3 месяца), то проведение всех необходимых работ нужно инициировать заранее.

После получения аттестата соответствия информационная система персональных данных вводится в эксплуатацию. Пример распоряжения о вводе в эксплуатацию информационных систем персональных данных в органе местного самоуправления приведен в приложении № 13 к настоящему пособию.

4.9. Уведомление территориального органа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

Правовым основанием данного этапа технологии организации обработки и обеспечения безопасности персональных данных в органах государственной власти и органах местного самоуправления является часть 1 статьи 22 Федерального закона от 27 июля 2006 года № 52-ФЗ «О персональных данных».

В соответствии с названными законодательными требованиями оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Пунктом 1 «Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций», утверждённого постановлением Правительства Российской Федерации от 16 марта 2009 года № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»,[36] в качестве такого органа определена Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Названным выше федеральным законом определены случаи, когда оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных. К числу таких случаев отнесена обработка персональных данных:

1) осуществляемая в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

---

[36] Постановление Правительства Российской Федерации от 16 марта 2009 года № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства Российской Федерации, 23.03.2009, № 12, Ст. 1431.

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Все иные случаи предусматривают обязательное уведомление уполномоченного органа по защите прав субъектов персональных данных.

Требования к форме и содержанию уведомления определены в части 3 статьи 22 Федерального закона от 27 июля 2006 года № 52-ФЗ «О персональных данных», а также детализированы в приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19 августа 2011 года № 706 «Об утверждении рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных» и приложении № 2 к административному регламенту Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»[37], утвержденному приказом Министерства связи и массовых коммуникаций Российской Федерации от 21 декабря 2011 года № 346.

В соответствии с названными актами уведомление направляется на бумажном носителе или в форме электронного документа в территориальный орган Роскомнадзора по месту нахождения оператора. Вся необходимая контактная информация территориальных органов приведена на сайте www.rsoc.ru.

Есть возможность заполнения уведомления на сайте Роскомнадзора по адресу: http://pd.rkn.gov.ru/operators-registry/notification/form/, после чего за-

[37] Приказ Министерства связи и массовых коммуникаций Российской Федерации от 21 декабря 2011 года № 346 (зарегистрирован в Минюсте России от 29 марта 2012 года № 23650) // Бюллетень нормативных актов федеральных органов исполнительной власти, № 24, 11.06.2012.

полненную форму необходимо распечатать, подписать и направить в территориальный орган Роскомнадзора.

Непредставление уведомления об обработке персональных данных или его несвоевременное представление либо представление уведомления, содержащего неполные или недостоверные сведения, образует состав административного правонарушения, предусмотренного статьёй 19.7 Кодекса об административных правонарушениях Российской Федерации. За данное правонарушение установлена ответственность в виде предупреждения или штрафа в размере от 300 до 500 рублей для должностных лиц и от 3000 до 5000 рублей для юридических лиц.

Пример заполнения уведомления территориального органа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций об обработке (о намерении осуществлять обработку) персональных данных органа государственной власти приведён в приложении № 14 к настоящему пособию.

В соответствии с требованиями части 4 статьи 22 Федерального закона от 27 июля 2006 года № 52-ФЗ «О персональных данных» территориальный орган Роскомнадзора в 30-дневный срок с даты поступления уведомления (15-дневный с момента регистрации уведомления – в соответствии с административным регламентом Роскомнадзора по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»), вносит сведения об операторе, осуществляющем обработку персональных данных, в реестр. Данной записи на основании приказа руководителя территориального органа Роскомнадзора присваивается регистрационный номер, и в срок не позднее 3 дней со дня подписания приказа информация о внесении в реестр сведений об операторе размещается на официальном сайте Роскомнадзора по адресу: http://pd.rkn.gov.ru/operators-registry/operators-list/.

Данные сведения (кроме информации о средствах защиты и предпринимаемых мерах по обеспечению безопасности персональных данных) являются общедоступными и могут быть предоставлены любому заинтересованному лицу по его запросу.

Пример заявления о предоставлении выписки из реестра операторов, разработанный в соответствии с административным регламентом Роскомнадзора по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», приведён в приложении № 15 к настоящему пособию.

Данное заявление может быть направлено как в бумажной форме по почте, так и в электронной форме через Единый портал государственных услуг (www.gosuslugi.ru).

В системе органов государственной власти и органов местного самоуправления достаточно часто происходят структурные и организационные изменения, поэтому вполне вероятна ситуация, когда сведения, размещенные в реестре, перестанут соответствовать реальному положению дел. В таких

случаях может возникнуть необходимость в уточнении сведений, внесённых в соответствующий реестр Роскомнадзора.

В случае изменения сведений, содержащихся в реестре, органы государственной власти и органы местного самоуправления обязаны уведомить территориальный орган Роскомнадзора в течение 10 рабочих дней. Форма информационного письма практически совпадает с уведомлением об обработке (о намерении осуществлять обработку) персональных данных. Отличием является лишь то, что в нём дополнительно указывается номер регистрационной записи в реестре операторов и основания вносимых изменений.

Пример информационного письма о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных органа государственной власти, разработанный в соответствии с административным регламентом Роскомнадзора по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», приведён в приложении № 16 к настоящему пособию.

Необходимые изменения вносятся территориальным органом Роскомнадзора в течение 15 дней со дня регистрации информационного письма на основании приказа его руководителя, и в течение 3 дней со дня подписания приказа информация об изменениях размещается на официальном сайте Роскомнадзора (www.rsoc.ru).

В случае прекращения обработки персональных данных орган государственной власти или местного самоуправления обязан уведомить об этом территориальный орган Роскомнадзора в течение 10 рабочих дней путем направления соответствующего заявления с указанием необходимых обоснований.

Пример заявления об исключении сведений об операторе из реестра приведён в приложении № 17 к настоящему пособию. Как и рассмотренное выше заявление о предоставлении выписки из реестра, оно может быть направлено в территориальный орган Роскомнадзора в бумажной форме по почте или в электронной форме через Единый портал государственных услуг.

4.10. Обеспечение защиты персональных данных в ходе эксплуатации и при выводе из эксплуатации информационной системы персональных данных

В соответствии с пунктом 13 требований, утверждённых приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», обеспечение квалифицированной эксплуатации аттестованной информационной системы и обеспечение безопасности персональных данных возложена на оператора информационной системы, т.е. на сам орган государственной власти или орган местного самоуправления.

Квалифицированная эксплуатация системы защиты и выполнение мероприятий по обеспечению безопасности персональных данных подразумевает выполнение следующих мероприятий:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов информационной безопасности и реагирование на них;
- управление конфигурацией аттестованной информационной системы и её системы защиты информации;
- контроль (мониторинг) за обеспечением уровня защищённости информации, содержащейся в информационной системе.

В свою очередь ***управление (администрирование) системой защиты информации*** включает в себя:

- заведение и удаление учётных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;
- управление средствами защиты информации в информационной системе, в том числе параметрами настройки используемого программного обеспечения, включая программное обеспечение средств защиты информации, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
- установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
- централизованное управление системой защиты информации информационной системы в случае эксплуатации многочисленных рабочих мест и использования централизованной системы защиты;
- регистрацию и анализ событий в информационной системе, связанных с защитой информации;
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;
- необходимую корректировку эксплуатационной документации на систему защиты информации и действующих в органе государственной власти или органе местного самоуправления организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных.

Практически все названные мероприятия выполняются администратором безопасности или, в нашем случае, при минимальном количестве со-

трудников, привлекаемых для обеспечения информационной безопасности, – ответственным за обеспечение безопасности персональных данных в органе государственной власти и органе местного самоуправления.

Вместе с тем, следует отметить, что в практике организации работы IT-подразделений и служб функции, связанные с сопровождением общего и прикладного программного обеспечения, выполняются системными администраторами и программистами, а сопровождение средств защиты информации, в том числе их программного обеспечения осуществляется администратором безопасности. Такое распределение достаточно логично и удобно для использования, однако не совсем вписывается в требования, утверждённые названным выше приказом ФСТЭК России, следуя которому все функции, связанные с настройками и обновлениями всего программного обеспечения аттестованной информационной системы, возлагаются на администратора безопасности.

Причём эта особенность не прописана в нормативных актах прямо, но неминуемо следует из того, что осуществлять администрирование системы защиты информации должен осуществлять только администратор безопасности, а в содержание администрирования систем защиты информации, входит, в частности, установка обновлений программного обеспечения.

Ведение учётных записей и установленные полномочия каждому из пользователей информационной системы целесообразно отражать в соответствующем журнале, который удобно вести в электронной форме (большинство информационных систем имеют такую функцию) и периодически выводить на бумажный носитель. Объём подобного журнала невелик, и его распечатка не вызовет каких-либо проблем, и в случае программно-технического сбоя будет очень полезен для квалифицированного восстановления системы.

Периодичность распечатки журнала учётных записей должна определяться интенсивностью использования аттестованной информационной системы и проводиться не реже одного раза в квартал. При этом следует помнить, что содержимое такой распечатки представляет собой не просто конфиденциальную информацию, а критически важную для обеспечения безопасности информации, и названный бумажный экземпляр журнала должен храниться в условиях, исключающих ознакомление с ним лиц, не имеющих для этого прав.

Этот же журнал может быть использован для отражения смены паролей пользователей информационной системы. Периодичность смены паролей может быть установлена администратором безопасности (ответственным за обеспечение безопасности персональных данных), исходя из конкретных условий эксплуатации информационной системы и её системы защиты, но не должна быть реже одного раза в квартал.

Достаточно важной функцией в ходе эксплуатации системы защиты информации является регистрация и анализ событий в аттестованной информационной системе, связанных с защитой информации. Подобная регистрация, как правило, обеспечивается штатными элементами средств защиты информации, и вся фиксируемая информация хранится в электронной форме.

Объём накапливаемой информации, как правило, зависит от принятых настроек системы защиты информации и в свою очередь диктует периодичность её просмотра, анализа и хранения. Все необходимые рекомендации по данным вопросам отражаются в документации на используемую систему защиты информации, но если существует такая возможность, то анализировать регистрируемую информацию (хотя бы по ключевым событиям) очень желательно в ежедневном режиме.

Весьма важной функцией по эксплуатации системы защиты информации является информирование всех пользователей, работающих с аттестованной информационной системой, об угрозах безопасности, правилах эксплуатации системы и отдельных средств защиты информации защиты информации информационной системы. Подобное информирование может осуществляться в письменном виде под роспись одновременно с установленными в органе государственной власти и органе местного самоуправления инструктажами по технике безопасности, пожарной безопасности и др.

В ходе периодического повышения квалификации государственных и муниципальных служащих[38] необходимо проводить их обучение по вопросам информационной безопасности и защиты обрабатываемых персональных данных. Для этого целесообразно включать соответствующие темы в программы повышения квалификации. Проводить подобные занятия должны преподаватели специализированных учебных центров, имеющие аттестацию регуляторов в области технической защиты информации и обладающие необходимой квалификацией.

Все происходящие организационно-штатные изменения структуры, кадровые перестановки, техническое переоснащение и т.п. должны находить своё своевременное отражение в эксплуатационной документации на систему защиты информации и действующих в органе государственной власти или органе местного самоуправления организационно-распорядительных документах по организации обработки и обеспечению безопасности персональных данных.

Выявление инцидентов информационной безопасности и реагирование на них заключается в:

- обнаружении и идентификации инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

[38] В соответствии с действующим законодательством о государственной гражданской и муниципальной службе этот период не должен превышать трёх лет.

- своевременном информировании лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в аттестованной информационной системе;
- анализе инцидентов, в том числе определении источников и причин возникновения инцидентов, а также оценке их последствий;
- планировании и принятии мер по устранению инцидентов, в том числе по восстановлению информационной системы и её сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планировании и принятии мер по предотвращению повторного возникновения инцидентов.

Для эффективного выявления и реагирования на инциденты информационной безопасности в первую очередь необходимо понять их суть и выяснить основные отличительные признаки, которые позволят правильно отграничивать их от иных событий, ежедневно происходящих в любой организации при использовании информационных систем и средств вычислительной техники. К сожалению, в ходе проведенного анализа действующего законодательства и доступной специальной литературы по вопросам информационной безопасности нам не удалось обнаружить ни одного нормативно закрепленного или однозначно воспринимаемого всеми определения инцидента информационной безопасности персональных данных. В связи с этим мы взяли на себя смелость предложить собственное определение, основанное на элементах, встречающихся в специальной литературе толкований.

Инцидент информационной безопасности представляет собой наступление одного или нескольких нежелательных или неожиданных событий, с которыми связана существенная вероятность реализации угрозы безопасности персональных данных.

В органах государственной власти или органах местного самоуправления сфера ответственности при работе с инцидентами информационной безопасности распределяется следующим образом. Выявлением инцидентов информационной безопасности занимается ответственный за обеспечение безопасности персональных данных, а за реагирование на выявленные инциденты – ответственный за организацию обработки персональных данных.

Выявление инцидентов, как правило, происходит в ходе анализа системных журналов общего, общесистемного программного обеспечения, а также журналов регистрации событий в аттестованной информационной системе, связанных с защитой информации. При обнаружении инцидента ответственный за обеспечение безопасности персональных данных должен зафиксировать все обстоятельства произошедшего, оценить возможные последствия и незамедлительно проинформировать ответственного за организацию обработки персональных данных. Все это может выполняться в устной форме. В случаях, когда весьма вероятно наступление особенно значимых

последствий, сообщение об обнаруженном инциденте следует оформить в виде служебной записки на имя руководителя (главы) органа государственной власти или органа местного самоуправления, зарегистрировав её в системе внутреннего документооборота.

Существенную помощь в предварительной оценке возможных последствий произошедшего инцидента информационной безопасности персональных данных окажет разработанная ранее Модель угроз.

Результатом реагирования на выявленный инцидент информационной безопасности должен стать разработанный ответственным за организацию обработки персональных данных план мероприятий по ликвидации последствий и предотвращению повторного возникновения подобных инцидентов. Содержание данного плана составляют технические и организационные мероприятия с указанием сроков и ответственных за их проведение. В связи с тем, что ряд мероприятий может потребовать перестройки конфигурации, изменения состава используемых технических средств, привлечения внешних исполнителей и, следовательно, потребовать выделения финансовых средств, данный план должен быть согласован с соответствующими руководителями (специалистами) и утверждён руководителем органа государственной власти или органа местного самоуправления. Следует помнить, что производимые в ходе реагирования на инцидент информационной безопасности изменения состава и/или конфигурации технических средств информационной системы персональных данных может привести к необходимости переаттестации системы и, как следствие, очередному незапланированному выделению финансовых средств.

Управление конфигурацией аттестованной информационной системы и её системы защиты информации подразумевает:

- поддержание конфигурации информационной системы и её системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и её системы защиты информации);
- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и её системы защиты информации;
- управление изменениями базовой конфигурации информационной системы и её системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и её системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и её системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и её системы защиты

информации, сохранение данных об изменениях базовой конфигурации информационной системы и её системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и её системы защиты информации;

- анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и её системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;
- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и её системы защиты информации;
- внесение информации (данных) об изменениях в базовой конфигурации информационной системы и её системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;
- принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

В ходе контроля (мониторинга) за обеспечением уровня защищённости информации, содержащейся в информационной системе персональных данных, осуществляются:

- контроль за событиями безопасности и действиями пользователей в информационной системе;
- контроль (анализ) защищённости информации, содержащейся в информационной системе;
- анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;
- периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе её эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищённости информации, содержащейся в информационной системе;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищённости информации о доработке (модернизации) системы защиты информации информационной

системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

При завершении эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных в соответствии с эксплуатационной документацией на систему защиты информации информационной системы персональных данных осуществляется либо архивирование персональных данных (если данная информация в дальнейшем может понадобиться), либо их уничтожение и удаление остаточной информации с машинных носителей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года) // Собрание законодательства Российской Федерации, 26.01.2009, № 4, ст. 445.

2. Конвенция (ЕТС № 108) от 28 января 1981 года «О защите частных лиц в отношении автоматизированной обработки данных личного характера».

3. Трудовой кодекс Российской Федерации // Собрание законодательства Российской Федерации, 07.01.2002, № 1 (ч. 1), ст. 3.

4. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3451.

5. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации, 10.03.1997, № 10, ст. 1127.

6. Указ Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» // Собрание законодательства Российской Федерации, 06.06.2005, № 23, ст. 2242.

7. Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // Собрание законодательства Российской Федерации, 24.03.2008, № 12, ст. 1110.

8. Указ Президента Российской Федерации от 15 января 2013 года № 31 «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка) // Собрание законодательства Российской Федерации, 21.01.2013, № 3, ст. 178.

9. Постановление Правительства Российской Федерации от 6 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // Собрание законодательства Российской Федерации, 14.07.2008, № 28, ст. 3384.

10. Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Собрание законодательства Российской Федерации, 22.09.2008, № 38, ст. 4320.

11. Постановление Правительства Российской Федерации от 21 марта 2012 года № 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» // Собрание законодательства Российской Федерации, 02.04.2012, № 14, ст. 1626.

12. Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.

13. Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // Бюллетень нормативных актов федеральных органов исполнительной власти, № 11, 14.03.2005.

14. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19 августа 2011 года № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных» // Опубликован на сайте Роскомнадзора 07.01.2010, http://77.rkn.gov.ru/p3848.

15. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 года № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» // Бюллетень нормативных актов федеральных органов исполнительной власти, № 9, 27.02.2012.

16. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 21 декабря 2011 года № 346 «Об утверждении Административного регламента Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных» // Бюллетень нормативных актов федеральных органов исполнительной власти, № 24, 11.06.2012.

17. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 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» // Российская газета, № 211, 17.09.2014.

18. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите

информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.062013.

19. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.

20. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета, № 208, 18.09.2013.

21. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем. – Введ. 1993-01-01. – М.: Издательство стандартов, 1992. – 6 с.

22. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – Введ. 2014-09-01.

23. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения. – Введ. 2000-06-30.

24. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Утвержден приказом Федерального агентства по техническому регулированию и метрологии 27 декабря 2006 года № 375-ст / М.: Стандартинформ, 2008.

25. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года // http://fstec.ru/component/attachments/download/290 (дата обращения 25.03.2014).

26. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года // http://fstec.ru/component/attachments/download/289 (дата обращения 25.03.2014).

27. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Утверждены руководителем Роскомнадзора 13 декабря 2013 года // СПС Консультант Плюс.

28. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 года // http://fstec.ru/component/attachments/download/675 (дата обращения 25.03.2014).

29. Зоркольцев Р.Д. Персональные данные, получаемые через Интернет: практические вопросы // СПС Консультант Плюс.

30. Кукина С.Л. Хранить как зеницу ока // Руководитель бюджетной организации. 2010. № 7. С. 15 - 24.

31. Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» (постатейный) // СПС Консультант Плюс, 2013.

32. Арешев А.Г., Бачило И.Л., Сергиенко Л.А. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. 2-е изд., доп. и перераб. – М., 2006. С. 75.

33. Кайль А.Н., Новиков Е.А. Комментарий к Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» (постатейный) // СПС Консультант Плюс. 2006.

34. Кухаренко Т.А. Комментарий к Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» (постатейный) // СПС Консультант Плюс, 2011.

35. Маркевич А.С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях: Автореф. дис. ... канд. юрид. наук. – Воронеж, 2007.

36. Петров М.И. Комментарий к Федеральному закону «О персональных данных» (постатейный). – М.: Юстицинформ, 2007. – 160 с.

37. Петросян М.Е. Защита персональных данных. Американская модель // США - Канада. 2000. № 6.

38. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. – М.: Статут, 2011. – 134 с.

39. Федеральная служба безопасности Российской Федерации // http://www.fsb.ru (дата обращения 16.05.2016).

40. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций // http://rkn.gov.ru (дата обращения 16.05.2016).

41. Федеральная служба по техническому и экспортному контролю // http://fstec.ru (дата обращения 16.05.2016).

42. Бизнес без опасности // http://lukatsky.blogspot.ru (дата обращения 16.05.2016).

43. Информационная безопасность по-русски. Персональные данные. Информационная безопасность и ИТ-инновации // http://www.tsarev.biz (дата обращения 16.05.2016).

ПРИЛОЖЕНИЕ 1

Примерный образец приказа о назначении ответственных за организацию обработки и обеспечение безопасности персональных данных в органе государственной власти и утверждении их должностных инструкций

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭНСКОЙ ОБЛАСТИ

ПРИКАЗ

« 15 » января 2014 года № 01-07/1

Энск

О назначении ответственных за организацию обработки и обеспечение безопасности персональных данных и утверждении их должностных инструкций

В соответствии с частью 1 статьи 22.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», подпунктами "а", "б" пункта 1 «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», утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, пунктом 9 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, и пунктом 16 «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» утвержденных приказом ФСБ России от 10 июля 2014 года № 378, п р и к а з ы в а ю:

1. Назначить Иванова И.И. – заместителя руководителя департамента – начальника отдела информационных ресурсов ответственным за организацию обработки персональных данных в департаменте информационных технологий Энской области.

2. Назначить Петрова А.А. – начальника отдела информационной безопасности ответственным за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области.

3. Назначить Петрова А.А. – начальника отдела информационной безопасности ответственным за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям[39].

4. Утвердить должностную инструкцию ответственного за организацию обработки персональных данных в департаменте информационных технологий Энской области (приложение 1).

5. Утвердить должностную инструкцию ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных в департаменте информационных технологий Энской области (приложение 2).

6. Иванову И.И. в срок до 1 марта 2014 года организовать проведение работ по организации обработки и обеспечению безопасности персональных данных в департаменте информационных технологий Энской области в соответствии с требованиями действующего законодательства и представить на утверждение документы, определяющие политику в отношении обработки персональных данных и регламентирующие обработку и обеспечение безопасности персональных данных в департаменте информационных технологий Энской области.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель департамента А.Б. Ветров

[39] Данный пункт необходимо включать в том случае, если в органе власти (учреждении) используются ИСПДн со вторым и выше уровнем защищенности. См. пункт 22 «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» утвержденных приказом ФСБ России от 10 июля 2014 года № 378.

Приложение 1

Должностная инструкция
ответственного за организацию обработки персональных данных
в департаменте информационных технологий Энской области

Общие положения

Настоящая должностная инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных в департаменте информационных технологий Энской области (далее – Департамент).

Ответственный за организацию обработки персональных данных назначается руководителем Департамента.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 12 марта 2012 года № 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»;
- постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года №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»;

- иными действующими нормативными правовыми актами в сфере организации обработки и обеспечения безопасности персональных данных, а также приказами руководителя Департамента.

Обязанности ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных в Департаменте обязан:

1. Организовать подготовку документов, определяющих политику в отношении обработки персональных данных и регламентирующих обработку и обеспечение безопасности персональных данных и обеспечивать их актуальность.
2. Привлекать при необходимости в специалистов из числа сотрудников Департамента в целях выполнения работ по организации обработки и обеспечению безопасности персональных данных в Департаменте.
3. Организовать определение уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных Департамента и классификацию информационных систем персональных данных Департамента.
4. Организовывать прием и обработку обращений и запросов субъектов персональных данных (их представителей), уполномоченного органа по защите прав субъектов персональных данных и осуществлять контроль за приемом и обработкой таких обращений и запросов.
5. Доводить до сведения сотрудников Департамента положения законодательства Российской Федерации в области персональных данных, документов Департамента по вопросам обработки и обеспечения безопасности персональных данных, требований к защите персональных данных.
6. Готовить предложения по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных Департамента, обоснованию такой необходимости и способам обезличивания.
7. Осуществлять внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством Российской Федерации, вести учёт и анализ результатов контроля.
8. Организовывать расследование причин и условий появления нарушений в процессе обработки и обеспечении безопасности персональных данных и разработке предложений по устранению недостатков и нарушений и их предупреждению, а также осуществлении контроля за устранением этих нарушений.
9. Готовить отчеты о состоянии работ по организации обработки и обеспечению безопасности персональных данных в Департаменте.

Права ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных в Департаменте имеет право:

1. Требовать от сотрудников Департамента выполнения документов, определяющих политику в отношении обработки персональных данных и регламентирующих обработку и обеспечение безопасности персональных данных в Департаменте.
2. Контролировать деятельность структурных подразделений Департамента в части выполнения ими требований в области организации обработки и обеспечения безопасности персональных данных.
3. Участвовать в разработке мероприятий по совершенствованию мер по организации обработки и обеспечению безопасности персональных данных в Департаменте.
4. Инициировать проведение служебных расследований по фактам нарушения установленных требований по защите персональных данных, нарушению конфиденциальности персональных данных, утраты технических средств из состава информационных систем персональных данных, машинных носителей персональных данных в Департаменте.
5. Обращаться к руководителю Департамента с предложением о приостановке процесса обработки персональных данных в информационных системах персональных данных или отстранению от работы с персональными данными сотрудников Департамента в случаях нарушения установленной технологии обработки персональных данных или нарушения требований по защите персональных данных.

Ответственность

Ответственный за организацию обработки персональных данных в Департаменте несет персональную ответственность, предусмотренную действующим законодательством, за:

- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
- качество проводимых работ по организации обработки персональных данных в соответствии с функциональными обязанностями;
- разглашение персональных данных, ставшими известными ему по роду своей работы.

Приложение 2

Должностная инструкция
ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области

Общие положения

Настоящая должностная инструкция определяет права, обязанности и ответственность лица, ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области (далее – Департамент).

Ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных, назначается руководителем Департамента.

Ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных, в своей деятельности руководствуется:

- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 12 марта 2012 года № 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»;
- постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 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»;
- иными действующими нормативными правовыми актами в сфере организации обработки и обеспечения безопасности персональных данных, а также приказами руководителя Департамента.

Обязанности ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных

Ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Департамента, обязан:

1. Организовать и координировать работу по обеспечению безопасности персональных данных в информационных системах персональных данных Департамента.
2. Проводить единую техническую политику по обеспечению безопасности персональных данных в Департаменте.
3. Проводить мероприятия по организационному обеспечению безопасности персональных данных.
4. Участвовать в определении уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных Департамента, и классификации информационных систем персональных данных Департамента.
5. Разрабатывать организационно-распорядительные документы по обеспечению безопасности персональных данных в Департаменте.
6. Проводить мероприятия по техническому обеспечению безопасности персональных данных, в том числе по:
   - размещению, охране, организации режима допуска в помещения, в которых ведется обработка персональных данных;
   - закрытию технических каналов утечки персональных данных при их обработке;
   - защите от несанкционированного доступа к персональным данным;
   - выбору средств защиты информации.
7. Обеспечивать возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8. Проводить мероприятия, направленные на предотвращение несанкционированного доступа к персональным данным или передаче их лицам, не имеющим права доступа к такой информации.

9. Осуществлять постоянный контроль за обеспечением установленного уровня защищенности персональных данных.

10. Осуществлять периодический контроль за ведением электронного журнала сообщений (не реже 1 раза в полгода)[40].

11. Осуществлять периодический контроль за ведением журнала безопасности (не реже 1 раза в месяц)[41].

12. Учитывать установленным порядком применяемые в Департаменте машинные носители персональных данных и средства защиты информации.

13. Принимать участие во внутреннем контроле соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством Российской Федерации.

14. Принимать участие в расследование причин и условий появления нарушений в процессе обработки и обеспечении безопасности персональных данных и разработке предложений по устранению недостатков и нарушений и их предупреждению, а также осуществлении контроля за устранением этих нарушений.

15. Готовить предложения по совершенствованию системы безопасности персональных данных в Департаменте.

16. Организовывать повышение осведомленности руководства и сотрудников Департамента по вопросам обеспечения безопасности персональных данных.

Права ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных

Ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Департамента, имеет право:

---

[40] Данный пункт необходимо включать в том случае, если в органе власти (учреждении) используются ИСПДн со вторым и выше уровнем защищенности. См. пункт 19 «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» утвержденных приказом ФСБ России от 10 июля 2014 года № 378.

[41] Данный пункт необходимо включать в том случае, если в органе власти (учреждении) используются ИСПДн с первым уровнем защищенности. См. пункт 22 «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» утвержденных приказом ФСБ России от 10 июля 2014 года № 378.

1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3. Контролировать деятельность структурных подразделений Департамента в части выполнения ими требований в области организации обработки и обеспечения безопасности персональных данных.

4. Готовить предложения о привлечении к проведению работ по обеспечению безопасности персональных данных на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

5. Участвовать в разработке мероприятий по совершенствованию мер по организации обработки и обеспечению безопасности персональных данных в Департаменте.

6. Участвовать в проведении служебных расследований по фактам нарушения установленных требований по защите персональных данных, нарушению конфиденциальности персональных данных, утраты технических средств из состава информационных систем персональных данных, машинных носителей персональных данных в Департаменте.

7. Обращаться к руководителю Департамента с предложением о приостановке процесса обработки персональных данных в информационных системах персональных данных или отстранению от работы с персональными данными сотрудников Департамента в случаях нарушения установленной технологии обработки персональных данных или нарушения требований по защите персональных данных.

Ответственность

Ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Департамента, несет персональную ответственность, предусмотренную действующим законодательством, за:

- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;
- разглашение персональных данных, ставшими известными ему по роду своей работы.

ПРИЛОЖЕНИЕ 2

Примерный образец распоряжения об утверждении перечней обрабатываемых персональных данных и информационных систем персональных данных в органе местного самоуправления

АДМИНИСТРАЦИЯ
Первого сельского поселения

РАСПОРЯЖЕНИЕ

« 17 » января 2014 года № 2-р

с. Первое

Об утверждении перечней обрабатываемых персональных данных, информационных систем персональных данных и перечня помещений, в которых осуществляется обработка персональных данных

В целях исполнения Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и в соответствии с подпунктом "б" пункта 1 «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», утвержденного постановлением Правительства Российской Федерации от 21 марта 20012 года № 211:

1. Утвердить перечни обрабатываемых персональных данных и информационных систем персональных данных, предназначенных для их обработки в администрации Первого сельского поселения Главного муниципального района Энской области в связи с реализацией трудовых отношений, оказанием муниципальных услуг и осуществлением муниципальных функций (прилагаются).
2. Утвердить Перечень помещений администрации Первого сельского поселения Главного муниципального района Энской области, в которых осуществляется обработка персональных данных.
3. Контроль за исполнением настоящего распоряжения возложить на главного бухгалтера администрации Первого сельского поселения Главного муниципального района Энской области Барсукову А.А.

Глава администрации Первого сельского
Поселения Главного муниципального района
Энской области А.Б. Ветров

Приложение 1

Перечни
обрабатываемых персональных данных и информационных систем персональных данных администрации Первого сельского поселения Главного муниципального района Энской области

Состав персональных данных	Обрабатываемые без использования средств автоматизации	Обрабатываемые в ИСПДн	
		«Зарплата и управление персоналом»	«Муниципальная информационная система поселений «Волость»
Фамилия, имя, отчество	✓	✓	✓
Число, месяц, год рождения	✓	✓	✓
Место рождения	✓	✓	—
Адрес (адрес регистрации, фактического проживания)	✓	✓	—
Паспортные данные (серия, номер, кем и когда выдан)	✓	—	✓
Идентификационный номер налогоплательщика (ИНН)	✓	—	✓
Семейное положение	✓	✓	—
Социальное положение	✓	✓	—
Имущественное положение	✓	✓	—
Гражданство	✓	✓	—
Образование	✓	✓	—
Владение иностранными языками	✓	✓	—
Судимость	✓	✓	—
Выполняемая работа с начала трудовой деятельности	✓	✓	—
Близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес)	✓	✓	—
Совместно проживающие граждане (степень родства, фамилия имя отчество, пол, число, месяц и год рождения).	✓	—	✓
Отношение к воинской обязанности, воинское звание (военный билет)	✓	✓	—
Номер телефона	✓	✓	—

Приложение 2

Перечень помещений администрации Первого сельского поселения Главного муниципального района Энской области, в которых осуществляется обработка персональных данных

№ п/п	Помещение	Данные обрабатываются без использования средств автоматизации	ИСПДН, расположенные в данных помещениях	
			«Зарплата и управление персоналом»	«Муниципальная информационная система поселений «Волость»
1.	Кабинет № 1	✓	✓	
2.	Кабинет № 2	✓	✓	
6.	Кабинет № 6			✓
7.	Кабинет № 15	✓	✓	
8.	Кабинет № 21			✓
9.	Серверная		✓	✓

ПРИЛОЖЕНИЕ 3

Примерный образец приказа о создании комиссии по определению уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных, и их классификации

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭНСКОЙ ОБЛАСТИ

ПРИКАЗ

« 19 » января 2014 года № 01-07/3

Энск

О создании комиссии по определению уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных, и их классификации

В целях исполнения пункта 8 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, и части 14 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17, п р и к а з ы в а ю:

1. Создать комиссию по определению уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области и их классификации в составе:

Иванова И.И. – заместителя руководителя департамента информационных технологий Энской области – начальника отдела информационных ресурсов (председатель комиссии);

Петрова А.А. – начальника отдела информационной безопасности департамента информационных технологий Энской области;

Жбанковой И.С. – начальника отдела бухгалтерского учета департамента информационных технологий Энской области.

2. Комиссии определить уровни защищенности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, в срок до 29 января 2013 года.

3. Комиссии определить классы защищенности информационных систем персональных данных департамента информационных технологий Энской области в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17, в срок до 29 января 2013 года.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель департамента А.Б. Ветров

ПРИЛОЖЕНИЕ 4

Примерный образец акта определения уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных органа государственной власти и ее классификации

УТВЕРЖДАЮ

Руководитель департамента
информационных технологий
Энской области

_____ А.Б. Ветров
« 21 » января 2014 года

АКТ
определения уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных «Зарплата и управление персоналом» департамента информационных технологий Энской области и ее классификации

В департаменте информационных технологий Энской области проведен анализ информационной системы персональных данных «Зарплата и управление персоналом» (далее - ИСПДн), в ходе которого установлено:

1. В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119:

1.1. Тип угроз безопасности персональных данных, актуальных для ИСПДн:

Актуальность угроз, связанных с наличием недокументированных (недекларированных) возможностей в программном обеспечении		Тип актуальных угроз безопасности персональных данных
Системное программное обеспечение	Прикладное программное обеспечение	
Нет	Нет	3

1.2. Категории персональных данных, обрабатываемых в ИСПДн:

Специальные	Биометрические	Общедоступные	Иные
–	–	–	✓

1.3. Субъекты персональных данных:

Являются сотрудниками оператора	Не являются сотрудниками оператора
✓	–

1.4. Объём обрабатываемых персональных данных в ИСПДн:

Количество субъектов, чьи персональные данные обрабатываются	
Менее 100 000	Более 100 000
✓	–

2. В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 года № 17:

2.1. Степень возможного ущерба от нарушения свойств безопасности персональных данных, обрабатываемых в ИСПДн:

Степень возможного ущерба от нарушения свойств безопасности персональных данных	Конфиденциальность	Целостность	Доступность
Информационная система/оператор не может выполнять возложенные функции (высокая степень)	–	–	–
Информационная система/оператор не может выполнять одну или несколько возложенных функций (средняя степень)	–	–	–
Информационная система/оператор выполняет возложенные функции с недостаточной эффективностью или выполнение возможно только с привлечением дополнительных сил и средств (низкая степень)	–	–	–
Степень ущерба не может быть определена	✓	✓	✓

2.2. Уровень значимости персональных данных, обрабатываемых в ИСПДн как минимальный – УЗ 4.

2.3. Масштаб ИСПДн:

Федеральный	Региональный	Объектовый
–	–	✓

Вывод:

Уровень защищенности персональных данных при их обработке в ИСПДн – четвертый.

Класс защищенности ИСПДн – К4.

Заместитель руководителя департамента
информационных технологий Энской области –
начальник отдела информационных ресурсов И.И. Иванов

ПРИЛОЖЕНИЕ 5

Примерный образец приказа об утверждении перечня должностей сотрудников органа государственной власти, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных и лиц их замещающих, типовой формы обязательства прекратить обработку персональных данных

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭНСКОЙ ОБЛАСТИ

ПРИКАЗ

« 23 » января 2014 года № 01-07/4

Энск

Об утверждении перечня должностей сотрудников и лиц их замещающих, в трудовые обязанности которых входит осуществление обработки персональных данных либо осуществление доступа к персональным данным, типовой формы обязательства прекратить обработку персональных данных

В соответствии с подпунктом "б" пункта 1 «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», утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, подпунктом "в" пункта 13 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 и подпунктом "в" пункта 5 «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378, п р и к а з ы в а ю:

1. Утвердить перечень должностей сотрудников департамента информационных технологий Энской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных и лиц их занимающих (приложение 1).

2. Утвердить типовую форму обязательства сотрудника департамента информационных технологий Энской области, 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 (приложение 2).

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя департамента – начальника отдела информационных ресурсов Иванова И.И.

Руководитель департамента А.Б. Ветров

Приложение 1

Перечень должностей
сотрудников департамента информационных технологий Энской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных и лиц их замещающих

№ п/п	Наименование должности	Фамилия, имя, отчество	Доступ в помещения	Обрабатываемые без использования средств автоматизации	Обезличивание персональных данных	Доступ к информационным системам персональных данных	
						Зарплата и управление персоналом	Муниципальная информационная система поселений «Волость»
1.	Руководитель департамента	Ветров Александр Борисович	Кабинет № 1, 2, Серверная	✓	–	✓	✓
2.	Заместитель руководителя департамента – начальник отдела информационных ресурсов	Иванов Иван Иванович	Кабинет № 1, 2, Серверная	✓	✓	✓	✓
3.	Ведущий советник отдела информационных ресурсов	Орлов Владимир Иванович	Кабинет № 1, 2, Серверная	✓	–	–	✓
4.	Советник отдела информационных ресурсов	Соколов Петр Григорьевич	Кабинет № 1, 2, Серверная	✓	–	–	✓
5.	Начальник отдела бухгалтерского учета	Жбанкова Ирина Сергеевна	Кабинет № 1	✓	–	✓	–
6.	Инспектор отдела бухгалтерского учета	Дмитриева Светлана Петровна	Кабинет № 2	✓	–	✓	–

Приложение 2

ОБЯЗАТЕЛЬСТВО
о прекращении обработки персональных данных

Я,_____
(фамилия, имя, отчество сотрудника)
исполняющий(ая) должностные обязанности по занимаемой должности _____,
(занимаемая должность)
предупрежден(а), 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 разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю.
3. Не использовать персональные данные с целью получения выгоды.
4. Выполнять требования законодательства Российской Федерации в области персональных данных, документов департамента информационных технологий Энской области по вопросам обработки и обеспечения безопасности персональных данных.
5. После прекращения права на допуск к персональным данным (расторжения служебного контракта) прекратить обработку персональных данных, не разглашать и не передавать персональные данные третьим лицам, ставших известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

«___»_____20__ г. _____ _____
(подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ 6

Примерный образец приказа об утверждении правил обработки персональных данных и регламента учета, хранения и уничтожения машинных носителей персональных данных в органе государственной власти

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭНСКОЙ ОБЛАСТИ

ПРИКАЗ

« 25 » января 2014 года № 01-07/5

Энск

Об утверждении правил обработки персональных данных и регламента учета, хранения и уничтожения машинных носителей персональных данных

В соответствии с подпунктом "б" пункта 1 «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», утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, подпунктом "б" пункта 13 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 и подпунктом "б" пункта 5 «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», утвержденных приказом ФСБ России от 10 июля 2014 года № 378, п р и к а з ы в а ю:

1. Утвердить правила обработки персональных данных в департаменте информационных технологий Энской области (приложение 1).
2. Утвердить регламент учета, хранения и уничтожения машинных носителей персональных данных в департаменте информационных технологий Энской области (приложение 2).
3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя департамента – начальника отдела информационных ресурсов Иванова И.И.

Руководитель департамента А.Б. Ветров

Приложение 1

Правила
обработки персональных данных
в департаменте информационных технологий Энской области

Настоящие Правила устанавливают в департаменте информационных технологий Энской области (далее - Департамент) порядок действий при обработке персональных данных и процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения; порядок рассмотрения запросов субъектов персональных данных или их представителей; порядок работы с обезличенными данными; порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных; порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных; типовую форму согласия на обработку персональных данных сотрудников Департамента, иных субъектов персональных данных; типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

1. Цели обработки персональных данных

Обработка персональных данных в Департаменте осуществляется в целях:

- реализации трудовых отношений;
- оказания государственных услуг и осуществления государственных функций.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

Департамент устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

- издание Департаментом нормативных правовых актов по вопросам обработки и обеспечения безопасности персональных данных;
- назначение ответственных за организацию обработки и обеспечение безопасности персональных данных в Департаменте;
- определение сотрудников Департамента, допущенных к обработке персональных данных и несущих в соответствии с действующим за-

конодательством Российской Федерации ответственность за нарушение требований по обеспечению безопасности персональных данных;

- ознакомление сотрудников Департамента, перед началом обработки персональных данных, под роспись с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных в Департаменте, документами Департамента, определяющими политику в отношении обработки персональных данных;
- обучение сотрудников Департамента, допущенных к обработке персональных данных, выполнению требований по их защите;
- получение персональных данных лично у субъекта персональных данных или в случаях, установленных действующим законодательством, у его законных представителей;
- при получении персональных данных у третьей стороны Департамент извещает об этом субъекта персональных данных заранее, получает его письменное согласие и сообщает ему о целях, предполагаемых источниках и способах получения персональных данных;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- опубликование на официальном сайте Департамента в сети Интернет документов Департамента, определяющих политику в отношении обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также документами Департамента.

3. Получение персональных данных

Все персональные данные получаются непосредственно от субъекта персональных данных.

Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку.

Типовая форма согласия на обработку персональных данных сотрудников Департамента, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные приведены соответственно в приложениях 1 и 2 к настоящим Правилам.

В случае недееспособности либо несовершеннолетия субъекта все персональные данные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает согласие на их обработку.

В случаях, когда необходимые персональные данные субъекта могут быть получены только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении необходимо сообщить о целях, правовых основаниях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение.

4. Допуск к персональным данным

Перечень должностей сотрудников Департамента, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным и лиц их занимающих, утверждается приказом Департамента[42].

Каждый сотрудник, допущенный к персональным данным, обязан подписать обязательство, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей.

Формирование перечня должностей сотрудников Департамента, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным и лиц их занимающих, а также внесение предложений по его корректировке, ознакомление данных лиц с обязательством под роспись осуществляет лицо, ответственное за организацию обработки персональных данных в Департаменте.

5. Обязанности сотрудников, допущенных к обработке персональных данных

Сотрудники Департамента, допущенные к обработке персональных данных, обязаны:

- знать и выполнять требования законодательства Российской Федерации в области персональных данных, документов Департамента по вопросам обработки и обеспечения безопасности персональных данных, настоящих Правил;
- соблюдать правила обработки персональных данных (машинных носителей персональных данных), порядок их учета и хранения, исключать доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей;
- не разглашать третьим лицам персональные данные, ставших известными, в связи с выполнением должностных обязанностей, информировать непосредственное руководство о фактах нарушения установ-

[42] Содержание и особенности формирования данного нормативного акта рассмотрено в параграфе 4.4. настоящего Пособия.

ленного порядка обработки персональных данных, о попытках несанкционированного доступа к персональным данным;
- в случае попытки третьих лиц получить от них персональные данные, сообщать непосредственному руководителю;
- не использовать персональные данные с целью получения выгоды;
- после прекращения права на допуск к персональным данным (расторжения служебного контракта) прекратить обработку персональных данных, не разглашать и не передавать персональные данные третьим лицам, ставшие известными в связи с исполнением должностных обязанностей.

Сотрудникам Департамента, допущенным к обработке персональных данных, запрещается:
- использовать персональные данные в неслужебных целях, а также в служебных целях – при ведении телефонных переговоров, в открытой переписке, статьях и выступлениях;
- передавать персональные данные по незащищенным каналам связи (факсимильная связь, электронная почта);
- использовать для обработки и хранения персональных данных не учтенные машинные носители информации;
- снимать копии с документов и машинных носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для фиксации персональных данных;
- передавать документы и машинные носители информации, содержащие персональные данные другим сотрудникам, не допущенным к обработке персональных данных;
- выполнять на дому работы, связанные с использованием персональных данных, выносить документы и машинные носители информации, содержащие персональные данные, из служебных помещений без санкции руководителя Департамента.

6. Содержание обрабатываемых персональных данных

В Департаменте персональные данные обрабатываются в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций.

Перечень персональных данных, обрабатываемых в Департаменте с привязкой к целям обработки персональных данных, а также указанием информационных систем, в которых они обрабатываются, утверждается приказом Департамента[43].

[43] Содержание и особенности формирования данного нормативного акт рассмотрены в параграфе 4.2. настоящего Пособия

Формирование перечня персональных данных, обрабатываемых в Департаменте, и внесение предложений по его корректировке осуществляет лицо, ответственное за организацию обработки персональных данных в Департаменте.

7. Категории субъектов, персональные данные которых обрабатываются

К категориям субъектов, персональные данные которых обрабатываются в Департаменте в связи с реализацией трудовых отношений, относятся:

- сотрудники Департамента;
- руководители подведомственных Департаменту учреждений;
- кандидаты на замещение вакантных должностей и на включение в кадровый резерв Департамента.

К категориям субъектов, персональные данные которых обрабатываются в Департаменте в связи с оказанием государственных услуг и осуществлением государственных функций, относятся граждане, обратившиеся в Департамент в целях получения государственной услуги.

8. Сроки обработки, хранения и уничтожения персональных данных

Персональные данные, связанные с реализацией трудовых отношений, обрабатываются и хранятся в течение действия служебного контракта (трудового договора) и в течение 75 (семидесяти пяти) лет после прекращения его действия.

Персональные данные, связанные с оказанием государственных услуг и осуществлением государственных функций, обрабатываются и хранятся до достижения цели их обработки или до момента прекращения необходимости в достижении заранее заявленных целей обработки персональных данных.

В случае достижения цели обработки персональных данных или при наступлении иных законных оснований обработка персональных данных прекращается, и они уничтожаются в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если Департамент не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных их обработка прекращается и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, они уничтожаются в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если Департамент не вправе осу-

ществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

Уничтожение машинных носителей персональных данных, выведенных из эксплуатации, производится на основании акта уничтожения, утверждаемого руководителем Департамента.

Решение о стирании записей, содержащих персональные данные, в электронных базах данных принимается сотрудниками Департамента, допущенными к обработке персональных данных, самостоятельно в срок, не превышающий тридцати дней по достижении целей обработки или с момента утраты необходимости в достижении этих целей.

9. Порядок рассмотрения запросов субъектов персональных данных или их представителей

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

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Департаментом способы обработки персональных данных;
- наименование и место нахождения Департамента, сведения о сотрудниках Департамента, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Департаментом или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения.

Сведения предоставляются ответственным за организацию обработки персональных данных в Департаменте субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Департаментом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Департаментом, подпись субъекта персональных данных или его представителя.

Субъект персональных данных вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно

полученными или не являются необходимыми для заявленной цели обработки.

В случае обращения субъекта персональных данных или его представителя либо при получении запроса от субъекта персональных данных или его представителя ответственный за организацию обработки персональных данных в Департаменте обязан:

- сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных;
- предоставить безвозмездно возможность субъекту персональных данных или его представителю ознакомления с этими персональными данными в течение тридцати дней с даты обращения или получения запроса. В случае принятия решения об отказе в предоставлении информации о наличии персональных данных о соответствующем субъекте ему или его представителю в срок, не превышающий тридцати дней со дня обращения (либо с даты получения запроса) в письменной форме направить мотивированный ответ, содержащий ссылку на норму Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иного федерального закона, являющуюся основанием для такого отказа;
- предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, инициировать процедуру внесения в них необходимых изменений;
- в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, инициировать процедуру уничтожения таких персональных данных;
- уведомить субъекта персональных данных или его представителя, а также третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах.

Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения сведений и ознакомления с

такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

Субъект персональных данных вправе обратиться повторно в Департамент или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцати дней в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с обязательными сведениями должен содержать обоснование направления повторного запроса.

В случае несоответствия повторного запроса субъекта персональных данных указанным выше условиям такой запрос может быть отклонен. Такой отказ должен быть мотивированным.

Регистрация обращений и запросов субъектов персональных данных или их представителей, а также уполномоченного органа по защите прав субъектов персональных данных осуществляется ответственным за организацию обработки персональных данных в Департаменте в журнале. Листы журнала нумеруются, прошиваются и опечатываются.

Журнал регистрации обращений и запросов субъектов персональных данных или их представителей, уполномоченного органа по защите прав субъектов персональных данных вносится в номенклатуру дел и журналов Департамента с постановкой на инвентарный учет. Форма журнала приведена в приложении 3 к настоящим Правилам.

10. Порядок работы с обезличенными данными

Обезличивание персональных данных в Департаменте проводится с целью снижения ущерба от утечки персональных данных, снижения уровня защищенности персональных данных, обрабатываемых в информационной системе и по достижении целей обработки персональных данных или утраты необходимости в достижении этих целей.

Способы обезличивания персональных данных, применяемые в Департаменте:

- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений.

Решение о необходимости обезличивания персональных данных и конкретных формах её реализации принимает руководитель Департамента.

Ответственный за организацию обработки персональных данных в Департаменте готовит предложения по обезличиванию персональных данных, обрабатываемых в информационных системах, обоснованию такой необходимости и способам обезличивания.

Перечень должностей сотрудников Департамента, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом Департамента[44].

Контроль за соблюдением порядка обезличивания персональных данных осуществляется ответственными за организацию обработки и обеспечение безопасности персональных данных в Департаменте в рамках внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и документами Департамента.

Обезличенные персональные данные не подлежат разглашению.

11. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных

Для помещений, в которых ведется обработка персональных данных, организуется режим безопасности, при котором обеспечивается сохранность документов и машинных носителей информации, содержащих персональные данные, средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

В помещениях, где размещены технические средства, участвующие в обработке персональных данных, а также хранятся машинные носители персональных данных (далее – Помещения), право самостоятельного доступа в рабочие дни имеют только сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, утвержденный приказом Департамента.

Нахождение иных лиц в Помещениях возможно только в сопровождении сотрудника Департамента, имеющего право самостоятельного доступа в это Помещение на время, ограниченное служебной необходимостью. При этом должна быть исключена возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через выводимую на экран монитора и принтер информацию, а также к машинным носителям персональных данных.

Технические средства, участвующие в обработке персональных данных, в Помещении должны располагаться таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в Помещение, а также через двери и окна Помещения.

В случае отсутствия сотрудников, имеющих право самостоятельного доступа, в Помещении в рабочее, а также в нерабочее время Помещение должно закрываться на ключ.

Уборка Помещения должна проводиться только в присутствии сотрудника, имеющего право самостоятельного доступа в Помещение.

---

[44] Содержание и особенности формирования данного нормативного акт рассмотрено в параграфе 4.2. настоящего пособия

На время проведения ремонта Помещения все технические средства, участвующие в обработке персональных данных, а также документы и машинные носители информации, содержащие персональные данные, переносятся в другое Помещение, используемое для обработки персональных данных.

В случае возникновения нештатных ситуаций необходимо незамедлительно сообщать о них руководителю Департамента. Доступ в Помещение с целью устранения нештатных ситуаций, а также в нерабочее время осуществляется с разрешение руководителя Департамента. В случае привлечения для устранения внештатных ситуаций внешних исполнителей и сотрудников Департамента, не включенных в Перечень лиц, имеющих доступ в Помещение, доступ в Помещение осуществляется с разрешения руководителя Департамента в присутствии сотрудника, имеющего право самостоятельного доступа в Помещение.

Контроль за соблюдением порядка доступа сотрудников в Помещения осуществляют ответственные за организацию обработки и обеспечение безопасности персональных данных в Департаменте.

12. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и документами Департамента, проводятся периодические проверки условий обработки персональных данных. Проверки проводятся ответственными за организацию обработки и обеспечение безопасности персональных данных в департаменте по плану проведения внутреннего контроля или поручению руководителя Департамента. План проведения внутреннего контроля формируется ответственным за организацию обработки персональных данных и утверждается руководителем Департамента ежегодно.

Проверки осуществляются путем опроса, а также путем осмотра рабочих мест сотрудников Департамента, участвующих в процессе обработки персональных данных.

Контролируемые вопросы в ходе проведения проверки:

- наличие у сотрудников допуска к обработке персональных данных;
- наличие согласий субъектов на обработку их персональных данных;
- соблюдение целей, состава и сроков обработки персональных данных;
- соблюдение правил по обезличиванию персональных данных;
- соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;
- соблюдение сотрудниками правил парольной политики;
- соблюдение сотрудниками правил антивирусной защиты;

- соблюдение сотрудниками правил работы с машинными носителями персональных данных;
- соблюдение порядка работы со средствами защиты информации.

По итогам каждой проверки составляется протокол проверки соответствия обработки персональных данных требованиям к защите персональных данных по форме, приведенной в приложение 5 к настоящим Правилам.

При выявлении в ходе проверки нарушений в протоколе указываются мероприятия по устранению этих нарушений и сроки их исполнения. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных докладывает руководителю Департамента.

Протоколы проверок подписываются ответственными за организацию обработки и обеспечение безопасности персональных данных и утверждаются руководителем Департамента. Хранятся протоколы проверок у ответственного за организацию обработки персональных данных в течение пяти лет.

Приложение 1
к правилам обработки
персональных данных

Типовая форма
согласия на обработку персональных данных сотрудников департамента информационных технологий Энской области, иных субъектов персональных данных

Я,_____
(фамилия, имя, отчество)

_____
(адрес проживания)

_____
(паспорт: серия, номер, дата выдачи, кем выдан)

_____

В соответствии *со статьями 26, 42 Федерального закона от 27 июля 2004 года № 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 мая 2005 года № 609,* даю согласие департаменту информационных технологий Энской области (далее – Департамент) на обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу в иные органы государственной власти и местного самоуправления и организации, обезличивание, блокирование, уничтожение) моих персональных данных, в составе:

фамилия, имя, отчество;
число, месяц, год рождения;
место рождения;
гражданство;
образование;
владение иностранными языками;
судимость;
допуск к государственной тайне;
выполняемая работа с начала трудовой деятельности;
награды и знаки отличия;
близкие родственники (степень родства, ФИО, год, число, месяц и место рождения, место работы, домашний адрес);
пребывание за границей;
отношение к воинской обязанности, воинское звание;
домашний адрес (адрес регистрации, фактического проживания);
номер телефона;
документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан);

наличие заграничного паспорта (серия, номер, кем и когда выдан);

номер страхового свидетельства обязательного пенсионного страхования;

индивидуальный номер налогоплательщика;

сведения о доходах, об имуществе и обязательствах имущественного характера.

Обработка моих персональных данных может осуществляться с использованием средств автоматизации и без использования таковых исключительно в целях *реализации трудовых отношений/предоставления государственной услуги*.

Согласие вступает в силу с момента его подписания.

Департамент может осуществлять обработку моих персональных данных *в течение действия служебного контракта и в течение 75 (семидесяти пяти) лет после его прекращения/до достижения цели их обработки или до момента прекращения необходимости в достижении заранее заявленных целей обработки персональных данных*.

Я вправе отозвать свое согласие на обработку персональных данных посредством письменного заявления.

«___»_____20__ г. _____ _____

(подпись) (расшифровка подписи)

Приложение 2
к правилам обработки
персональных данных

Типовая форма
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне,_____
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные департаменту информационных технологий Энской области.

В соответствии *со статьями 26, 42 Федерального закона от 27 июля 2004 года № 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 мая 2005 года № 609*, определен перечень персональных данных, которые субъект персональных данных обязан предоставить департаменту информационных технологий Энской области в целях *реализации трудовых отношений/предоставления государственной услуги*.

Без представления субъектом персональных данных *служебный контракт не может быть заключен/государственная услуга не может быть предоставлена*.

«___»_____20__ г. _____ _____
(подпись) (расшифровка подписи)

Приложение 3
к правилам обработки
персональных данных

Инв. №_____

Журнал регистрации обращений и запросов субъектов персональных данных или их представителей, уполномоченного органа по защите прав субъектов персональных данных в департаменте информационных технологий Энской области

Начат «___»_____20__г.
Окончен «___»_____20__г.

Пронумеровано, прошито и опечатано _____ листов.

№ п/п	Сведения о запрашивающем лице/органе	Номер входящего документа, дата	Цель обращения/запроса	Действия по результатам обращения/запроса	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7

Приложение 4
к правилам обработки
персональных данных

УТВЕРЖДАЮ

Руководитель департамента
информационных технологий
Энской области

_____ А.Б. Ветров
« __ » _____ 20__ года

Протокол
проверки соответствия обработки персональных данных требованиям к защите персональных данных в департаменте информационных технологий Энской области

Настоящий Протокол составлен о том, что «____» _____ 20__ года заместителем руководителя департамента информационных технологий Энской области – начальником отдела информационных ресурсов Ивановым И.И. и начальником отдела информационной безопасности департамента информационных технологий Энской области Петровым А.А. проведена проверка соответствия обработки персональных данных в департаменте информационных технологий Энской области (далее - Департамент) требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и документами Департамента.

1. Поверка осуществлялась в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 12 марта 2012 года № 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», постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных» и правовых актов Департамента, определяющих политику в отношении обработки персональных данных.

2. В ходе проверки контролировались следующие вопросы:

наличие у сотрудников допуска к обработке персональных данных;

наличие согласий субъектов на обработку их персональных данных;

соблюдение целей, состава и сроков обработки персональных данных;

соблюдение правил по обезличиванию персональных данных;

соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

соблюдение сотрудниками правил парольной политики;

соблюдение сотрудниками правил антивирусной защиты;

соблюдение сотрудниками правил работы с машинными носителями персональных данных;

соблюдение порядка работы со средствами защиты информации.

3. В ходе проверки выявлены следующие нарушения:

_____,
_____,
_____.

4. Меры по устранению выявленных нарушений:

_____,
_____,
_____.

5. Срок устранения нарушений: «____» _____ 20__ года.

Заместитель руководителя департамента
информационных технологий Энской области –
начальник отдела информационных ресурсов _____И.И. Иванов

Начальник отдела информационных ресурсов
департамента информационных технологий
Энской области _____П.П. Петров

Приложение 2

Регламент
учета, хранения и уничтожения машинных носителей персональных данных в департаменте информационных технологий Энской области

1. Общие положения

Настоящий Регламент устанавливает порядок учета, хранения и уничтожения машинных носителей информации, содержащих персональные данные в департаменте информационных технологий Энской области (далее - Департамент).

Требования настоящего Регламента распространяются на всех сотрудников Департамента, допущенных к обработке персональных данных.

На сотрудников Департамента, допущенных к обработке персональных данных, возлагается персональная ответственность за выполнение всех обязанностей, возложенных на них в настоящем Регламенте.

Ознакомление сотрудников Департамента с требованиями Регламента осуществляет ответственный за организацию обработки персональных данных в Департаменте.

Контроль за соблюдением порядка учета, хранения и уничтожения машинных носителей персональных данных осуществляет ответственный за организацию обработки персональных данных в Департаменте в рамках внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в Департаменте.

2. Порядок учета машинных носителей персональных данных

В Департаменте учет и хранение машинных носителей персональных данных осуществляет ответственный за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Департамента (далее - Ответственный).

При смене Ответственного составляется акт приема-передачи машинных носителей персональных данных и всех журналов учета машинных носителей персональных данных, который утверждается руководителем Департамента.

Учет машинных носителей персональных данных производится в журнале учета машинных носителей персональных данных, листы которого нумеруются, прошиваются и опечатываются.

Журнал учета машинных носителей персональных данных вносится в номенклатуру дел и журналов Департамента с постановкой на инвентарный учет. Форма журнала приведена в приложении к настоящему Регламенту.

Машинные носители персональных данных учитываются поэкземплярно, тиражируются только по распоряжению руководителя Департамента.

На машинных носителях персональных данных в удобном для просмотра месте проставляются следующие учетные реквизиты:

- учетный номер;
- дата постановки на учет.

Ответственный выдает машинные носители персональных данных только сотрудникам Департамента, допущенным к обработке персональных данных. Машинные носители персональных данных выдаются сотруднику под его личную роспись в журнале учета машинных носителей персональных данных.

Перед записью персональных данных на машинный носитель сотрудник передает его Ответственному для учета.

При получении машинного носителя персональных данных из сторонней организации он передается Ответственному для учета, после чего может быть выдан сотрудникам для работы.

Движение (выдача и возврат) машинных носителей персональных данных между сотрудниками осуществляется только через Ответственного, с обязательной записью в журнале учета машинных носителей персональных данных.

Машинные носители персональных данных пересылаются сторонним организациям с сопроводительным письмом заказным почтовым отправлением.

Перед передачей машинного носителя персональных данных другому сотруднику или в сторонние организации для ремонта, технического обслуживания вся информация и остаточные данные с него должны быть уничтожены.

3. Порядок хранения машинных носителей персональных данных

Машинные носители персональных данных должны храниться в служебных помещениях Департамента, в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить машинные носители персональных данных из служебных помещений без санкции руководителя Департамента.

Машинные носители персональных данных, служебная необходимость использования которых в дальнейшем отсутствует незамедлительно сдаются Ответственному.

4. Порядок уничтожения машинных носителей персональных данных

В ходе внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в Департаменте определяется перечень машинных носителей персональных данных технически неисправных или утративших свое практическое значение и не подлежащих архивному хранению, которые могут быть выведены из эксплуатации.

Машинные носители персональных данных, выведенные из эксплуатации, подлежат только физическому уничтожению способом исключающим возможность восстановления информации с них, с оформлением акта уничтожения. В журнале учета машинных носителей персональных данных об этом делается отметка со ссылкой на соответствующий акт.

Акты уничтожения подписываются ответственными за организацию обработки и обеспечение безопасности персональных данных в Департаменте и утверждаются руководителем Департамента. Хранятся акты уничтожения у ответственного за организацию обработки персональных данных в течении пяти лет.

Приложение 1
к регламенту учета, хранения и уничтожения машинных носителей персональных данных

Инв. №_____

Журнал учета машинных носителей персональных данных в департаменте информационных технологий Энской области

Начат «___»_____20__г.
Окончен «___»_____20__г.
Пронумеровано, прошито и опечатано _____ листов.
Ответственный _____

№ п/п	Инвентарный номер, дата регистрации	Заводской номер	Место хранения машинного носителя персональных данных	Тип/емкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/ дата установки	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (Подпись, дата)	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1.	Инв. № 1	150065770	каб. № 9	Флеш-накопитель JetFlash Transcend 16 Gb	1	каб.№1			
2.	Инв. № 2	150065771	каб. № 7	Жесткий диск 2,5" WD 1Tb	1	каб.№ 7, 20.05.2015			
3	Инв. № 2	150065772	каб. № 9	внешний жесткий диск 3Q Fast Portable HDD Extermal 2,5 500 Gb	1	каб.№ 21			

ПРИЛОЖЕНИЕ 7

Примерный образец модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных органа местного самоуправления

УТВЕРЖДАЮ

Глава администрации Первого
сельского поселения Главного
муниципального района
Энской области

_____ А.Б. Ветров
« 27 » января 2014 года

МОДЕЛЬ УГРОЗ
безопасности персональных данных при их обработке в информационной системе персональных данных «Муниципальная информационная система поселений «Волость» администрации Первого сельского поселения Главного муниципального района Энской области

Методической основой построения настоящей Модели угроз являются Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Методика определения актуальных угроз), утвержденная заместителем директора ФСТЭК России 14 февраля 2008 года, Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Базовая модель), утвержденная заместителем директора ФСТЭК России 15 февраля 2008 года, и приказ ФСБ России от 10 июля 2014 года № 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».

1. Общая характеристика информационной системы персональных данных

Информационная система персональных данных «Муниципальная информационная система поселений «Волость» (далее – ИСПДн) предназначена для ведения электронной формы расширенной похозяйственной книги,

содержание которой закреплено в приказе Министерства сельского хозяйства Российской Федерации от 11 октября 2010 года № 345 «Об утверждении формы и порядка ведения похозяйственных книг органами местного самоуправления поселений и органами местного самоуправления городских округов» (зарегистрировано в Министерстве юстиции Российской Федерации 22 ноября 2010 года № 19007). В ИСПДн обрабатываются иные категории персональных данных не более 1000 субъектов персональных данных, не являющихся сотрудниками администрации Первого сельского поселения.

Для информационной системы актуальны угрозы **3 типа.**

Для ИСПДн установлен **4 уровень защищенности** персональных данных и класс защищенности – К4 (акт классификации утвержден главой администрации Первого сельского поселения Главного муниципального района Энской области 21 января 2014 года).

ИСПДн представляет собой автоматизированное рабочее место, построенное на базе IBM PC-совместимого персонального компьютера под управлением операционной системы Windows XP. Режим обработки персональных данных в ИСПДн многопользовательский с разграничением прав доступа пользователей.

Все технические средства ИСПДн находятся в пределах Российской Федерации и размещаются в пределах контролируемой зоны в помещении № 3 администрации Первого сельского поселения.

ИСПДн не имеет подключения к локальным вычислительным сетям, но имеет доступ к сети Интернет через беспроводную сеть оператора сотовой связи при этом передача персональных данных через сеть Интернет не осуществляется.

Исходя из предложенных в Базовой модели критериев типизации, ИСПДн относится к системам типа: автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

На основании требований, утверждённых приказом ФСБ России № 378, минимальный класс СКЗИ, применяемых для ИСПДн данного типа: **КС1**.

2. Исходный уровень защищенности информационной системы персональных данных

Характеристики уровня исходной защищенности для ИСПДн.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования:			

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с записями баз ПДн: модификация, передача	-	-	+
4. По разграничению доступа к ПДн: ИСПДн, к которой имеет доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	-	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	-	+	-
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации	+	-	-

Таким образом, в соответствии с Методикой определения актуальных угроз ИСПДн имеет **средний (5)** уровень исходной защищенности.

3. Оценка актуальности угроз безопасности персональных данных при их обработке в информационной системе персональных данных

На основании Базовой модели для ИСПДн определены следующие угрозы безопасности персональных данных:

- Угрозы утечки информации по техническим каналам;
- Угрозы несанкционированного доступа к персональным данным, обрабатываемым на автоматизированном рабочем месте.

3.1. Угрозы утечки информации по техническим каналам

3.1.1. Угрозы утечки акустической (речевой) информации.

В ИСПДн функции голосового ввода или функции воспроизведения персональных данных акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятно (0).**

3.1.2. Угрозы утечки видовой информации.

Контролируется доступ в помещение с ИСПДн, персональный компьютер расположен так, что практически исключен визуальный доступ к экрану монитора и принтеру.

Вероятность реализации угрозы – **маловероятно (0)**.

3.1.3. Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок.

Элементы ИСПДн экранируются несущими стенами здания и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

Вероятность реализации угрозы – **маловероятно (0)**.

3.2. Угрозы несанкционированного доступа к персональным данным, обрабатываемым на автоматизированном рабочем месте

3.2.1. Угрозы уничтожения, хищения аппаратных средств, носителей информации путем физического доступа к элементам информационных систем персональных данных.

3.2.1.1. Кража компьютеров.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации.

Вероятность реализации угрозы – **маловероятно (0)**.

3.2.1.2. Кража носителей информации.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Системный блок персонального компьютера опломбирован, физический доступ к жесткому диску отсутствует. Внешние машинные носители персональных данных в ИСПДн не используются.

Вероятность реализации угрозы – **маловероятно (0)**.

3.2.1.3. Кража ключей и атрибутов доступа.

Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. В ИСПДн используются «сложные» пароли доступа, осуществляется их периодическая смена, не реже одного раза в 90 дней. Пользователи ИСПДн проинструктированы о недопустимости какой-либо записи парольно-ключевой информации. Аппаратные атрибуты доступа в ИСПДн не используются.

Вероятность реализации угрозы – **низкая (2)**.

3.2.1.4. Кража, модификация, уничтожение информации.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Осуществляется идентификация и аутентификация пользователей ИСПДн по уникальным именам и паролям. Сотрудники администрации, допущенные к обработке персональных данных, проинструктированы о недопустимости их передачи третьим лицам. Однако

пользователи ИСПДн потенциально могут осуществить кражу, модификацию или уничтожение обрабатываемых персональных данных.

Вероятность реализации угрозы – **средняя (5).**

3.2.1.5. Вывод из строя узлов информационной системы персональных данных, каналов связи.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Доступ к сети Интернет осуществляется с использованием беспроводной сети оператора сотовой связи. Повреждение канала связи без специальных технических средств крайне затруднительно.

Вероятность реализации угрозы – **низкая (2).**

3.2.1.6. Несанкционированное отключение средств защиты информации.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Осуществляется разграничение доступа пользователей к настройкам средств защиты информации.

Вероятность реализации угрозы – **маловероятно (0).**

3.2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств.

3.2.2.1. Действия вредоносных программ (вирусов).

В ИСПДн применяется средство антивирусной защиты: антивирус Касперского 6.0 для Windows Workstations. Антивирусный контроль осуществляется в автоматическом режиме (постоянный мониторинг). Обновление баз сигнатур антивируса производится в ручном и автоматическом режимах посредством сети Интернет не реже одного раза в неделю. Осуществляется разграничение доступа пользователей к настройкам антивирусного средства.

Вероятность реализации угрозы – **маловероятно (0).**

3.2.2.2. Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных.

В ИСПДн применяется лицензионное системное и прикладное программное обеспечение, разработанное сторонними организациями и потенциально содержащее недекларированные возможности. Однако использование недекларированных возможностей программного обеспечения требует высокой квалификации нарушителя, наличия специализированного программного и аппаратного обеспечения и финансово затратно.

Вероятность реализации угрозы – **низкая (2).**

3.2.2.3. Установка программного обеспечения, не связанного с исполнением служебных обязанностей.

В ИСПДн осуществляется разграничение доступа пользователей к системным настройкам.

Вероятность реализации угрозы – **маловероятно (0)**.

3.2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы персональных данных и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера.

3.2.3.1. Утрата ключей и атрибутов доступа.

Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Пользователи ИСПДн проинструктированы о недопустимости какой-либо записи парольно-ключевой информации. Аппаратные атрибуты доступа в ИСПДн не используются.

Вероятность реализации угрозы – **низкая (2)**.

3.2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые могут осуществить непреднамеренную модификацию или уничтожение обрабатываемых персональных данных.

Вероятность реализации угрозы – **средняя (5)**.

3.2.3.3. Непреднамеренное отключение средств защиты информации.

Осуществляется разграничение доступа пользователей к настройкам средств защиты информации.

Вероятность реализации угрозы – **маловероятно (0)**.

3.2.3.4. Выход из строя аппаратно-программных средств.

В ИСПДн используется лицензионное системное и прикладное программное обеспечение, однако применяемые аппаратно-программных средства несовершенны.

Вероятность реализации угрозы – **средняя (5)**.

3.2.3.5. Сбой системы электроснабжения.

В ИСПДн ко всем ключевым элементам подключен источник бесперебойного питания.

Вероятность реализации угрозы – **низкая (2)**.

3.2.4. Угрозы преднамеренных действий внутренних нарушителей.

3.2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке.

Осуществляется идентификация и аутентификация пользователей ИСПДн по уникальным именам и паролям.

Вероятность реализации угрозы – **низкая (2)**.

3.2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

Сотрудники администрации, допущенные к обработке персональных данных, проинструктированы о недопустимости их передачи третьим лицам. Однако пользователи ИСПДн потенциально могут осуществить кражу, модификацию или уничтожение обрабатываемых персональных данных.

Вероятность реализации угрозы – **средняя (5)**.

3.2.5. Угрозы несанкционированного доступа по каналам связи.

3.2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из информационной системы персональных данных и принимаемой из внешних сетей информации.

3.2.5.1.1. Перехват за переделами контролируемой зоны.

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В то же время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.

Вероятность реализации угрозы – **низкая (2)**.

3.2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями.

Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. Осуществляется идентификация и аутентификация пользователей ИСПДн по уникальным именам и паролям. ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В то же время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.

Вероятность реализации угрозы – **маловероятно (0).**

3.2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.

Осуществляется идентификация и аутентификация пользователей ИСПДн по уникальным именам и паролям. ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.

Вероятность реализации угрозы – **маловероятно (0).**

*3.2.5.2. Угрозы сканирования сети**,** направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.*

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В то же время сканирование сети требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.

Вероятность реализации угрозы – **низкая (2)**.

3.2.5.3. Угрозы выявления паролей по сети.

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В то же время выявление паролей по сети требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.

Вероятность реализации угрозы – **низкая (2).**

3.2.5.4. Угрозы подмены доверенного объекта в сети.

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В то же время подмена доверенного объекта в сети требует высокой квалификации нарушителя.

Вероятность реализации угрозы – **низкая (2).**

3.2.5.5. Угрозы типа «Отказ в обслуживании».

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В то же время отказ в обслуживании требует высокой квалификации нарушителя.

Вероятность реализации угрозы – **низкая (2).**

3.2.5.6. Угрозы удаленного запуска приложений.

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В то же время, удаленный запуск приложений требует высокой квалификации нарушителя.

Вероятность реализации угрозы – **низкая (2).**

3.2.5.7. Угрозы внедрения по сети вредоносных программ.

ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. В ИСПДн применяется средство антивирусной защиты: антивирус Касперского 6.0 для Windows Workstations. Антивирусный контроль осуществляется в автоматическом режиме (постоянный мониторинг). Обновление баз сигнатур антивируса производится в ручном и автоматическом режимах посредством сети Интернет не реже одного раза в неделю.

Вероятность реализации угрозы – **маловероятно (0).**

Оценка реализуемости, возможности, опасности и актуальности угроз безопасности персональных данных при их обработке в ИСПДн представлена в таблице 1.

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Муниципальная информационная система поселений «Волость» администрации Первого сельского поселения Главного муниципального района Энской области (сводная таблица)

Тип угроз безопасности персональных данных	Коэффициент реализуемости УБПДн (Y)	Возможность реализации УБПДн	Опасность УБПДн	Актуальность УБПДн
1. Угрозы утечки информации по техническим каналам				
1.1. Угрозы утечки акустической (речевой) информации	0,25	низкая	средняя	неактуальна
1.2. Угрозы утечки видовой информации	0,25	низкая	средняя	неактуальна
1.3. Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	0,25	низкая	средняя	неактуальна
2. Угрозы несанкционированного доступа к персональным данным, обрабатываемым на автоматизированном рабочем месте				
2.1. Угрозы уничтожения, хищения аппаратных средств, носителей информации путем физического доступа к элементам информационных систем персональных данных				
2.1.1. Кража компьютеров	0,25	низкая	средняя	неактуальна
2.1.2. Кража носителей информации	0,25	низкая	средняя	неактуальна
2.1.3. Кража ключей и атрибутов доступа	0,35	низкая	средняя	неактуальна
2.1.4. Кража, модификация, уничтожение информации	0,5	средняя	средняя	актуальна
2.1.5. Вывод из строя узлов информационной системы персональных данных, каналов связи	0,35	низкая	низкая	неактуальна
2.1.6. Несанкционированное отключение средств защиты информации	0,25	низкая	средняя	неактуальна
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств				
2.2.1. Действия вредоносных программ (вирусов)	0,25	низкая	низкая	неактуальна
2.2.2. Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных	0,35	низкая	средняя	неактуальна
2.2.3. Установка программного обеспечения, не связанного с исполнением служебных обязанностей	0,25	низкая	средняя	неактуальна

Тип угроз безопасности персональных данных	Коэффициент реализуемости УБПДн (Y)	Возможность реализации УБПДн	Опасность УБПДн	Актуальность УБПДн
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы персональных данных и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера				
2.3.1. Утрата ключей и атрибутов доступа	0,35	низкая	средняя	неактуальна
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,5	средняя	средняя	актуальна
2.3.3. Непреднамеренное отключение средств защиты информации	0,25	низкая	средняя	неактуальна
2.3.4. Выход из строя аппаратно-программных средств	0,5	средняя	низкая	неактуальна
2.3.5. Сбой системы электроснабжения	0,35	низкая	низкая	неактуальна
2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	0,35	низкая	средняя	неактуальна
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,5	средняя	средняя	актуальна
2.5. Угрозы несанкционированного доступа по каналам связи				
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из информационной системы персональных данных и принимаемой из внешних сетей информации				
2.5.1.1. Перехват за переделами контролируемой зоны	0,35	низкая	средняя	неактуальна
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая	средняя	неактуальна
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями	0,25	низкая	средняя	неактуальна
2.5.2. Угрозы сканирования сети**,** направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.	0,35	низкая	средняя	неактуальна
2.5.3. Угрозы выявления паролей по сети	0,35	низкая	средняя	неактуальна
2.5.4. Угрозы подмены доверенного объекта в сети	0,35	низкая	средняя	неактуальна

Тип угроз безопасности персональных данных	Коэффициент реализуемости УБПДн (Y)	Возможность реализации УБПДн	Опасность УБПДн	Актуальность УБПДн
2.5.5. Угрозы типа «Отказ в обслуживании»	0,35	низкая	низкая	неактуальна
2.5.6. Угрозы удаленного запуска приложений	0,35	низкая	средняя	неактуальна
2.5.7. Угрозы внедрения по сети вредоносных программ	0,25	низкая	низкая	неактуальна

В результате построения модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Муниципальная информационная система поселений «Волость» администрации Первого сельского поселения Главного муниципального района Энской области были выявлены следующие актуальные угрозы:

1. Кража, модификация, уничтожение информации.
2. Непреднамеренная модификация (уничтожение) информации сотрудниками.
3. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке.

4. Формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ

№ п/п	Наименование атаки	Меры, применяемые для нейтрализации атаки	Актуальность атаки
1	**2**	**3**	**4**
Атаки, нейтрализуемые СКЗИ класса КС1			
1.	**Возможность создания способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ.**		актуальна
2.	**Возможность создания способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ.**		актуальна
3.	**Возможность проведения атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона).**	ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.	неактуальна
4.	**Атаки, производимые на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы).**		
4.1.	Внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использо-		актуальна

	ванием вредоносных программ.		
4.2.	Внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.		актуальна
5.	**Атаки, производимые на этапе эксплуатации СКЗИ на:**		
5.1.	Персональные данные.	Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации. В ИСПДн используются «сложные» пароли доступа, осуществляется их периодическая смена, не реже одного раза в 90 дней. Пользователи ИСПДн проинструктированы о недопустимости какой-либо записи парольно-ключевой информации. Аппаратные атрибуты доступа в ИСПДн не используются.	неактуальна
5.2.	Ключевую, аутентифицирующую и парольную информацию СКЗИ.		неактуальна
5.3.	Программные компоненты СКЗИ.		неактуальна
5.4.	Аппаратные компоненты СКЗИ.		неактуальна
5.5.	Программные компоненты СФ, включая программное обеспечение BIOS.		неактуальна
5.6.	Аппаратные компоненты СФ.		неактуальна
5.7.	Данные, передаваемые по каналам связи.	ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.	неактуальна
6.	**Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:**		
6.1.	Общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы).	Информация об информационной системе, в которой используется СКЗИ, в свободном доступе отсутствует	неактуальна
6.2.	Сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ин-		неактуальна

	формационной системе совместно с СКЗИ.		
6.3.	Содержание конструкторской документации на СКЗИ;		неактуальна
6.4.	Содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ.		неактуальна
6.5.	Общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ.		неактуальна
6.6.	Сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи).		неактуальна
6.7.	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами.		неактуальна
6.8.	Сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ.		неактуальна
6.9.	Сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ.		неактуальна
6.10.	Сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.		неактуальна
7.	**Применение:**		
7.1.	Находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ.	ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.	неактуальна
7.2.	Специально разработанных АС и ПО.		актуальна

8.	**Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:**		
8.1.	Каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами.	ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.	неактуальна
8.2.	Каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.	Элементы ИСПДн экранируются несущими стенами здания и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.	неактуальна
9.	**Атаки, проводимые на этапе эксплуатации из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети.**	ИСПДн не имеет подключения к локальным вычислительным сетям, а имеющееся подключение к сети Интернет не постоянно и используется для получения электронной почты. Передача персональных данных через сеть Интернет не осуществляется. В тоже время анализ сетевого трафика требует высокой квалификации нарушителя, наличия специализированного программного обеспечения.	неактуальна
10.	**Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства).**	Информационная система представляет собой автоматизированные рабочие места, расположенные в пределах контролируемой зоны	неактуальна
Атаки, нейтрализуемые СКЗИ класса КС2			
11.	**Возможность проведение атаки при нахождении в пределах контролируемой зоны.**	Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников	неактуальна

		администрации.	
12.	**Возможность проведения атак на этапе эксплуатации СКЗИ на следующие объекты:**		
12.1.	Документацию на СКЗИ и компоненты СФ.	Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации.	неактуальна
12.2.	Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.		неактуальна
13.	**Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации**		
13.1.	Сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы.	Сотрудники администрации, ответственные за организацию обработки, обработку и обеспечение безопасности ПДн, имеют высокую степень профессиональной квалификации, продолжительный стаж работы на текущих должностях и ознакомлены с требованиями действующего законодательства в области обеспечения безопасности ПДн	неактуальна
13.2.	Сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы.		неактуальна
13.3.	Сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.		неактуальна
14.	**Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.**	Для реализации данной меры требуется высокая квалификация нарушителя.	неактуальна
Атаки, нейтрализуемые СКЗИ класса КС3			
15.	**Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.**	Контролируется доступ в помещение с ИСПДн, входные двери закрываются на замок, помещение оборудовано охранной сигнализацией. Посторонние лица находятся в помещении с ИСПДн только в присутствии сотрудников администрации.	неактуальна
16.	**Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.**	Для реализации данной меры требуется высокая квалификация нарушителя.	неактуальна

Атаки, нейтрализуемые СКЗИ класса КВ			
17.	**Возможность создания способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.**	Требуется высокая степень затрат для проведения данных способов атак. В тоже время, информация, функционирующая в ИСПДн, в случае ее раскрытия, модификации, уничтожения, не несет большого ущерба для субъекта ПДн и не представляет собой большой ценности для предполагаемых нарушителей.	неактуальна
18.	**Возможность проведения лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.**		неактуальна
19.	**Возможность проведения работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.**		неактуальна
Атаки, нейтрализуемые СКЗИ класса КА			
20.	**Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.**	Требуется высокая степень затрат для проведения данных способов атак. В тоже время, информация, функционирующая в ИСПДн, в случае ее раскрытия, модификации, уничтожения, не несет большого ущерба для субъекта ПДн и не представляет собой большой ценности для предполагаемых нарушителей.	неактуальна
21.	**Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.**		неактуальна
22.	**Возможность располагать всеми аппаратными компонентами СКЗИ и СФ.**		неактуальна

На основании проведенного анализа, для ИСПДн «Муниципальная информационная система поселений «Волость» актуальны следующие атаки безопасности персональных данных:

- Возможность создания способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ.
- Возможность создания способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ.
- Внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ.
- Внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.
- Применение специально разработанных АС и ПО.

Для нейтрализации имеющихся актуальных угроз, с учетом минимального класса СКЗИ для ИСПДн данного типа, применяются СКЗИ класса **КС1 и выше.**

ПРИЛОЖЕНИЕ 8

Образец сертификата соответствия средства защиты информации Федеральной службы по техническому и экспортному контролю

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Система сертификации
№ РОСС RU.0001.01БИ00

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№

Выдан 16 августа 2013 г.
Действителен до 16 августа 2016 г.

Настоящий сертификат удостоверяет, что **система защиты информации от несанкционированного доступа «** **»**, разработанная и производимая ООО « » в соответствии с техническими условиями , функционирующая под управлением операционных систем, указанных в формуляре , является программным средством защиты информации от несанкционированного доступа и соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **2** уровню контроля и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по **3** классу защищенности при выполнении ограничений по применению, указанных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Лаборатория ППШ» (аттестат аккредитации от 01.03.2004 № СЗИ RU.054.Б01.002) – техническое заключение от , и экспертного заключения от органа по сертификации ЗАО «Научно-производственное объединение «Эшелон» (аттестат аккредитации от 02.12.2010 № СЗИ RU.2321.А101.013).

Заявитель:
Адрес:
Телефон

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ЗАО «Лаборатория ППШ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 16 августа 2013 г.

ПРИЛОЖЕНИЕ 9

Образец сертификата соответствия средства защиты информации Федеральной службы безопасности Российской Федерации

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер _____ от "01" мая 2011 г.

Действителен до "01" мая 2014 г.

Выдан закрытому акционерному обществу «_____».

Настоящий сертификат удостоверяет, что изделие «_____»

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к СКЗИ класса КС3 и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление электронной цифровой подписи для данных, содержащихся в областях оперативной памяти СКЗИ) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований» **сертификационных испытаний образцов продукции** _____

Безопасность информации обеспечивается при использовании изделия, изготовленного в соответствии с техническими условиями _____, выполнении требований правил пользования _____

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **А.Е.Андреечкин**

Настоящий сертификат зарегистрирован в государственный реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев

ПРИЛОЖЕНИЕ 10

Матрица соответствия мер по обеспечению безопасности персональных данных угрозам безопасности персональных данных при их обработке в информационных системах персональных данных

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ИАФ.1	ИАФ.2	ИАФ.3	ИАФ.4	ИАФ.5	ИАФ.6	ИАФ.7
Угрозы от утечки по техническим каналам							
Угрозы утечки акустической (речевой) информации							
Угрозы утечки видовой информации							
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок							
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных							
Кража компьютеров							
Кража носителей информации							
Кража ключей и атрибутов доступа							
Кража, модификация, уничтожение информации							
Вывод из строя узлов информационной системы персональных данных, каналов связи							
Несанкционированное отключение средства защиты информации							
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств							
Действия вредоносных программ (вирусов)							
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных							
Установка программного обеспечения, не связанного с исполнением слу-							✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ИАФ.1	ИАФ.2	ИАФ.3	ИАФ.4	ИАФ.5	ИАФ.6	ИАФ.7
жебных обязанностей							
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера							
Утрата ключей и атрибутов доступа							
Непреднамеренная модификация (уничтожение) информации сотрудниками							
Непреднамеренное отключение средства защиты информации							
Выход из строя аппаратно-программных средств							
Сбой системы электроснабжения							
Угрозы преднамеренных действий внутренних нарушителей							
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓		✓	✓		✓	
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке		✓					✓
Угрозы несанкционированного доступа по каналам связи							
Угроза «Анализ сетевого трафика»							
Перехват за переделами здания							
Перехват в пределах здания внешними нарушителями							
Перехват в пределах здания внутренними нарушителями							

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ИАФ.1	ИАФ.2	ИАФ.3	ИАФ.4	ИАФ.5	ИАФ.6	ИАФ.7
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.							
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях							
Угрозы подмены доверенного объекта							
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях							
Угрозы выявления паролей по сети					✓		
Угрозы типа «Отказ в обслуживании»							
Угрозы удаленного запуска приложений							
Угрозы внедрения по сети вредоносных программ							

Примечание:

ИАФ.1 – Идентификация и аутентификация пользователей, являющихся работниками оператора

ИАФ.2 – Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

ИАФ.3 – Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

ИАФ.4 – Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

ИАФ.5 – Защита обратной связи при вводе аутентификационной информации

ИАФ.6 – Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

ИАФ.7 – Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

II. Управление доступом субъектов доступа к объектам доступа (УПД)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*																
	УПД.1	УПД.2	УПД.3	УПД.4	УПД.5	УПД.6	УПД.7	УПД.8	УПД.9	УПД.10	УПД.11	УПД.12	УПД.13	УПД.14	УПД.15	УПД.16	УПД.17
Угрозы от утечки по техническим каналам																	
Угрозы утечки акустической (речевой) информации																	
Угрозы утечки видовой информации																	
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок																	
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных																	
Кража компьютеров															✓		
Кража носителей информации															✓		
Кража ключей и атрибутов доступа															✓		
Кража, модификация, уничтожение информации											✓				✓		
Вывод из строя узлов информационной системы персональных данных, каналов связи																	
Несанкционированное отключение средства защиты информации																	
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств																	
Действия вредоносных программ (вирусов)																	
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных																	
Установка программного обеспечения, не связанного с исполнением служебных обязанностей		✓		✓	✓												

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*																
	УПД.1	УПД.2	УПД.3	УПД.4	УПД.5	УПД.6	УПД.7	УПД.8	УПД.9	УПД.10	УПД.11	УПД.12	УПД.13	УПД.14	УПД.15	УПД.16	УПД.17
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера																	
Утрата ключей и атрибутов доступа																	
Непреднамеренная модификация (уничтожение) информации сотрудниками		✓															
Непреднамеренное отключение средства защиты информации		✓		✓	✓												
Выход из строя аппаратно-программных средств																	
Сбой системы электроснабжения																	
Угрозы преднамеренных действий внутренних нарушителей																	
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓	✓		✓		✓		✓	✓	✓	✓	✓		✓	✓		✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке			✓				✓							✓	✓		
Угрозы несанкционированного доступа по каналам связи																	
Угроза «Анализ сетевого трафика»			✓										✓	✓			
Перехват за переделами здания			✓										✓	✓			
Перехват в пределах здания внешними нарушителями			✓										✓	✓			
Перехват в пределах здания внутренними нарушителями			✓										✓	✓			
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.			✓											✓			

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*																
	УПД.1	УПД.2	УПД.3	УПД.4	УПД.5	УПД.6	УПД.7	УПД.8	УПД.9	УПД.10	УПД.11	УПД.12	УПД.13	УПД.14	УПД.15	УПД.16	УПД.17
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях			✓										✓	✓		✓	
Угрозы подмены доверенного объекта			✓										✓	✓		✓	
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях			✓										✓	✓		✓	
Угрозы выявления паролей по сети			✓										✓	✓			
Угрозы типа «Отказ в обслуживании»			✓													✓	
Угрозы удаленного запуска приложений			✓											✓		✓	
Угрозы внедрения по сети вредоносных программ														✓			

Примечание:

УПД.1 – Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.

УПД.2 – Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

УПД.3 – Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

УПД.4 – Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

УПД.5 – Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

УПД.6 – Ограничение неуспешных попыток входа в информационную систему доступа к информационной системе.

УПД.7 – Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации.

УПД.8 – Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему.

УПД.9 – Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы.

УПД.10 – Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
УПД.11 – Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.
УПД.12 – Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки.
УПД.13 – Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
УПД.14 – Регламентация и контроль использования в информационной системе технологий беспроводного доступа.
УПД.15 – Регламентация и контроль использования в информационной системе мобильных технических средств.
УПД.16 – Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
УПД.17 – Обеспечение доверенной загрузки средств вычислительной техники.

III. Ограничение программной среды (ОПС)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	ОПС.1	ОПС.2	ОПС.3	ОПС.4
Угрозы от утечки по техническим каналам				
Угрозы утечки акустической (речевой) информации				
Угрозы утечки видовой информации				
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок				
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных				
Кража компьютеров				
Кража носителей информации				
Кража ключей и атрибутов доступа				
Кража, модификация, уничтожение информации				
Вывод из строя узлов информационной системы персональных данных, каналов связи				
Несанкционированное отключение средства защиты информации				

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	ОПС.1	ОПС.2	ОПС.3	ОПС.4
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств				
Действия вредоносных программ (вирусов)				
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных	✓		✓	
Установка программного обеспечения, не связанного с исполнением служебных обязанностей		✓	✓	
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера				
Утрата ключей и атрибутов доступа				
Непреднамеренная модификация (уничтожение) информации сотрудниками				
Непреднамеренное отключение средства защиты информации				
Выход из строя аппаратно-программных средств				
Сбой системы электроснабжения				
Угрозы преднамеренных действий внутренних нарушителей				
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке				✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке				
Угрозы несанкционированного доступа по каналам связи				
Угроза «Анализ сетевого трафика»				
Перехват за переделами здания				
Перехват в пределах здания внешними нарушителями				
Перехват в пределах здания внутренними нарушителями				
Угрозы сканирования сети, направленные на выявление типа или типов				

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	ОПС.1	ОПС.2	ОПС.3	ОПС.4
используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.				
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях				
Угрозы подмены доверенного объекта				
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях				
Угрозы выявления паролей по сети				
Угрозы типа «Отказ в обслуживании»				
Угрозы удаленного запуска приложений				
Угрозы внедрения по сети вредоносных программ				

Примечание:

ОПС.1 – Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения

ОПС.2 – Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

ОПС.3 – Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

ОПС.4 – Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов

IV. Защита машинных носителей информации (ЗНИ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ЗНИ.1	ЗНИ.2	ЗНИ.3	ЗНИ.4	ЗНИ.5	ЗНИ.6	ЗНИ.7	ЗНИ.8
Угрозы от утечки по техническим каналам								
Угрозы утечки акустической (речевой) информации								
Угрозы утечки видовой информации								
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок								
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных								
Кража компьютеров								
Кража носителей информации	✓	✓	✓					
Кража ключей и атрибутов доступа								
Кража, модификация, уничтожение информации		✓	✓					✓
Вывод из строя узлов информационной системы персональных данных, каналов связи								
Несанкционированное отключение средства защиты информации								
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств								
Действия вредоносных программ (вирусов)								
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных								
Установка программного обеспечения, не связанного с исполнением служебных обязанностей								
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера								
Утрата ключей и атрибутов доступа								

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ЗНИ.1	ЗНИ.2	ЗНИ.3	ЗНИ.4	ЗНИ.5	ЗНИ.6	ЗНИ.7	ЗНИ.8
Непреднамеренная модификация (уничтожение) информации сотрудниками								
Непреднамеренное отключение средства защиты информации								
Выход из строя аппаратно-программных средств								
Сбой системы электроснабжения								
Угрозы преднамеренных действий внутренних нарушителей								
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		✓		✓				✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке			✓		✓	✓	✓	✓
Угрозы несанкционированного доступа по каналам связи								
Угроза «Анализ сетевого трафика»								
Перехват за переделами здания								
Перехват в пределах здания внешними нарушителями								
Перехват в пределах здания внутренними нарушителями								
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.								
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях								
Угрозы подмены доверенного объекта								
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях								
Угрозы выявления паролей по сети								
Угрозы типа «Отказ в обслуживании»								

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ЗНИ.1	ЗНИ.2	ЗНИ.3	ЗНИ.4	ЗНИ.5	ЗНИ.6	ЗНИ.7	ЗНИ.8
Угрозы удаленного запуска приложений								
Угрозы внедрения по сети вредоносных программ								

Примечание:
ЗНИ.1 – Учет машинных носителей информации
ЗНИ.2 – Управление доступом к машинным носителям информации
ЗНИ.3 – Контроль перемещения машинных носителей информации за пределы контролируемой зоны
ЗНИ.4 – Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах
ЗНИ.5 – Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.6 – Контроль ввода (вывода) информации на машинные носители информации
ЗНИ.7 – Контроль подключения машинных носителей информации
ЗНИ.8 – Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

V. Регистрация событий безопасности (РСБ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	РСБ.1	РСБ.2	РСБ.3	РСБ.4	РСБ.5	РСБ.6	РСБ.7	РСБ.8
Угрозы от утечки по техническим каналам								
Угрозы утечки акустической (речевой) информации								
Угрозы утечки видовой информации								
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок								
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных								
Кража компьютеров								
Кража носителей информации								
Кража ключей и атрибутов доступа								
Кража, модификация, уничтожение информации	✓	✓	✓	✓	✓	✓	✓	
Вывод из строя узлов информационной системы персональных данных, каналов связи								
Несанкционированное отключение средства защиты информации	✓	✓	✓	✓	✓	✓	✓	
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств								
Действия вредоносных программ (вирусов)	✓	✓	✓	✓	✓	✓	✓	✓
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных								
Установка программного обеспечения, не связанного с исполнением служебных обязанностей	✓	✓	✓	✓	✓	✓	✓	✓
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера								
Утрата ключей и атрибутов доступа								

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	РСБ.1	РСБ.2	РСБ.3	РСБ.4	РСБ.5	РСБ.6	РСБ.7	РСБ.8
Непреднамеренная модификация (уничтожение) информации сотрудниками	✓	✓	✓	✓	✓	✓	✓	✓
Непреднамеренное отключение средства защиты информации	✓	✓	✓	✓	✓	✓	✓	✓
Выход из строя аппаратно-программных средств	✓	✓	✓	✓	✓	✓	✓	✓
Сбой системы электроснабжения								
Угрозы преднамеренных действий внутренних нарушителей								
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓	✓	✓	✓	✓	✓	✓	✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	✓	✓	✓	✓	✓	✓	✓	✓
Угрозы несанкционированного доступа по каналам связи								
Угроза «Анализ сетевого трафика»								
Перехват за переделами здания								
Перехват в пределах здания внешними нарушителями								
Перехват в пределах здания внутренними нарушителями								
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.								
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях								
Угрозы подмены доверенного объекта								
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях								
Угрозы выявления паролей по сети								
Угрозы типа «Отказ в обслуживании»	✓	✓	✓	✓	✓	✓	✓	

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	РСБ.1	РСБ.2	РСБ.3	РСБ.4	РСБ.5	РСБ.6	РСБ.7	РСБ.8
Угрозы удаленного запуска приложений	✓	✓	✓	✓	✓	✓	✓	
Угрозы внедрения по сети вредоносных программ	✓	✓	✓	✓	✓	✓	✓	

Примечание:

РСБ.1 – Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

РСБ.2 – Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

РСБ.3 – Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

РСБ.4 – Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

РСБ.5 – Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

РСБ.6 – Генерирование временных меток и (или) синхронизация системного времени в информационной системе.

РСБ.7 – Защита информации о событиях безопасности.

РСБ.8 – Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17.

VI. Антивирусная защита (АВЗ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	АВЗ.1	АВЗ.2
Угрозы от утечки по техническим каналам		
Угрозы утечки акустической (речевой) информации		
Угрозы утечки видовой информации		
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок		
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных		
Кража компьютеров		
Кража носителей информации		
Кража ключей и атрибутов доступа		
Кража, модификация, уничтожение информации		
Вывод из строя узлов информационной системы персональных данных, каналов связи		
Несанкционированное отключение средства защиты информации		
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств		
Действия вредоносных программ (вирусов)	✓	✓
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных		
Установка программного обеспечения, не связанного с исполнением служебных обязанностей		
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера		
Утрата ключей и атрибутов доступа		

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	АВЗ.1	АВЗ.2
Непреднамеренная модификация (уничтожение) информации сотрудниками		
Непреднамеренное отключение средства защиты информации		
Выход из строя аппаратно-программных средств		
Сбой системы электроснабжения		
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке		
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика»		
Перехват за переделами здания		
Перехват в пределах здания внешними нарушителями		
Перехват в пределах здания внутренними нарушителями		
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.		
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях		
Угрозы подмены доверенного объекта		
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях		
Угрозы выявления паролей по сети		
Угрозы типа «Отказ в обслуживании»		

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	АВЗ.1	АВЗ.2
Угрозы удаленного запуска приложений		
Угрозы внедрения по сети вредоносных программ	✓	✓

Примечание:
АВЗ.1 – Реализация антивирусной защиты
АВЗ.2 – Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

VII. Обнаружение вторжений (СОВ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	СОВ.1	СОВ.2
Угрозы от утечки по техническим каналам		
Угрозы утечки акустической (речевой) информации		
Угрозы утечки видовой информации		
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок		
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных		
Кража компьютеров		
Кража носителей информации		
Кража ключей и атрибутов доступа		
Кража, модификация, уничтожение информации		

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	СОВ.1	СОВ.2
Вывод из строя узлов информационной системы персональных данных, каналов связи		
Несанкционированное отключение средства защиты информации		
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств		
Действия вредоносных программ (вирусов)		
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных		
Установка программного обеспечения, не связанного с исполнением служебных обязанностей		
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера		
Утрата ключей и атрибутов доступа		
Непреднамеренная модификация (уничтожение) информации сотрудниками		
Непреднамеренное отключение средства защиты информации		
Выход из строя аппаратно-программных средств		
Сбой системы электроснабжения		
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке		
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика»		
Перехват за переделами здания		

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*	
	СОВ.1	СОВ.2
Перехват в пределах здания внешними нарушителями		
Перехват в пределах здания внутренними нарушителями		
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.	✓	✓
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях		
Угрозы подмены доверенного объекта		
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях		
Угрозы выявления паролей по сети		
Угрозы типа «Отказ в обслуживании»		
Угрозы удаленного запуска приложений	✓	✓
Угрозы внедрения по сети вредоносных программ	✓	✓

Примечание:
СОВ.1 – Обнаружение вторжений
СОВ.2 – Обновление базы решающих правил

VIII. Контроль (анализ) защищенности информации (АНЗ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	АНЗ.1	АНЗ.2	АНЗ.3	АНЗ.4	АНЗ.5
Угрозы от утечки по техническим каналам					
Угрозы утечки акустической (речевой) информации					
Угрозы утечки видовой информации					
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок					
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных					
Кража компьютеров					
Кража носителей информации					
Кража ключей и атрибутов доступа					✓
Кража, модификация, уничтожение информации					
Вывод из строя узлов информационной системы персональных данных, каналов связи				✓	
Несанкционированное отключение средства защиты информации				✓	
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств					
Действия вредоносных программ (вирусов)					
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных		✓			
Установка программного обеспечения, не связанного с исполнением служебных обязанностей				✓	
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера					
Утрата ключей и атрибутов доступа					✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	АНЗ.1	АНЗ.2	АНЗ.3	АНЗ.4	АНЗ.5
Непреднамеренная модификация (уничтожение) информации сотрудниками					
Непреднамеренное отключение средства защиты информации	✓		✓	✓	
Выход из строя аппаратно-программных средств			✓	✓	
Сбой системы электроснабжения					
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке					✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке					✓
Угрозы несанкционированного доступа по каналам связи					
Угроза «Анализ сетевого трафика»					
Перехват за переделами здания					
Перехват в пределах здания внешними нарушителями					
Перехват в пределах здания внутренними нарушителями					
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.					
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях	✓				
Угрозы подмены доверенного объекта	✓				

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	АНЗ.1	АНЗ.2	АНЗ.3	АНЗ.4	АНЗ.5
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях	✓				
Угрозы выявления паролей по сети					
Угрозы типа «Отказ в обслуживании»	✓				
Угрозы удаленного запуска приложений	✓				
Угрозы внедрения по сети вредоносных программ					

Примечание:

АНЗ.1 – Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

АНЗ.2 – Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

АНЗ.3 – Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

АНЗ.4 – Контроль состава технических средств, программного обеспечения и средств защиты информации

АНЗ.5 – Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

IX. Обеспечение целостности информационной системы и информации (ОЦЛ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ОЦЛ.1	ОЦЛ.2	ОЦЛ.3	ОЦЛ.4	ОЦЛ.5	ОЦЛ.6	ОЦЛ.7	ОЦЛ.8
Угрозы от утечки по техническим каналам								
Угрозы утечки акустической (речевой) информации								
Угрозы утечки видовой информации								

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ОЦЛ.1	ОЦЛ.2	ОЦЛ.3	ОЦЛ.4	ОЦЛ.5	ОЦЛ.6	ОЦЛ.7	ОЦЛ.8
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок								
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных								
Кража компьютеров								
Кража носителей информации								
Кража ключей и атрибутов доступа								
Кража, модификация, уничтожение информации		✓						
Вывод из строя узлов информационной системы персональных данных, каналов связи								
Несанкционированное отключение средства защиты информации								
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств								
Действия вредоносных программ (вирусов)	✓		✓					
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных	✓		✓					
Установка программного обеспечения, не связанного с исполнением служебных обязанностей	✓		✓					
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера								
Утрата ключей и атрибутов доступа								
Непреднамеренная модификация (уничтожение) информации сотрудниками		✓				✓	✓	✓
Непреднамеренное отключение средства защиты информации								
Выход из строя аппаратно-программных средств	✓		✓					

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*							
	ОЦЛ.1	ОЦЛ.2	ОЦЛ.3	ОЦЛ.4	ОЦЛ.5	ОЦЛ.6	ОЦЛ.7	ОЦЛ.8
Сбой системы электроснабжения	✓	✓	✓					
Угрозы преднамеренных действий внутренних нарушителей								
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		✓						
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке		✓			✓	✓	✓	✓
Угрозы несанкционированного доступа по каналам связи								
Угроза «Анализ сетевого трафика»								
Перехват за переделами здания								
Перехват в пределах здания внешними нарушителями								
Перехват в пределах здания внутренними нарушителями								
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.								
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях								
Угрозы подмены доверенного объекта								
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях								
Угрозы выявления паролей по сети								
Угрозы типа «Отказ в обслуживании»				✓				
Угрозы удаленного запуска приложений								
Угрозы внедрения по сети вредоносных программ	✓	✓	✓	✓				

Примечание:

ОЦЛ.1 – Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.2 – Контроль целостности информации, содержащейся в базах данных информационной системы
ОЦЛ.3 – Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4 – Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
ОЦЛ.5 – Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы
ОЦЛ.6 – Ограничение прав пользователей по вводу информации в информационную систему
ОЦЛ.7 – Контроль точности, полноты и правильности данных, вводимых в информационную систему
ОЦЛ.8 – Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях

X. Обеспечение доступности информации (ОДТ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ОДТ.1	ОДТ.2	ОДТ.3	ОДТ.4	ОДТ.5	ОДТ.6	ОДТ.7
Угрозы от утечки по техническим каналам							
Угрозы утечки акустической (речевой) информации							
Угрозы утечки видовой информации							
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок							
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных							
Кража компьютеров							
Кража носителей информации							
Кража ключей и атрибутов доступа							
Кража, модификация, уничтожение информации				✓	✓		
Вывод из строя узлов информационной системы персональных данных, каналов связи		✓	✓	✓	✓	✓	

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ОДТ.1	ОДТ.2	ОДТ.3	ОДТ.4	ОДТ.5	ОДТ.6	ОДТ.7
Несанкционированное отключение средства защиты информации							
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств							
Действия вредоносных программ (вирусов)		✓		✓	✓		
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных							
Установка программного обеспечения, не связанного с исполнением служебных обязанностей							
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера							
Утрата ключей и атрибутов доступа							
Непреднамеренная модификация (уничтожение) информации сотрудниками				✓	✓		
Непреднамеренное отключение средства защиты информации							
Выход из строя аппаратно-программных средств	✓	✓	✓	✓	✓	✓	✓
Сбой системы электроснабжения	✓	✓	✓	✓	✓		✓
Угрозы преднамеренных действий внутренних нарушителей							
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке				✓	✓		
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке				✓	✓		
Угрозы несанкционированного доступа по каналам связи							
Угроза «Анализ сетевого трафика»							
Перехват за переделами здания							
Перехват в пределах здания внешними нарушителями							
Перехват в пределах здания внутренними нарушителями							

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*						
	ОДТ.1	ОДТ.2	ОДТ.3	ОДТ.4	ОДТ.5	ОДТ.6	ОДТ.7
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.							
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях							
Угрозы подмены доверенного объекта							
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях							
Угрозы выявления паролей по сети							
Угрозы типа «Отказ в обслуживании»							
Угрозы удаленного запуска приложений							
Угрозы внедрения по сети вредоносных программ							

Примечание:

ОДТ.1 – Использование отказоустойчивых технических средств

ОДТ.2 – Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы

ОДТ.3 – Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

ОДТ.4 – Периодическое резервное копирование информации на резервные машинные носители информации

ОДТ.5 – Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала

ОДТ.6 – Кластеризация информационной системы и (или) ее сегментов. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ОДТ.7 – Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

XI. Защита среды виртуализации (ЗСВ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*									
	ЗСВ.1	ЗСВ.2	ЗСВ.3	ЗСВ.4	ЗСВ.5	ЗСВ.6	ЗСВ.7	ЗСВ.8	ЗСВ.9	ЗСВ.10
Угрозы от утечки по техническим каналам										
Угрозы утечки акустической (речевой) информации										
Угрозы утечки видовой информации										
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок										
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных										
Кража компьютеров										
Кража носителей информации										
Кража ключей и атрибутов доступа										
Кража, модификация, уничтожение информации			✓		✓	✓		✓		
Вывод из строя узлов информационной системы персональных данных, каналов связи							✓	✓		
Несанкционированное отключение средства защиты информации			✓				✓			
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств										
Действия вредоносных программ (вирусов)			✓				✓	✓	✓	
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных								✓		
Установка программного обеспечения, не связанного с исполнением служебных обязанностей			✓				✓			
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера										
Утрата ключей и атрибутов доступа										

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*									
	ЗСВ.1	ЗСВ.2	ЗСВ.3	ЗСВ.4	ЗСВ.5	ЗСВ.6	ЗСВ.7	ЗСВ.8	ЗСВ.9	ЗСВ.10
Непреднамеренная модификация (уничтожение) информации сотрудниками			✓					✓		
Непреднамеренное отключение средства защиты информации			✓				✓			
Выход из строя аппаратно-программных средств			✓				✓	✓		
Сбой системы электроснабжения			✓				✓	✓		
Угрозы преднамеренных действий внутренних нарушителей										
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓	✓	✓	✓	✓	✓		✓		✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке			✓			✓		✓		
Угрозы несанкционированного доступа по каналам связи										
Угроза «Анализ сетевого трафика»										
Перехват за переделами здания										
Перехват в пределах здания внешними нарушителями										

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*									
	ЗСВ.1	ЗСВ.2	ЗСВ.3	ЗСВ.4	ЗСВ.5	ЗСВ.6	ЗСВ.7	ЗСВ.8	ЗСВ.9	ЗСВ.10
Перехват в пределах здания внутренними нарушителями										
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.										
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях				✓						
Угрозы подмены доверенного объекта				✓						
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях				✓						
Угрозы выявления паролей по сети										
Угрозы типа «Отказ в обслуживании»				✓						
Угрозы удаленного запуска приложений		✓	✓							
Угрозы внедрения по сети вредоносных программ								✓	✓	

Примечание:

ЗСВ.1 – Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

ЗСВ.2 – Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

ЗСВ.3 – Регистрация событий безопасности в виртуальной инфраструктуре

ЗСВ.4 – Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

ЗСВ.5 – Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией

ЗСВ.6 – Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

ЗСВ.7 – Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ.8 – Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9 – Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10 – Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей

XII. Защита технических средств (ЗТС)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	ЗТС.1	ЗТС.2	ЗТС.3	ЗТС.4	ЗТС.5
Угрозы от утечки по техническим каналам					
Угрозы утечки акустической (речевой) информации	✓	✓	✓		
Угрозы утечки видовой информации	✓	✓	✓	✓	
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	✓	✓	✓		
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных					
Кража компьютеров		✓	✓		
Кража носителей информации		✓	✓		
Кража ключей и атрибутов доступа		✓	✓		
Кража, модификация, уничтожение информации		✓	✓	✓	
Вывод из строя узлов информационной системы персональных данных, каналов связи		✓	✓		
Несанкционированное отключение средства защиты информации		✓	✓		
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств					
Действия вредоносных программ (вирусов)					

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	ЗТС.1	ЗТС.2	ЗТС.3	ЗТС.4	ЗТС.5
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных					
Установка программного обеспечения, не связанного с исполнением служебных обязанностей					
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера					
Утрата ключей и атрибутов доступа					
Непреднамеренная модификация (уничтожение) информации сотрудниками					
Непреднамеренное отключение средства защиты информации					
Выход из строя аппаратно-программных средств					✓
Сбой системы электроснабжения					✓
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке			✓	✓	
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке					
Угрозы несанкционированного доступа по каналам связи					
Угроза «Анализ сетевого трафика»					
Перехват за переделами здания					
Перехват в пределах здания внешними нарушителями					
Перехват в пределах здания внутренними нарушителями					

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*				
	ЗТС.1	ЗТС.2	ЗТС.3	ЗТС.4	ЗТС.5
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.					
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях					
Угрозы подмены доверенного объекта					
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях					
Угрозы выявления паролей по сети					
Угрозы типа «Отказ в обслуживании»					
Угрозы удаленного запуска приложений					
Угрозы внедрения по сети вредоносных программ					

Примечание:

ЗТС.1 – Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам

ЗТС.2 – Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

ЗТС.3 – Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены

ЗТС.4 – Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

ЗТС.5 – Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.1	ЗИС.2	ЗИС.3	ЗИС.4	ЗИС.5	ЗИС.6	ЗИС.7	ЗИС.8	ЗИС.9	ЗИС 10	ЗИС 11	ЗИС 12	ЗИС 13	ЗИС 14	ЗИС 15
Угрозы от утечки по техническим каналам															
Угрозы утечки акустической (речевой) информации					✓			✓							
Угрозы утечки видовой информации					✓				✓						
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок															
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных															
Кража компьютеров															
Кража носителей информации														✓	
Кража ключей и атрибутов доступа															
Кража, модификация, уничтожение информации														✓	✓
Вывод из строя узлов информационной системы персональных данных, каналов связи															
Несанкционированное отключение средства защиты информации															✓
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств															
Действия вредоносных программ (вирусов)							✓								
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных															

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.1	ЗИС.2	ЗИС.3	ЗИС.4	ЗИС.5	ЗИС.6	ЗИС.7	ЗИС.8	ЗИС.9	ЗИС 10	ЗИС 11	ЗИС 12	ЗИС 13	ЗИС 14	ЗИС 15
Установка программного обеспечения, не связанного с исполнением служебных обязанностей	✓														
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера															
Утрата ключей и атрибутов доступа															
Непреднамеренная модификация (уничтожение) информации сотрудниками	✓														
Непреднамеренное отключение средства защиты информации	✓														✓
Выход из строя аппаратно-программных средств															
Сбой системы электроснабжения															
Угрозы преднамеренных действий внутренних нарушителей															
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓					✓									
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке												✓	✓		
Угрозы несанкционированного доступа по каналам связи															
Угроза «Анализ сетевого трафика»			✓												
Перехват за переделами здания			✓												
Перехват в пределах здания внешними нарушителями															
Перехват в пределах здания внутренними нарушителями															

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.1	ЗИС.2	ЗИС.3	ЗИС.4	ЗИС.5	ЗИС.6	ЗИС.7	ЗИС.8	ЗИС.9	ЗИС 10	ЗИС 11	ЗИС 12	ЗИС 13	ЗИС 14	ЗИС 15
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.															
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях				✓						✓	✓				
Угрозы подмены доверенного объекта				✓						✓	✓				
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях				✓							✓				
Угрозы выявления паролей по сети			✓				✓								
Угрозы типа «Отказ в обслуживании»		✓													
Угрозы удаленного запуска приложений							✓								
Угрозы внедрения по сети вредоносных программ							✓								

Примечание:

ЗИС.1 – Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы

ЗИС.2 – Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом

ЗИС.3 – Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

ЗИС.4 – Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)

ЗИС.5 – Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

ЗИС.6 – Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами
ЗИС.7 – Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.8 – Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
ЗИС.9 – Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации
ЗИС.10 – Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам
ЗИС.11 – Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12 – Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13 – Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.14 – Использование устройств терминального доступа для обработки информации
ЗИС.15 – Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

(продолжение)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.16	ЗИС.17	ЗИС.18	ЗИС.19	ЗИС.20	ЗИС.21	ЗИС.22	ЗИС.23	ЗИС.24	ЗИС 25	ЗИС 26	ЗИС 27	ЗИС 28	ЗИС 29	ЗИС 30
Угрозы от утечки по техническим каналам															
Угрозы утечки акустической (речевой) информации															
Угрозы утечки видовой информации															

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.16	ЗИС.17	ЗИС.18	ЗИС.19	ЗИС.20	ЗИС.21	ЗИС.22	ЗИС.23	ЗИС.24	ЗИС 25	ЗИС 26	ЗИС 27	ЗИС 28	ЗИС 29	ЗИС 30
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок															
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных															
Кража компьютеров															✓
Кража носителей информации															✓
Кража ключей и атрибутов доступа															✓
Кража, модификация, уничтожение информации															✓
Вывод из строя узлов информационной системы персональных данных, каналов связи											✓				
Несанкционированное отключение средства защиты информации															
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств															
Действия вредоносных программ (вирусов)			✓	✓						✓					
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных			✓												
Установка программного обеспечения, не связанного с исполнением служебных обязанностей															
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера															
Утрата ключей и атрибутов доступа															
Непреднамеренная модификация (уничтожение) информации сотрудниками															

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.16	ЗИС.17	ЗИС.18	ЗИС.19	ЗИС.20	ЗИС.21	ЗИС.22	ЗИС.23	ЗИС.24	ЗИС 25	ЗИС 26	ЗИС 27	ЗИС 28	ЗИС 29	ЗИС 30
Непреднамеренное отключение средства защиты информации														✓	
Выход из строя аппаратно-программных средств											✓			✓	
Сбой системы электроснабжения															
Угрозы преднамеренных действий внутренних нарушителей															
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		✓			✓	✓									✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	✓		✓												
Угрозы несанкционированного доступа по каналам связи															
Угроза «Анализ сетевого трафика»					✓			✓	✓						
Перехват за переделами здания					✓			✓	✓						
Перехват в пределах здания внешними нарушителями					✓			✓	✓						
Перехват в пределах здания внутренними нарушителями									✓						
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.					✓			✓	✓	✓		✓	✓		
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях					✓							✓	✓		
Угрозы подмены доверенного объекта					✓							✓	✓		
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях					✓							✓	✓		
Угрозы выявления паролей по сети					✓			✓	✓			✓	✓		

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*														
	ЗИС.16	ЗИС.17	ЗИС.18	ЗИС.19	ЗИС.20	ЗИС.21	ЗИС.22	ЗИС.23	ЗИС.24	ЗИС 25	ЗИС 26	ЗИС 27	ЗИС 28	ЗИС 29	ЗИС 30
Угрозы типа «Отказ в обслуживании»							✓	✓	✓			✓	✓		
Угрозы удаленного запуска приложений								✓				✓	✓		
Угрозы внедрения по сети вредоносных программ												✓			

Примечание:

ЗИС.16 – Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов

ЗИС.17 – Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

ЗИС.18 – Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения

ЗИС.19 – Изоляция процессов (выполнение программ) в выделенной области памяти

ЗИС.20 – Защита беспроводных соединений, применяемых в информационной системе

ЗИС.21 – Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.22 – Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.23 – Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.24 – Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.25 – Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды). Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.26 – Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.27 – Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.28 – Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.29 – Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

ЗИС.30 – Защита мобильных технических средств, применяемых в информационной системе. Данная мера предусмотрена только приказом ФСТЭК России от 11 февраля 2013 года № 17

XIV. Выявление инцидентов и реагирование на них (ИНЦ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*					
	ИНЦ.1	ИНЦ.2	ИНЦ.3	ИНЦ.4	ИНЦ.5	ИНЦ.6
Угрозы от утечки по техническим каналам						
Угрозы утечки акустической (речевой) информации	✓	✓	✓	✓	✓	✓
Угрозы утечки видовой информации	✓	✓	✓	✓	✓	✓
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	✓	✓	✓	✓	✓	✓
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных						
Кража компьютеров	✓	✓	✓	✓	✓	✓
Кража носителей информации	✓	✓	✓	✓	✓	✓
Кража ключей и атрибутов доступа	✓	✓	✓	✓	✓	✓
Кража, модификация, уничтожение информации	✓	✓	✓	✓	✓	✓
Вывод из строя узлов информационной системы персональных данных, каналов связи	✓	✓	✓	✓	✓	✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*					
	ИНЦ.1	ИНЦ.2	ИНЦ.3	ИНЦ.4	ИНЦ.5	ИНЦ.6
Несанкционированное отключение средства защиты информации	✓	✓	✓	✓	✓	✓
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств						
Действия вредоносных программ (вирусов)	✓	✓	✓	✓	✓	✓
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных	✓	✓	✓	✓	✓	✓
Установка программного обеспечения, не связанного с исполнением служебных обязанностей	✓	✓	✓	✓	✓	✓
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера						
Утрата ключей и атрибутов доступа	✓	✓	✓	✓	✓	✓
Непреднамеренная модификация (уничтожение) информации сотрудниками	✓	✓	✓	✓	✓	✓
Непреднамеренное отключение средства защиты информации	✓	✓	✓	✓	✓	✓
Выход из строя аппаратно-программных средств	✓	✓	✓	✓	✓	✓
Сбой системы электроснабжения	✓	✓	✓	✓	✓	✓
Угрозы преднамеренных действий внутренних нарушителей						
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓	✓	✓	✓	✓	✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	✓	✓	✓	✓	✓	✓
Угрозы несанкционированного доступа по каналам связи						
Угроза «Анализ сетевого трафика»	✓	✓	✓	✓	✓	✓
Перехват за переделами здания	✓	✓	✓	✓	✓	✓
Перехват в пределах здания внешними нарушителями	✓	✓	✓	✓	✓	✓
Перехват в пределах здания внутренними нарушителями	✓	✓	✓	✓	✓	✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*					
	ИНЦ.1	ИНЦ.2	ИНЦ.3	ИНЦ.4	ИНЦ.5	ИНЦ.6
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.	✓	✓	✓	✓	✓	✓
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях	✓	✓	✓	✓	✓	✓
Угрозы подмены доверенного объекта	✓	✓	✓	✓	✓	✓
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях	✓	✓	✓	✓	✓	✓
Угрозы выявления паролей по сети	✓	✓	✓	✓	✓	✓
Угрозы типа «Отказ в обслуживании»	✓	✓	✓	✓	✓	✓
Угрозы удаленного запуска приложений	✓	✓	✓	✓	✓	✓
Угрозы внедрения по сети вредоносных программ	✓	✓	✓	✓	✓	✓

Примечание:

Все перечисленные ниже меры предусмотрены только приказом ФСТЭК России от 18 февраля 2013 года № 21

ИНЦ.1 – Определение лиц, ответственных за выявление инцидентов и реагирование на них

ИНЦ.2 – Обнаружение, идентификация и регистрация инцидентов

ИНЦ.3 – Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами

ИНЦ.4 – Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

ИНЦ.5 – Принятие мер по устранению последствий инцидентов

ИНЦ.6 – Планирование и принятие мер по предотвращению повторного возникновения инцидентов

XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	УКФ.1	УКФ.2	УКФ.3	УКФ.4
Угрозы от утечки по техническим каналам				
Угрозы утечки акустической (речевой) информации	✓	✓	✓	✓
Угрозы утечки видовой информации	✓	✓	✓	✓
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	✓	✓	✓	✓
Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных, носителей информации путем физического доступа к элементам информационной системы персональных данных				
Кража компьютеров	✓	✓	✓	✓
Кража носителей информации	✓	✓	✓	✓
Кража ключей и атрибутов доступа	✓	✓	✓	✓
Кража, модификация, уничтожение информации	✓	✓	✓	✓
Вывод из строя узлов информационной системы персональных данных, каналов связи	✓	✓	✓	✓
Несанкционированное отключение средства защиты информации	✓	✓	✓	✓
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств				
Действия вредоносных программ (вирусов)	✓	✓	✓	✓
Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных	✓	✓	✓	✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	УКФ.1	УКФ.2	УКФ.3	УКФ.4
Установка программного обеспечения, не связанного с исполнением служебных обязанностей	✓	✓	✓	✓
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационной системы и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и стихийного характера				
Утрата ключей и атрибутов доступа	✓	✓	✓	✓
Непреднамеренная модификация (уничтожение) информации сотрудниками	✓	✓	✓	✓
Непреднамеренное отключение средства защиты информации	✓	✓	✓	✓
Выход из строя аппаратно-программных средств	✓	✓	✓	✓
Сбой системы электроснабжения	✓	✓	✓	✓
Угрозы преднамеренных действий внутренних нарушителей				
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	✓	✓	✓	✓
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	✓	✓	✓	✓
Угрозы несанкционированного доступа по каналам связи				
Угроза «Анализ сетевого трафика»	✓	✓	✓	✓
Перехват за переделами здания	✓	✓	✓	✓
Перехват в пределах здания внешними нарушителями	✓	✓	✓	✓
Перехват в пределах здания внутренними нарушителями	✓	✓	✓	✓
Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и др.	✓	✓	✓	✓

	Меры защиты информации в информационных системах органов государственной власти и местного самоуправления, предусмотренные приказами ФСТЭК России *(см. примечание к таблице)*			
	УКФ.1	УКФ.2	УКФ.3	УКФ.4
Угрозы внедрения ложного объекта, как в информационных системах персональных данных, так и во внешних сетях	✓	✓	✓	✓
Угрозы подмены доверенного объекта	✓	✓	✓	✓
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях	✓	✓	✓	✓
Угрозы выявления паролей по сети	✓	✓	✓	✓
Угрозы типа «Отказ в обслуживании»	✓	✓	✓	✓
Угрозы удаленного запуска приложений	✓	✓	✓	✓
Угрозы внедрения по сети вредоносных программ	✓	✓	✓	✓

Примечание:

Все перечисленные ниже меры предусмотрены только приказом ФСТЭК России от 18 февраля 2013 года № 21

УКФ.1 – Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных

УКФ.2 – Управление изменениями конфигурации информационной системы и системы защиты персональных данных

УКФ.3 – Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных

УКФ.4 – Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

Приложение 11

Примерный образец требований к системе защиты персональных данных в информационной системе персональных данных органа местного самоуправления

УТВЕРЖДАЮ

Глава администрации Первого сельского поселения Главного муниципального района Энской области

_____ А.Б. Ветров
« 29 » января 2014 года

ТРЕБОВАНИЯ
к системе защиты персональных данных информационной системы персональных данных «Муниципальная информационная система поселений «Волость»

В соответствии с перечнем обрабатываемых персональных данных и информационных систем персональных данных администрации Первого сельского поселения Главного муниципального района Энской области, утвержденного распоряжением от 17 января 2014 года № 2-р, в информационной системе персональных данных «Муниципальная информационная система поселений «Волость» (далее – ИСПДн) осуществляется обработка персональных данных категории «иные». На основании положения части 1 статьи 13 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ИСПДн является государственной информационной системой.

Для ИСПДн установлен 4 уровень защищенности персональных данных и класс защищенности – К4 (акт классификации утвержден главой администрации Первого сельского поселения Главного муниципального района Энской области 21 января 2014 года).

Согласно «Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 года № 17, к ИСПДн предъявляется следующий базовый состав мер защиты информации:

Усл. обозначение	Меры защиты информации в информационных системах
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

Усл. обозначение	Меры защиты информации в информационных системах
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

Согласно разработанной модели угроз безопасности персональных данных при их обработке в ИСПДн (утверждена главой администрации Пер-

вого сельского поселения Главного муниципального района Энской области 27 января 2014 года) были выявлены следующие актуальные угрозы:

1. Кража, модификация, уничтожение информации.
2. Непреднамеренная модификация (уничтожение) информации сотрудниками.
3. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

Исходя из перечня выявленных актуальных угроз безопасности персональных данных, сформирован следующий адаптированный базовый набор мер защиты, которые необходимо реализовать в ИСПДн:

Усл. обозначение	Меры защиты информации в информационных системах
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

Усл. обозначение	Меры защиты информации в информационных системах
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Для выполнения адаптированного базового набора мер защиты ИСПДн и нейтрализации выявленных актуальных угроз безопасности персональных данных, обрабатываемых в ИСПДн, необходимо применение комплекса организационных и технических мер:

1. Установить на все рабочие места ИСПДн средство защиты от несанкционированного доступа к информации, сертифицированное ФСТЭК России по требованиям безопасности информации и настроить его с целью выполнения мер из адаптивного базового набора по:

управлению доступом субъектов доступа к объектам доступа;

регистрации событий безопасности.

2. Определить лицо, ответственное за учет, хранение и уничтожение машинных носителей персональных данных в администрации.

3. Регламентировать и организовать учет, хранение и уничтожение машинных носителей персональных данных в администрации.

4. Регламентировать и организовать контроль доступа в помещения администрации, в которых ведется обработка персональных данных.

5. Разработка документов, определяющих политику в отношении обработки персональных данных и регламентирующих обработку и обеспечение безопасности персональных данных в администрации.

6. Довести до сведения сотрудников администрации положения законодательства Российской Федерации в области персональных данных, документов администрации по вопросам обработки и обеспечения безопасности персональных данных, требований к защите персональных данных.

7. Регламентация и проведение внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Заместитель руководителя департамента
информационных технологий Энской области –
начальник отдела информационных ресурсов И.И. Иванов

ПРИЛОЖЕНИЕ 12

Образец лицензии Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации

СЕРИЯ КИ 0092 НОМЕР

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер от 31 октября 2002 г.

Лицензия предоставлена Обществу с ограниченной ответственностью

« »

(ООО « »)

ОГРН . ИНН

Адрес места нахождения:

Адрес места осуществления лицензируемой деятельности:

Перечень работ и услуг, на которые распространяется настоящая лицензия:

контроль защищенности конфиденциальной информации от утечки по техническим каналам в: средствах и системах информатизации; технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается; помещениях со средствами (системами), подлежащими защите; защищаемых помещениях;

контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

аттестационные испытания и аттестация на соответствие требованиям по защите информации: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;

проектирование в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;

установка, монтаж, испытания, ремонт средств защиты информации: технических средств защиты информации; защищенных технических средств обработки информации; технических средств контроля эффективности мер защиты информации; программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля защищенности информации.

Лицензия переоформлена
на основании приказа ФСТЭК России от 9 ноября 2012 г. № 242-л
Лицензия действует бессрочно

Начальник 1 управления

м.п. И.Назаров

ПРИЛОЖЕНИЕ 13

Примерный образец распоряжения о вводе в эксплуатацию информационных систем персональных данных в органе местного самоуправления

АДМИНИСТРАЦИЯ
Первого сельского поселения

РАСПОРЯЖЕНИЕ

« 31 » января 2014 года № 6-р

с. Первое

О вводе в эксплуатацию информационных систем персональных данных

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами:

1. Ввести в эксплуатацию для обработки сведений, содержащих персональные данные, следующие информационные системы персональных данных администрации Первого сельского поселения Главного муниципального района Энской области:

«Зарплата и управление персоналом»;

«Муниципальная информационная система поселений «Волость».

2. Все работы, связанные с обработкой сведений, содержащих персональные данные в информационных системах, осуществлять в соответствии с документами администрации Первого сельского поселения Главного муниципального района, определяющими политику в отношении обработки персональных данных.

3. Контроль за исполнением настоящего распоряжения возложить на главного бухгалтера администрации Первого сельского поселения Главного муниципального района Энской области Барсукову А.А.

Глава администрации Первого сельского
Поселения Главного муниципального района
Энской области А.Б. Ветров

ПРИЛОЖЕНИЕ 14

Примерный образец уведомления территориального органа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций об обработке (о намерении осуществлять обработку) персональных данных органа государственной власти

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных технологий
и массовых коммуникаций по Энской области

111000, г. Энск, ул. Неизвестная, д. 1

УВЕДОМЛЕНИЕ
об обработке (о намерении осуществлять обработку)
персональных данных

Наименование (фамилия, имя, отчество) оператора:
Департамент информационных технологий Энской области (ДИТ Энской области) (далее - Департамент),
Адрес оператора
Адрес местонахождения: 111000, г. Энск, пл. Ленина, д. 1.
Почтовый адрес: 111000, г. Энск, пл. Ленина, д. 1.
Контактная информация оператора:
телефон: +7(255)255-55-55;
факс: +7(255)255-55-55;
адрес электронной почты: iivanov@ensk.ru.
ИНН: 3612345678.
Коды: ОГРН 1133612345678; Дата выдачи ОГРН 01-01-2000; ОКВЭД 123456789; ОКПО 987654321; ОКФС 123456789; ОКОГУ 987654321; ОКОПФ 123456789.
Правовое основание обработки персональных данных
руководствуясь статьями 23 и 24 Конституции Российской Федерации, статьями 85 – 90 Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», положениями, инструкциями и учредительными документами, определяющими деятельность Департамента.
Цель обработки персональных данных:
реализация трудовых отношений, предоставление государственных услуг и осуществления государственных функций.
Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона «О персональных данных»:

Приказом департамента информационных технологий Энской области:

– Иванов И.И. – заместитель руководителя департамента – начальник отдела информационных ресурсов назначен ответственным за организа-

цию обработки персональных данных в департаменте информационных технологий Энской области;

- Петров А.А. – начальник отдела информационной безопасности назначен ответственным за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области;
- Петров А.А. – начальник отдела информационной безопасности назначен ответственным за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям.

Данным приказом также утверждены должностные инструкции ответственных лиц.

Соответствующими приказами департамента

- утверждены перечни обрабатываемых персональных данных и информационных систем персональных данных;
- утверждены перечни должностей сотрудников и лиц их замещающих, служебные обязанности которых предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным, список лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

Отдельным приказом Департамента утверждены правила обработки персональных данных, которые:

- определяют цели обработки персональных данных;
- описывают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- регламентируют допуск сотрудников к персональным данным и их получение;
- определяют обязанности сотрудников, допущенных к обработке персональных данных;
- устанавливают категории субъектов, персональные данные которых обрабатываются и содержание обрабатываемых персональных данных;
- устанавливают сроки обработки, хранения и уничтожения персональных данных;
- устанавливают порядок рассмотрения запросов субъектов персональных данных или их представителей;
- устанавливают порядок работы с обезличенными данными;
- устанавливают порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;
- устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Правила обработки персональных данных размещены на официальном сайте Департамента в сети «Интернет».

Регламент учета, хранения и уничтожения машинных носителей персональных данных в департаменте информационных технологий Энской области утвержден приказом департамента.

Сотрудники департамента, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

средства обеспечения безопасности:

В качестве средств защиты информации используются только те средства, которые прошли в установленном порядке процедуру оценки соответствия требованиям безопасности информации и имеют соответствующие сертификаты ФСТЭК России и ФСБ России.

Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ:

С целью обеспечения безопасности персональных данных в Департаменте для всех используемых в Департаменте информационных систем персональных данных (далее – ИСПДН) в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, определены уровни защищенности персональных данных. Для ИСПДн, являющихся государственными информационными системами, в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17 дополнительно определены классы защищенности.

Для всех ИСПДН определены угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных, приняты необходимые организационные и технические меры по обеспечению безопасности персональных данных. Защита ИСПДН, использующих средства криптографической защиты информации осуществляется в соответствии с требованиями приказа ФСБ России от 10.07.2014 г. № 378.

Дата начала обработки персональных данных: 01.04.2009.

Срок или условие прекращения обработки персональных данных: прекращение деятельности.

Сведения об информационной системе № 1:

Категории персональных данных

осуществляет обработку следующих категорий персональных данных: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; ме-

сто рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы;
специальные категории персональных данных: расовая принадлежность; национальная принадлежность; политические взгляды; религиозные убеждения; философские убеждения; состояние здоровья;
а также:
гражданство; владение иностранными языками; судимость; допуск к государственной тайне; выполняемая работа с начала трудовой деятельности; награды и знаки отличия; близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес); пребывание за границей; отношение к воинской обязанности; воинское звание (военный билет); номер телефона; документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан); наличие заграничного паспорта (серия, номер, кем и когда выдан); номер страхового свидетельства обязательного пенсионного страхования; идентификационный номер налогоплательщика.
Категории субъектов, персональные данные которых обрабатываются принадлежащих: сотрудникам (бывшим сотрудникам) Департамента, руководителям подведомственных Департаменту учреждений, кандидатам на замещение вакантных должностей и на включение в кадровый резерв Департамента, гражданам, обратившимся в Департамент.
Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: получение (сбор), хранение, систематизация, накопление, уточнение (обновление, изменение), копирование, использование, уничтожение;
обработка вышеуказанных персональных данных будет осуществляться путем: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;
осуществление трансграничной передачи персональных данных: не осуществляется.
Сведения о местонахождении базы данных информации, содержащей персональные данные граждан РФ:
страна: Россия;
адрес ЦОДа: г. Энск, пл. Ленина, д. 1;
собственный ЦОД: да.
Сведения об информационной системе № 2:
Категории персональных данных
осуществляет обработку следующих категорий персональных данных: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы;
специальные категории персональных данных: расовая принадлежность; национальная принадлежность; политические взгляды; религиозные убеждения; философские убеждения; состояние здоровья;
а также:

гражданство; владение иностранными языками; судимость; допуск к государственной тайне; выполняемая работа с начала трудовой деятельности; награды и знаки отличия; близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес); пребывание за границей; отношение к воинской обязанности; воинское звание (военный билет); номер телефона; документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан); наличие заграничного паспорта (серия, номер, кем и когда выдан); номер страхового свидетельства обязательного пенсионного страхования; идентификационный номер налогоплательщика.

Категории субъектов, персональные данные которых обрабатываются принадлежащих: сотрудникам (бывшим сотрудникам) Департамента, руководителям подведомственных Департаменту учреждений, кандидатам на замещение вакантных должностей и на включение в кадровый резерв Департамента, гражданам, обратившимся в Департамент.

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: получение (сбор), хранение, систематизация, накопление, уточнение (обновление, изменение), копирование, использование, уничтожение.

Обработка вышеуказанных персональных данных будет осуществляться путем: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет.

Осуществление трансграничной передачи персональных данных: не осуществляется.

Сведения о местонахождении базы данных информации, содержащей персональные данные граждан РФ:

страна: Россия;

адрес ЦОДа: г. Энск, пл. Ленина, д. 1;

собственный ЦОД: да.

Использование шифровальных (криптографических) средств: используются.

Наименование используемых криптографических средств: Программный комплекс ViPNet Client 3.2 КС3;

класс СКЗИ: КС3.

Категории персональных данных

осуществляет обработку следующих категорий персональных данных: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы;

специальные категории персональных данных: расовая принадлежность; национальная принадлежность; политические взгляды; религиозные убеждения; философские убеждения; состояние здоровья;

а также:

гражданство; владение иностранными языками; судимость; допуск к государственной тайне; выполняемая работа с начала трудовой деятельности;

награды и знаки отличия; близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес); пребывание за границей, отношение к воинской обязанности, воинское звание (военный билет), номер телефона, документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан); наличие заграничного паспорта (серия, номер, кем и когда выдан); номер страхового свидетельства обязательного пенсионного страхования; идентификационный номер налогоплательщика.

Категории субъектов, персональные данные которых обрабатываются принадлежащих: сотрудникам (бывшим сотрудникам) Департамента, руководителям подведомственных Департаменту учреждений, кандидатам на замещение вакантных должностей и на включение в кадровый резерв Департамента, гражданам, обратившимся в Департамент.

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: получение (сбор), хранение, систематизация, накопление, уточнение (обновление, изменение), копирование, использование, уничтожение.

обработка вышеуказанных персональных данных будет осуществляться путем: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет;

осуществление трансграничной передачи персональных данных: не осуществляется.

Сведения о местонахождении базы данных информации, содержащей персональные данные граждан РФ:

страна: Россия;

адрес ЦОДа: г. Энск, пл. Ленина, д. 1;

собственный ЦОД: да .

Ответственный за организацию обработки персональных данных: Иванов Иван Иванович;

номера контактных телефонов, почтовые адреса и адреса электронной почты:

+7(255)255-55-55, +7(255)255-55-55, iivanov@ensk.ru.

Документ сформирован на портале Роскомнадзора
Номер уведомления: **111111**, ключ: **22222222**

Руководитель департамента		А.Б. Ветров
(должность)	(подпись)	(расшифровка подписи)

"___" января 2014 г.

Исполнитель: Заместитель руководителя департамента информационных технологий Энской области Иванов И.И.;
Контактная информация исполнителя: +7 (255) 255 55 55.

ПРИЛОЖЕНИЕ 15

Примерный образец заявления о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных органа государственной власти

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных технологий
и массовых коммуникаций по Энской области

111000, г. Энск, ул. Неизвестная, д. 1

Заявление
о предоставлении выписки из реестра операторов,
осуществляющих обработку персональных данных

Департамент информационных технологий Энской области (ИНН 361234567890 ОГРН 1133612345678) (далее – Департамент), расположенный по адресу 111000, г. Энск, пл. Ленина, д. 1, в лице руководителя А.Б. Ветрова, действующего на основании Положения о Департаменте, утвержденного постановлением правительства Энской области от 15 января 2011 года № 25 «Об утверждении положения о департаменте информационных технологий Энской области».

Сведения о запрашиваемом операторе: ИНН 361234567890, регистрационный номер записи в реестре – № 1276.

Руководитель управления информационных
технологий Энской области А.Б. Ветров

«__» января 2014 года

ПРИЛОЖЕНИЕ 16

Примерный образец информационного письма о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных органа государственной власти

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных технологий
и массовых коммуникаций по Энской области

111000, г. Энск, ул. Неизвестная, д. 1

Информационное письмо
о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных

Наименование (фамилия, имя, отчество) оператора:
Департамент информационных технологий Энской области (ДИТ Энской области) (далее - Департамент),
Адрес оператора:
Адрес местонахождения: 111000, г. Энск, пл. Ленина, д. 1.
Почтовый адрес: 111000, г. Энск, пл. Ленина, д. 1.
Регистрационный номер записи в Реестре: 11-11-111111.
Основания изменений: реорганизация оператора – постановление правительства Энской области от 15 января 2014 года № 11.
ИНН: 3612345678.
Коды: ОГРН 1133612345678; ОКВЭД 123456789; ОКПО 987654321; ОКФС 123456789; ОКОГУ 987654321; ОКОПФ 123456789.
Правовое основание обработки персональных данных
руководствуясь статьями 23 и 24 Конституции Российской Федерации, статьями 85 – 90 Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», положениями, инструкциями и учредительными документами, определяющими деятельность Департамента.
Цель обработки персональных данных
с целью реализация трудовых отношений, предоставление государственных услуг и осуществления государственных функций.
Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона «О персональных данных»:

Приказом департамента информационных технологий Энской области:

- Иванов И.И. – заместитель руководителя департамента – начальник отдела информационных ресурсов назначен ответственным за организацию обработки персональных данных в департаменте информационных технологий Энской области;
- Петров А.А. – начальник отдела информационной безопасности назначен ответственным за обеспечение безопасности персональных дан-

ных, обрабатываемых в информационных системах персональных данных департамента информационных технологий Энской области;

- Петров А.А. – начальник отдела информационной безопасности назначен ответственным за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям.

Данным приказом также утверждены должностные инструкции ответственных лиц.

Соответствующими приказами департамента

- утверждены перечни обрабатываемых персональных данных и информационных систем персональных данных;
- утверждены перечни должностей сотрудников и лиц их замещающих, служебные обязанности которых предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным, список лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

Отдельным приказом Департамента утверждены правила обработки персональных данных, которые:

- определяют цели обработки персональных данных;
- описывают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- регламентируют допуск сотрудников к персональным данным и их получение;
- определяют обязанности сотрудников, допущенных к обработке персональных данных;
- устанавливают категории субъектов, персональные данные которых обрабатываются и содержание обрабатываемых персональных данных;
- устанавливают сроки обработки, хранения и уничтожения персональных данных;
- устанавливают порядок рассмотрения запросов субъектов персональных данных или их представителей;
- устанавливают порядок работы с обезличенными данными.
- устанавливают порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;
- устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Правила обработки персональных данных размещены на официальном сайте Департамента в сети «Интернет».

Регламент учета, хранения и уничтожения машинных носителей персональных данных в департаменте информационных технологий Энской области утвержден приказом департамента.

Сотрудники департамента, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства

Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

средства обеспечения безопасности:

В качестве средств защиты информации используются только те средства, которые прошли в установленном порядке процедуру оценки соответствия требованиям безопасности информации и имеют соответствующие сертификаты ФСТЭК России и ФСБ России.

Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ:

С целью обеспечения безопасности персональных данных в Департаменте для всех используемых в Департаменте информационных систем персональных данных (далее – ИСПДН) в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, определены уровни защищенности персональных данных. Для ИСПДн, являющихся государственными информационными системами, в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17 дополнительно определены классы защищенности.

Для всех ИСПДН определены угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных, приняты необходимые организационные и технические меры по обеспечению безопасности персональных данных. Защита ИСПДН, использующих средства криптографической защиты информации осуществляется в соответствии с требованиями приказа ФСБ России от 10.07.2014 г. № 378.

Дата начала обработки персональных данных: 01.04.2009.

Срок или условие прекращения обработки персональных данных: прекращение деятельности.

Сведения об информационной системе:

Категории персональных данных

осуществляет обработку следующих категорий персональных данных: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы;

специальные категории персональных данных:

расовая принадлежность; национальная принадлежность; политические взгляды; религиозные убеждения; философские убеждения; состояние здоровья;

а также:

гражданство; владение иностранными языками; судимость; допуск к государственной тайне; выполняемая работа с начала трудовой деятельности; награды и знаки отличия; близкие родственники (степень родства, фамилия,

имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес); пребывание за границей, отношение к воинской обязанности, воинское звание (военный билет); номер телефона; документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан); наличие заграничного паспорта (серия, номер, кем и когда выдан); номер страхового свидетельства обязательного пенсионного страхования; идентификационный номер налогоплательщика.

Категории субъектов, персональные данные которых обрабатываются принадлежащих: сотрудникам (бывшим сотрудникам) Департамента, руководителям подведомственных Департаменту учреждений, кандидатам на замещение вакантных должностей и на включение в кадровый резерв Департамента, гражданам, обратившимся в Департамент.

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: получение (сбор), хранение, систематизация, накопление, уточнение (обновление, изменение), использование, уничтожение.

Обработка вышеуказанных персональных данных будет осуществляться путем: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет.

Осуществление трансграничной передачи персональных данных: не осуществляется.

Сведения о местонахождении базы данных информации, содержащей персональные данные граждан РФ:

страна: Россия;

адрес ЦОДа: г. Энск, пл. Ленина, д. 1;

собственный ЦОД: да;

использование шифровальных (криптографических) средств: используются.

Наименование используемых криптографических средств: Программный комплекс ViPNet Client 3.2 КС3;

класс СКЗИ: КС3.

Ответственный за организацию обработки персональных данных: Иванов Иван Иванович,

номера контактных телефонов, почтовые адреса и адреса электронной почты: +7(255)255-55-55, iivanov@ensk.ru.

Документ сформирован на портале Роскомнадзора
Номер уведомления: **111111**, ключ: **22222222**

Руководитель департамента		А.Б. Ветров
(должность)	(подпись)	(расшифровка подписи)

"___" января 2014 г.

Исполнитель: Заместитель руководителя департамента информационных технологий Энской области Иванов И.И.;
Контактная информация исполнителя: +7 (255) 255 55 55.

ПРИЛОЖЕНИЕ 17

Примерный образец заявления об исключении сведений об операторе из реестра операторов, осуществляющих обработку персональных данных органа государственной власти

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных технологий
и массовых коммуникаций по Энской области

Заявление
об исключении сведений об операторе из реестра операторов, осуществляющих обработку персональных данных

Департамент информационных технологий Энской области (ИНН 361234567890 ОГРН 1133612345678) (далее – Департамент), расположенный по адресу 111000, г. Энск, пл. Ленина, д. 1, в лице руководителя А.Б. Ветрова, действующего на основании Положения о департаменте, утвержденного указом губернатора Энской области от 15 января 2011 года № 25-у.

Сведения об операторе: ИНН 361234567890, ОГРН 1133612345678, регистрационный номер записи в реестре – 1276.

Основание исключения из реестра: – реорганизация оператора – указ губернатора Энской области от 15 января 2014 года № 11-у.

Руководитель департамента
информационных технологий Энской области А.Б. Ветров

«___» января 2014 года

СОДЕРЖАНИЕ

Учебное издание

МЕЩЕРЯКОВ Владимир Алексеевич,
ЖЕЛЕЗНЯК Владимир Петрович, БОНДАРЬ Артём Олегович,
РЯПОЛОВ Константин Яковлевич, ВЯЛЫХ Сергей Ариевич

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ОРГАНИЗАЦИЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ

Учебно-методическое пособие

Подписано в печать 11.01.2016 г. Формат $60\times84^{1}/_{16}$. Печать электрографическая.
Гарнитура «Таймс». Усл. печ. л. 13. Уч.-изд. л. 12,09.

Отпечатано в множительном бюро правительства Воронежской области.
394018, г. Воронеж, пл. Ленина, 1