Рекомендации
по организации работ
в образовательных учреждениях
городского округа Тольятти,
обеспечивающих выполнения требований
законодательства Российской Федерации
при обработке персональных данных

МОУДПОС Центр информационных технологий
Тольятти
2009

СОДЕРЖАНИЕ

В настоящие рекомендации включены материалы, касающиеся практического применения законодательства Российской Федерации в области обработки персональных данных.

Адресовано руководителям образовательных учреждений, заместителям руководителей образовательных учреждений, в ведении которых находятся вопросы информатизации и информационной безопасности, а также специалистам по информационной безопасности.

Тексты статей законов РФ, а также выдержки из нормативной документации приведены в соответствии с оригиналами и актуальны на момент выпуска настоящих рекомендаций.

Приведенный в рекомендациях перечень законов и нормативных документов, которыми регламентируется обработка персональных данных, постоянно изменяется и дополняется.

Необходимо обратить особое внимание на то, что в рекомендациях описываются лишь общие случаи применения законодательства, в котором имеет место множество оговорок и исключений для частных случаев обработки персональных данных ведомствами, различными юридическими и физическими лицами, а актуальность документов требует подтверждения на момент их использования.

Данный документ подготовлен специалистами МОУДПОС Центра информационных технологий г. о. Тольятти на основе Памятки, составленной специалистами Центра информационной безопасности Курского ГТУ с их письменного разрешения на использование.

Обозначения по тексту:

- *курсив* – цитаты из законодательства;
- подчеркивание – обратить особое внимание.

Данные рекомендации носят общий характер, могут редактироваться в соответствии с изменениями требований Российского законодательства.

1. СФЕРА ДЕЙСТВИЯ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Федеральный закон № 152-ФЗ «О персональных данных» в статье 1 устанавливает следующую сферу действия:

Статья 1. *Сфера действия настоящего Федерального закона*

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее – государственные органы), органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами (далее – муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Данная статья определяет:

- перечень органов и лиц, подпадающих под действие федерального закона;
- условия обработки персональных данных.

Если перечень органов и лиц не вызывает вопросов, то из условий следует, что Федеральный закон направлен на определение порядка обработки персональных данных средствами автоматизации.

Часть 3 статьи 4 Федерального закона № 152-ФЗ «О персональных данных» устанавливает особенности обработки персональных данных, осуществляемой без использования средств автоматизации:

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

В соответствии с Распоряжением Правительства РФ № 1055-р, особенности порядка обработки персональных данных без использования средств автоматизации разработаны Мининформсвязи, Минэкономразвития и ФМС России в первом квартале 2008 г. Постановлением Правительства РФ от 15 сентября 2008 года № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

В Положении дается следующее определение неавтоматизированной обработки ПДн:

1. Обработка персональных данных, содержащихся в информационной системе персо-

нальных данных либо извлеченных из такой системы (далее – персональные данные), 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.

2. 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 нее.

Особое внимание стоит уделить определению понятия «обработка персональных данных», данному в части 3 статьи 3 Федерального закона № 152-ФЗ «О персональных данных»: *обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.*

2. СВЕДЕНИЯ, ОТНОСЯЩИЕСЯ К ПЕРСОНАЛЬНЫМ ДАННЫМ

В соответствии с ФЗ № 152-ФЗ «О персональных данных»:

Статья 3:

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Статья 8:

...В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Статья 10:

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

В статье 85 Федерального закона № 197-ФЗ «Трудовой кодекс Российской Федерации» имеется определение персональных данных работника и понятия обработки: *Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Обработка персональных данных работника – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника*.

3. ПЕРЕЧЕНЬ ЗАКОНОВ И НОРМАТИВНЫХ ДОКУМЕНТОВ, РЕГЛАМЕНТИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Работа с персональными данными регламентируется следующими основными документами:

- «Конституция Российской Федерации» от 12.12.93 г.;
- Указ Президента РФ от 06.03.97 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Федеральный закон от 27.07.06 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 30.12.01 г. № 197-ФЗ «Трудовой кодекс Российской Федерации» (Глава 14);
- Федеральный закон от 27.07.06 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 17.11.07 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Россвязьохранкультуры от 28.03.08 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных»;
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.08 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Указ Президента РФ от 17.03.08 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Указ Президента РФ от 30.05.05 г. № 609 «Об утверждении положения о персональных данных государственного гражданского служащего российской Федерации и ведении его личного дела»;
- Постановление Правительства РФ от 03.11.94 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- Распоряжение Правительства Российской Федерации от 15.08.07 г. № 1055-р «Об утверждении плана подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.08 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без

использования средств автоматизации»;

- Федеральный закон от 10.01.02 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральный закон от 10.01.03 г. № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы»;
- Федеральный закон от 19.12.05 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон Российской Федерации от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»;
- Постановление Правительства РФ от 06.07.08 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Распоряжение Президента РФ от 10.07.01 г. № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;
- Приказ Россвязькомнадзора от 17.07.08 г. № 08 «Об утверждении образца формы уведомления об обработке персональных данных»;
- Приказ ФСБ Российской Федерации от 09.02.05 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- другие законодательные акты.

Техническая защита персональных данных регламентируется следующими основными документами:

- Федеральный закон от 08.08.01 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»;
- Постановление Правительства РФ от 26.01.06 г. № 45 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства от 15.08.06 г. РФ № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- «Положение о государственном лицензировании деятельности в области защиты информации», решение Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27.04.94 г. № 10;
- «Положение об аттестации объектов информатизации по требованиям безопасности информации», утверждено Председателем Государственной технической комиссии при Президенте РФ 25.11.94 г.;

- Постановление Правительства РФ от 26.06.95 г. № 608 «О сертификации средств защиты информации»;
- «Положение о сертификации средств защиты информации по требованиям безопасности информации», приказ Председателя Гостехкомиссии России от 27.10.95 г. № 199;
- Указ Президента РФ от 03.04.95 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;
- Указ Президента РФ от 16.08.04 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
- Методические материалы ФСТЭК. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (документ ДСП – для служебного пользования);
- Методические материалы ФСТЭК. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (документ ДСП);
- Методические материалы ФСТЭК. «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года (документ ДСП);
- Методические материалы ФСТЭК. «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (документ ДСП);
- Методические материалы ФСБ. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 года;
- Методические материалы ФСБ. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» от 21 февраля 2008 года;
- Другие документы ФСБ и ФСТЭК России по обеспечению безопасности конфиденциальной (персональные данные) информации; другие законодательные акты.

Нормативно-правовая база по смежным направлениям:

- Закон от 07.07.93 г. № 5341-1 «Об архивном фонде Российской Федерации и архивах»;
- Федеральный закон от 02.03.07 г. № 25-ФЗ «О муниципальной службе в Российской

Федерации»;

- Постановление Государственного Комитета Российской Федерации по стандартизации и метрологии от 06.11.01 г. № 454-ст «О принятии и введении в действие ОКВЭД»;
- Материалы Минэкономразвития России «О создании системы персонального учета населения Российской Федерации»;
- Распоряжение Правительства Российской Федерации от 09.06.05 г. № 748-р «Концепция создания системы персонального учета населения Российской Федерации»;
- Указ Президента РФ от 12.03.07 г. № 320 «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»;
- Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;
- Приказ Федеральной Службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 19.03.08 г. № 128 «Об утверждении административного регламента Федеральной Службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия по исполнению государственной функции по рассмотрению обращений операторов связи по вопросам присоединения сетей электросвязи и взаимодействия операторов связи, принятию по ним решений и выдаче предписаний в соответствии с федеральным законом»;
- Федеральный закон от 03.04.95 г. № 40-ФЗ «О федеральной службе безопасности»;
- Руководящий нормативный документ МВД России, утвержденный Заместителем Министра внутренних дел России «РД 78.143-92. Системы и комплексы охранной сигнализации, элементы технической укрепленности объектов. Нормы проектирования»;
- Руководящий документ ГУВО МВД России «Р 78.36.007-99. Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. Рекомендации»;
- Государственный стандарт РФ ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения», утвержденный Постановлением Госстандарта РФ № 28 от 27.02.98 г.;
- «Квалификационный справочник должностей руководителей, специалистов и других служащих», утвержденный Постановлением Минтруда РФ от 21.08.98 г. № 37;
- «Правила устройства электроустановок», утвержденные приказом Минпромэнерго России;
- другие законодательные акты.

Меры ответственности за нарушение требований в части защиты персональных данных отражены в следующих документах:

- Федеральный закон от 30.12.01г. № 197-ФЗ (с изменениями) «Трудовой кодекс Россий-

ской Федерации»;

- Федеральный закон от 13.06.96 г. № 63-ФЗ (с изменениями) «Уголовный кодекс Российской Федерации»;
- Федеральный закон от 30.12.01 г. № 195-ФЗ (с изменениями) «Кодекс Российской Федерации об административных правонарушениях»;
- В субъектах РФ и ведомствах издаются подзаконные акты по работе с персональными данными.

4. ДЕЙСТВИЯ ОРГАНИЗАЦИИ В ПЛАНЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В общем случае для обработки персональных данных в организации необходимо:

1. Уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации;
2. Оформить правовое основание обработки персональных данных (см. ниже гл. 5);
3. Разработать документы, регламентирующие обработку персональных данных в организации (положение по обработке персональных данных, регламенты, положения по защите персональных данных и т. д., см. Приложение 2);
4. Создать систему защиты информационной системы персональных данных;
5. Выполнить требования по инженерной защите помещений, пожарной безопасности, охране, электропитанию и заземлению, санитарные и экологические требования;
6. Провести аттестацию по требованиям безопасности информации; организовать повышение квалификации сотрудников в области защиты персональных данных.

Подробнее об этих этапах, а также о законодательных основаниях на их проведение, изложено далее.

Официальным разрешением обработки персональных данных в организации с использованием средств автоматизации является наличие в организации двух документов: «Аттестата по требованиям безопасности информации» и выписки из приказа о внесении организации в Реестр Операторов или выписка из этого Реестра.

5. ЧТО ЯВЛЯЕТСЯ ОСНОВАНИЕМ ДЛЯ ЗАКОННОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ?

5.1. Виды экономической деятельности, заявляемые хозяйствующими субъектами при регистрации в учредительных документах

В соответствии со статьей 22 ФЗ № 152-ФЗ «О персональных данных», организация должна иметь правовое основание на обработку персональных данных:

3. Уведомление, предусмотренное частью 1 настоящей статьи, должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения: 5) правовое основание обработки персональных данных; Таким основанием могут являться коды ОКВЭД.

В подтверждение этого в инструкции по заполнению Уведомления Приказа Россвязькомнадзора № 08 «Об утверждении образца формы уведомления об обработке персональных данных» имеется… рекомендация *использовать… ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).*

В соответствии с Постановлением Госстандарта России № 454-ст «О принятии и введении в действие ОКВЭД»:

Общероссийский классификатор видов экономической деятельности ОК 029-2007 (КДЕС Ред. 1.1) ...применяется при решении задач, связанных с:

- классификацией и кодированием видов экономической деятельности, заявляемых хозяйствующими субъектами при регистрации.

Приложение А к ОКВЭД включает в себя описание видов экономической деятельности, которые соответствуют характеру действий при обработке персональных данных:

72.30. Обработка данных. Эта группировка включает в себя:

- все стадии обработки данных, включая подготовку и ввод данных, с применением технического и программного обеспечения потребителя или собственного;

- предоставление услуг по обеспечению информационной безопасности вычислительных систем и сетей;

72.40. Деятельность по созданию и использованию баз данных и информационных ресурсов. Эта группировка включает в себя:

- проектирование баз данных (разработку концепций, структуры, состава баз данных);

- формирование и ведение баз данных, в том числе сбор данных из одного или более источников, а также ввод, верификацию и актуализацию данных;

- администрирование баз данных, в том числе обеспечение возможности доступа к базе

данных в режиме непосредственного или телекоммуникационного доступа;

- *поиск данных, их отбор и сортировку по запросам, предоставление отобранных данных пользователям, в том числе в режиме непосредственного доступа;*

- *создание информационных ресурсов различных уровней (федеральных, ведомственных, корпоративных, ресурсов предприятий).*

Таким образом, в учредительные документы (Положение, Устав) необходимо внести соответствующие виды деятельности, которые будут являться правовым основанием для обработки персональных данных в организации.

5.2. Какие документы необходимо разработать в организации?

С учетом требований руководящих документов различного уровня и личного мнения авторов, с целью стандартизации подходов к созданию внутренней нормативной базы организации, регулирующей обработку и защиту персональных данных, предлагается создать строго регламентированный перечень организационно-распорядительной документации (ОРД), а также требования к ее содержанию.

Возможный рабочий вариант структуры ОРД и примерных вопросов, которые должны быть отражены в документах, предлагается в Приложении 1.

Часть указанных документов разрабатывается специализированными организациями, имеющими лицензии в области защиты информации, и регламентируется руководящими документами федеральных органов исполнительной власти. Создание остальных документов осуществляется на основании требований Федерального закона № 152-ФЗ «О персональных данных», постановлений правительства, президента, федеральных органов исполнительной власти, в части, их касающейся. Кроме этих документов, в организации должны быть разработаны различные формы в рамках положений и регламентов, а также другие документы.

Попытаемся разобраться, какие документы нужны оператору для организации работы по защите персональных данных, чтобы быть, в том числе, готовым к проверкам, которые проводятся уполномоченным органом в соответствии с требованиями законодательства.

Прежде всего, это документы, связанные с получением согласия физических лиц на обработку их персональных данных.

Кроме определенных случаев, перечисленных в ФЗ № 152-ФЗ, обработка персональных данных может осуществляться только с согласия субъекта персональных данных. Согласие обязательно должно быть дано в письменном виде, если:

- персональные данные включаются в общедоступные источники;

- оператором обрабатываются специальные (раса, национальность, политические взгляды, религиозные убеждения, состояние здоровья, интимной жизни), биометрические персональ-

ные данные (характерные физиологические особенности).

Кроме того, письменное согласие субъекта требуется в случае:

- любой передачи (распространении) его персональных данных;
- запрашивания любых персональных данных субъекта у третьего лица;
- принятия оператором решения, порождающего юридические последствия в отношении субъекта персональных данных;
- трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных.

Требования к форме письменного согласия установлены ФЗ № 152-ФЗ (п. 4 ст. 9).

Однако имеют место случаи, когда законодатель, обязывая оператора получить согласие субъекта, не прописывает обязанность получить его именно в письменном виде. При этом в случае проверки уполномоченным органом или спорной ситуации в суде оператор остается «крайней стороной», так как, согласно ФЗ № 152-ФЗ (ч. 3 ст. 9), именно оператор «обязан предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных». На практике это выражается в том, что крупные операторы, работающие с субъектами в массовом порядке (банки, сетевые маркетинговые фирмы), не отказываются от возможности подтвердить согласие клиентов на обработку их персональных данных в устном виде (разговоры записываются), в виде принятия определенных условий и проставлении подписи субъекта на рекламных бланках. Таким образом, кроме риска «доказывания» подлинности такого согласия, в случаях, когда от субъекта требуют только подтверждение факта согласия, ничего не объясняя, остается риск несоответствия формы такого согласия принципам ФЗ № 152-ФЗ, в которых заложено право субъекта персональных данных давать согласие «в своем интересе» и знать с самого начала цель обработки, способы обработки, перечень обрабатываемых данных и сроки обработки (п. 1 ст. 18 ФЗ № 152-ФЗ).

Не требуется согласия субъекта в случае, если его персональные данные общедоступны. Но и в этом вопросе не все просто. Если оператор обрабатывает такие персональные данные, то в его арсенале также должен быть документ, подтверждающий, что источник является «общедоступным» и у «источника» есть письменное согласие субъекта (ст. 8 и п. 3 ст. 9 ФЗ № 152-ФЗ). Например, документом, подтверждающим «общедоступность», может быть распечатка страницы сайта с персональными данными, которые обрабатывает оператор. Каждый конкретный случай обработки общедоступных данных требует индивидуального подхода в решении вопросов документального подтверждения факта «общедоступности» источника. При этом оператор должен провести предварительную работу и «типизировать» обрабатываемые персональные данные, чтобы использовать эту информацию для разработки типового

подхода к решению вопроса о подтверждении «общедоступности» источника.

Другой важный аспект, связанный с защитой персональных данных, – наличие в организации нормативного документа, аккумулирующего информацию о персональных данных, обрабатываемых оператором.

Наличие такого документа, во-первых, устанавливается требованием Трудового кодекса (ст. 88 ТК: «Передача персональных данных работника должна осуществляться в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись»), во-вторых, в ФЗ «О персональных данных» заложена обязанность оператора направить в уполномоченный орган по защите прав субъектов персональных данных уведомление об обработке персональных данных (ст. 22 ФЗ № 152-ФЗ). Согласно этой обязанности, оператор должен уже до того, как подаст уведомление по форме (ч. 3 ст. 22), закрепить в своей организации механизм организации работы со всеми обрабатываемыми персональными данными, а именно: сформулировать цель обработки, категории обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, правовые основания обработки, перечень действий с персональными данными, описание способов их обработки, мер, которые оператор осуществляет с целью обеспечения безопасности; зафиксировать дату начала обработки, срок или условие ее прекращения. В связи с тем что эти критерии с течением времени изменяются, такой документ в организации должен быть также изменяем.

Согласно ст. 22 п. 2 ФЗ № 152-ФЗ и гл. 14 ТК, можно сформировать перечень операторов, которым не нужно формально иметь такой документ (они не обрабатывают персональные данные работников и не обязаны по закону подавать уведомления в уполномоченный орган):

- те операторы, которые работают с персональными данными субъекта в связи с заключением и исполнением договоров, стороной которого является субъект персональных данных;

- операторы, обрабатывающие общедоступные персональные данные (либо только фамилии, имена, отчества субъектов персональных данных);

- операторы, являющиеся общественными объединениями (религиозными организациями), действующими в соответствии с законодательством РФ и обрабатывающими персональные данные своих членов (участников) для достижения законных целей, предусмотренных учредительными документами;

- операторы федеральных автоматизированных информационных систем, государственных информационных систем персональных данных, созданных в целях защиты безопасности государства и общественного порядка;

- операторы, обрабатывающие персональные данные без использования средств автоматизации, но в соответствии с федеральными законами (иными правовыми актами

РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке).

Перечень таких операторов является исчерпывающим.

Но можно ли утверждать, что перечисленные категории операторов могут в своей деятельности обойтись без документа, аккумулирующего информацию о персональных данных, обрабатываемых оператором? В этой связи необходимость такого документа обусловлена тем, что всем операторам необходимо, в первую очередь, для себя, закрепить документально основные понятия обработки конкретных персональных данных субъектов, так как:

Во-первых, у него есть обязанность представить субъекту персональных данных на основании обращения либо запроса, информацию, касающуюся обработки его персональных данных, в том числе:

- цель обработки;
- способы обработки;
- сведения о лицах, имеющих доступ к персональным данным;
- перечень обрабатываемых персональных данных;
- источник получения;
- сроки обработки и хранения персональных данных.

Предоставить субъекту такого рода информацию оперативно можно только на основании уже существующих документов, где планомерно изложены принципы и критерии обработки, иначе, например, операторы мобильной связи, выдавая ответы на обращения одного и того же субъекта в силу большого количества обрабатываемых персональных данных, могут дать противоречивый (по сравнению с предыдущим) ответ.

Во-вторых, необходимость анализа всех обрабатываемых организацией персональных данных и аккумулирования этой информации в едином документе (назовем его по аналогии с ТК «Положением о персональных данных») обусловлена требованием к технической защите обрабатываемых оператором персональных данных. Поясним. Приказом ФСТЭК, ФСБ и Мининформтехнологии от 13.02.08 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» при классификации информационных систем с целью определения уровня их защиты и степени расходования средств организации на техническую защиту персональных данных субъектов учитываются категории обрабатываемых персональных данных и их объем. Соответственно, возникает необходимость фиксировать и документировать такую информацию.

В-третьих, формулирование в Положении, в частности, понятия цели обработки, поможет оператору обосновать в спорных ситуациях отсутствие согласия субъекта персональных данных в случаях, когда такая возможность предусмотрена ФЗ № 152-ФЗ (ч. 2 ст. 6), потому что

законодатель, описывая такие случаи, привязывает их описание к понятию «цель обработки».

В-четвертых, проверяющий уполномоченный орган, выясняя причину нарушения тех или иных положений законодательства в сфере персональных данных, будет ориентироваться, в первую очередь, на соблюдение принципов ФЗ № 152-ФЗ (ст. 5), которые могут быть проверены только на основании документа (документов) по организации защиты персональных данных.

Для того чтобы единый документ об обработке персональных данных в организации «предвосхитил» все вопросы, которые могут возникнуть у уполномоченного органа, необходим предварительный анализ всей документации оператора, которая содержит персональные данные субъектов.

В свою очередь, при проведенного такого анализа и составлении текста Положения необходимо учитывать возможность типизации ПДн. К примеру, когда оператор обрабатывает персональные данные субъектов с единой целью (оператор связи с целью предоставления услуги связи), в Положении должны быть четко сформулированы понятия цели, способов, перечня обрабатываемых персональных данных и др. А в случаях, когда оператор обрабатывает персональные данные, преследуя различные цели, к примеру, обрабатывая данные работников для начисления заработной платы, установления пропускного режима, учета в кадровом делопроизводстве, возникает потребность их типизировать относительно цели обработки, и это может быть отражено в Положении. Такая система описания (например, относительно критерия цели обработки) позволит оператору эффективно ориентироваться в документах, содержащих персональные данные, давать ответы на запросы субъектов и уполномоченного органа.

Другим вопросом, имеющим отношение к документации оператора персональных данных, является вопрос о сроках хранения документов и информации, содержащей персональные данные. В данном случае законодательство, пожалуй, впервые устанавливает для информации и документов максимальный, и к тому же условный срок хранения – «по достижении целей обработки». Организации должны будут установить сроки хранения документов, содержащих персональные данные, причем необходимо заранее продумать обоснование выбранных сроков хранения. В противном случае организация сама может «подставить» себя: цели будут выполнены, а персональные данные не будут уничтожены, то есть при формулировании цели обработки необходимо закладывать возможность хранения документа в организации, допустим, для хранения. К примеру, первичные учетные документы, регистры бухгалтерского учета и бухгалтерская отчетность хранятся оператором в течение периода, который установлен в соответствии с правилами организации государственного архивного дела, но не менее пяти лет (п. 1 ст. 17 Закона о бухгалтерском учете). В случае самостоятельного хранения оператором учетных документов, регистров бухгалтерского учета

и бухгалтерской отчетности, формулировка цели обработки должна учитывать срок их хранения внутри организации, то есть пятилетний срок.

Таким образом, можно предложить операторам следующую схему организации защиты персональных данных: при наличии единого управленческого звена – руководство вопросами организации защиты персональных данных – в организации необходимо создать два направления по формированию обеспечения защиты обрабатываемых персональных данных: техническое направление и направление «нетехнической» защиты, обязанности которой, в свою очередь, можно перераспределить по структурным подразделениям согласно целям обработки (например, защита персональных данных в кадровом делопроизводстве), в контрольно-пропускной системе, юридическом структурном подразделении (при учете договоров с субъектами персональных данных). При этом внутренним документом (должностной инструкцией) должна быть установлена персональная ответственность работников этих направлений за надлежащую защиту персональных данных.

В Приложении 2 приведено примерное содержание некоторых документов:

- Положение о персональных данных;
- Положение об организации и проведении работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- Требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- Вопросы, которые необходимо отразить в Специальном технологическом регламенте;
- Заявление о согласии работника на обработку персональных данных;
- Заявление о согласии работника на получение/передачу персональных данных от третьей стороны/третьей стороне;
- Соглашение о неразглашении персональных данных сотрудников, учащихся и воспитанников;
- Заявление о согласии родителей (законных представителей) на обработку их персональных данных и данных ребенка;
- Заявление о согласии родителей (законных представителей) на получение/передачу их персональных данных и данных ребенка от третьей стороны/третьей стороне;
- Форма Акта классификации ИСПДн.

5.3. Уведомление об обработке персональных данных с использованием средств автоматизации

В соответствии с частью 1 статьи 22 ФЗ № 152-ФЗ «О персональных данных» организация обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных с использованием

средств автоматизации: *1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.*

Сведения, которые необходимо указать в Уведомлении, и порядок его подачи определяются частью 3 статьи 22 ФЗ № 152-ФЗ «О персональных данных», Приказом Россвязьохранкультуры № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных» и Приказом Россвязькомнадзора № 08 «Об утверждении образца формы уведомления об обработке персональных данных» (последний приказ за последний год менялся не менее трех раз).

В Приказе Россвязькомнадзора № 08 «Об утверждении образца формы уведомления об обработке персональных данных» приводятся Рекомендации по заполнению образца формы уведомления об обработке персональных данных.

В качестве справочного материала Приказ Россвязькомнадзора № 08, форма Уведомления и Рекомендации из данного Приказа приведены в Приложении 3.

Обращаем внимание, что в Рекомендациях, из-за несогласованности действий федеральных органов исполнительной власти, в пункте, касающегося описания мер по обеспечению безопасности персональных данных, следует правильно указывать следующие сведения: «Аттестация по требованиям безопасности информации» (основание будет разъяснено далее).

В части 2 статьи 22 ФЗ № 152-ФЗ «О персональных данных» указаны случаи, когда не требуется уведомлять уполномоченный орган контроля:

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

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) 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.

Отсюда следует, что для работы с персональными данными сотрудников и с персональными данными в бумажном виде уведомление не требуется.

Приказ Россвязьохранкультуры от 28.03.2008 № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных», определяет порядок внесения оператора в Реестр:

8. По результатам проверки сведений, содержащихся в обработанном Уведомлении, Служба в течение тридцати дней с даты поступления Уведомления принимает решение о включении Оператора в Реестр, которое оформляется в виде приказа руководителя Службы или заместителя руководителя Службы о включении Оператора в Реестр.

9. На основании изданного приказа в Реестр вносится запись об Операторе, которой присваивается регистрационный номер.

10. Датой внесения Оператора в Реестр считается дата подписания приказа.

11. Информация о внесении Оператора в Реестр должна быть опубликована на официальном сайте Службы в Интернете не позднее трех дней с даты подписания приказа.

Этот же Приказ регулирует порядок исключения оператора из Реестра: *18. Вопрос об исключении Оператора из Реестра рассматривается в следующих случаях:*

- поступление в Службу или ее территориальные управления письменного заявления (обращения) от Оператора, включенного в Реестр, об исключении с приложением обоснований;

- принятие Службой или ее территориальными управлениями мер по приостановлению или прекращению Оператором обработки персональных данных, осуществляемой с нарушением требований закона.

19. Операторы исключаются из Реестра при наступлении одного из следующих условий:

- ликвидация Оператора;

- прекращение деятельности Оператора в результате его реорганизации, за исключением реорганизации в форме преобразования;

- аннулирование лицензии на осуществление лицензируемой деятельности Оператора, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

- наступление срока или условия прекращения обработки персональных данных, указанных в Уведомлении;

- решение суда о прекращении оператором деятельности по обработке персональных данных;

- иные установленные законодательством Российской Федерации в области персональных данных.

20. Решение об исключении Оператора из Реестра оформляется приказом руководителя Службы или заместителя руководителя Службы.

На основании изданного приказа в Реестр вносятся сведения об исключении Оператора из Реестра. После исключения Оператора из Реестра регистрационный номер соответствующей записи в дальнейшем не используется.

21. Информация об исключении Оператора из Реестра должна быть опубликована на официальном сайте Службы в сети Интернет не позднее трех дней с даты подписания приказа.

На основании вышеприведенных статей можно заключить, что включение оператора в Реестр – есть разрешение на обработку персональных данных средствами автоматизации. Кроме того, в них указаны нарушения, которые лишают организацию права на обработку персональных данных средствами автоматизации.

В связи с тем, что правоохранительные органы с недоверием относятся к сведениям, отраженным в Интернете, рекомендуется запросить выписку из приказа о внесении в Реестр Операторов или выписку из Реестра.

Заполненное Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронном виде и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации в территориальные управления Россвязьохранкультуры (Роскомнадзора), на подведомственной территории которых оператор осуществляет (будет осуществлять) обработку персональных данных.

Приказом Россвязьохранкультуры (Роскомнадзора) определены территориальные органы, осуществляющие внесение сведений об операторах в Реестр:

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (www.rsoc.ru)	
Управление Роскомнадзора по Самарской области	
Почтовый адрес	443099, г. Самара, ул. А. Толстого, 118
Телефон, факс, e-mail учреждения	Телефон: (846) 3325326, факс: (846) 2704400, e-mail ugnsi@smr.ru
Сайт	http://63.rsoc.ru

5.4. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 1 статьи 19 Федерального закона № 152-ФЗ «О персональных данных» оператор обязан проводить мероприятия по обеспечению безопасности персональных данных при их обработке:

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

Часть 2 статьи 19 Федерального закона № 152-ФЗ «О персональных данных» определяет:

2. Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

В статьях 3, 9 и 18 Постановления Правительства РФ № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» указаны федеральные органы исполнительной власти, определяющие требования к мероприятиям по безопасности персональных данных:

3. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

9. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

18. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

В «Положении об особенностях обработки персональных данных, осуществляемой без использования средства автоматизации» (утв. Постановлением Правительства РФ № 687) о мерах по обеспечению безопасности ПДн, при их обработке без использования средств автоматизации в главах 13 – 15, сказано:

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

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

6. КТО МОЖЕТ ПРОВОДИТЬ РАБОТЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Согласно требованиям статьи 17 Федерального закона № 128-ФЗ «О лицензировании отдельных видов деятельности», деятельность по технической защите конфиденциальной информации подлежит обязательному лицензированию:

1. В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности:

5) деятельность по распространению шифровальных (криптографических) средств;

6) деятельность по техническому обслуживанию шифровальных (криптографических) средств;

7) предоставление услуг в области шифрования информации;

8) разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

9) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

10) деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

11) деятельность по технической защите конфиденциальной информации.

Постановление Правительства РФ № 45 «Об организации лицензирования отдельных видов деятельности» определяет Перечень федеральных органов исполнительной власти, осуществляющих лицензирование в областях:

ФСТЭК России: деятельность по технической защите конфиденциальной информации;

ФСТЭК России, ФСБ России: деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

ФСБ России:

- Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

- Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, ко-

гда указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- Деятельность по распространению шифровальных (криптографических) средств;

- Деятельность по техническому обслуживанию шифровальных (криптографических) средств;

- Предоставление услуг в области шифрования информации;

- Разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем.

Постановление Правительство РФ № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» определяет порядок и условия выполнения работ по технической защите конфиденциальной информации.

В Положении о ФСТЭК (в ред. Указов Президента РФ от 30.11.2006 г. № 1321, от 23.10.2008 г. № 1517, от 17.11.2008 г. № 1625) говорится:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (далее – ключевые системы информационной инфраструктуры), в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям (далее – безопасность информации в ключевых системах информационной инфраструктуры);

(пп. 1 в ред. Указа Президента РФ от 30.11.2006 г. № 1321)

2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее – противодействие техническим разведкам);

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации);

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

2. ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

(в ред. Указа Президента РФ от 30.11.2006 г. № 1321).

В соответствии со статьей 11.2 Федерального закона № 40-ФЗ «О Федеральной службе безопасности», обязанности по обеспечению информационной безопасности возлагаются на органы Федеральной службы безопасности Российской Федерации в пределах их полномочий:

1) при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

2) при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

Таким образом, для выполнения работ по обеспечению безопасности персональных данных при их обработке требуется получение лицензий ФСТЭК и ФСБ России. В целях реализации оператором обязанности по обеспечению безопасности персональных данных при их обработке с применением технических мер и использованием шифровальных (криптографических) средств, требуется оформление лицензий или обращение в организации, имеющие лицензии и аккредитованные ФСТЭК/ФСБ России в системе сертификации средств защиты информации в соответствии с требованиями безопасности информации для проведения аттестации объектов информатизации.

6.1. Техническая защита персональных данных при их обработке в информационных системах персональных данных

В соответствии с изложенным выше, основным регулирующим органом по организации безопасности персональных данных является ФСТЭК России, которая в «Основных мероприятиях по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утвержденных Заместителем директора ФСТЭК России 15.02.08 г.) предписывает: *3.11. На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:*

…Оценка соответствия ИСПДн требованиям безопасности ПДн.

… проводится:

- для ИСПДн 1-го и 2-го классов – обязательная сертификация (аттестация) по требованиям безопасности информации;

- для ИСПДн 3-го класса – декларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению оператора);

- для ИСПДн 4-го класса оценка соответствия проводится по решению оператора.

В соответствии с Федеральным законом № 184-ФЗ «О техническом регулировании» и Постановлением Госстандарта России от 30 июля 2002 г. № 64 «О номеклатуре продукции и услуг (работ), подлежащих обязательной сертификации, и номенклатуре продукции, соответствие которой может быть подтверждено декларацией о соответствии», на данный момент законодательной базы «обязательного декларирования соответствия» услуг не существует.

На основании этого можно сделать вывод, что документом, подтверждающим выполнение требований безопасности персональных данных при их обработке с использованием средств автоматизации и дающим право на внесение в Реестр Операторов, является «Аттестат соответствия по требованиям безопасности информации».

6.2. Инженерная защита помещений, требования по пожарной безопасности, охране, электропитанию и заземлению, санитарные и экологические требования

Основным регулятором в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств, в соответствии со статьей 11.2 Федерального закона № 40-ФЗ «О Федеральной службе безопасности», является ФСБ России.

В настоящее время для использования в работе доступны два документа:

- Методические материалы ФСБ. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 года.
- Методические материалы ФСБ. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» от 21 февраля 2008 года.

Наиболее доступными по вопросам пожарной и охранной сигнализации являются руководящие документы МВД России:

- руководящий нормативный документ МВД России, утвержденный заместителем министра внутренних дел России «РД 78.143-92 Системы и комплексы охранной сигнализации, элементы технической укрепленности объектов. Нормы проектирования»;

- руководящий документ ГУВО МВД России «Р 78.36.007-99 Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. Рекомендации».

Требования по пожарной безопасности *(производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений),* в соответствии с Постановлением Правительства РФ № 45 «Об организации лицензирования отдельных видов деятельности», регулируется МЧС России.

Электропитание и заземление объектов выполняется в соответствии с требованиями «Правил устройства электроустановок», утвержденных приказом Минпромэнерго России.

Санитарные требования регулируются Роспотребнадзором России. Экологические требования регулируются Ростехнадзором России.

6.3. Повышение квалификации персонала в плане обеспечения безопасности информации

Повышение квалификации (дополнительное профессиональное образование) специалистов является лицензируемым видом деятельности и регулируется Законом Российской Федерации № 3266-1 «Об образовании», Федеральным законом № 125-ФЗ «О высшем и послевузовском профессиональном образовании» и Постановлением Правительства России № 796 «Об утверждении положения о лицензировании образовательной деятельности». При этом повышение квалификации с выдачей документов о повышении квалификации государственного образца разрешается только по тем образовательным программам, которые указаны в документах о лицензировании учебного заведения.

7. КАКИЕ СРОКИ НЕОБХОДИМО ВЫДЕРЖАТЬ ДЛЯ ВЫПОЛНЕНИЯ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ КАСАТЕЛЬНО ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ?

В соответствии с частью 4 статьи 25 Федерального закона № 152-ФЗ «О персональных данных», *операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу,* обязаны направить Уведомление о намерении осуществлять обработку персональных данных в уполномоченный орган по защите прав субъектов персональных данных не позднее 1 января 2008 года. В соответствии со ст. 19.7 «Кодекса Российской Федерации об административных правонарушениях» невыполнение этого требования влечет за собой наложение административного штрафа на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.

В соответствии с частью 3 статьи 25 Федерального закона № 152-ФЗ «О персональных данных»:

Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

В соответствии с пунктом 3.8.4 «Положения по аттестации объектов информатизации по требованиям безопасности информации», утвержденного Председателем Государственной технической комиссии при Президенте России:

3.8.4. «Аттестат соответствия» выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

8. КТО ИМЕЕТ ПРАВО ОСУЩЕСТВЛЯТЬ КОНТРОЛЬ И НАДЗОР ЗА ВЫПОЛНЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ?

В соответствии с частью 1 статьи 23 Федерального закона № 152-ФЗ «О персональных данных» и пункта 1 «Положения о Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия», утвержденного Постановлением Правительства Российской Федерации № 354, уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи (Россвязьохранкультура)[1].

В соответствии с частями 1, 2 и 3 статьи 19 Федерального закона № 152-ФЗ «О персональных данных»:

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

2. Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

[1] Федеральная служба по надзору в сфере связи и массовых коммуникаций преобразована в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Указ Президента РФ от 03.12.2008 г. № 1715). Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций утверждено Постановлением Правительства РФ от 16.03.2009 г. № 228.

Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, является ФСБ России.

В соответствии с Указом Президента РФ № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю», федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, является ФСТЭК России:

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею…

…5. ФСТЭК России в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, приказами и директивами Министра обороны Российской Федерации в части, касающейся ФСТЭК России, настоящим Положением, а также другими нормативными правовыми актами Российской Федерации, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

6. ФСТЭК России осуществляет свою деятельность непосредственно и (или) через свои территориальные органы.

ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

Кроме того, органы внутренних дел, прокуратуры, Роспотребнадзора и другие органы федеральной исполнительной власти, в рамках контроля соблюдения законности, в соответствии с действующим законодательством, имеют право реагировать и проводить соответствующие мероприятия в связи с обращениями граждан по поводу нарушения их законных прав и свобод.

Особое внимание стоит уделить ограничениям, накладываемым частями 1, 2 и 3 статьи 19 Федерального закона № 152-ФЗ «О персональных данных» на порядок и объем контроля законности защиты персональных данных федеральными органами исполнительной власти.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ЧАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии со статьей 23 Федерального закона № 152-ФЗ «О персональных данных»:

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

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

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

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

В соответствии со статьей 23 Федерального закона № 152-ФЗ «О персональных данных»:

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Таким образом, невыполнение требований по обработке и защите персональных данных может привести к серьезным последствиям для организации, вплоть до отзыва лицензии на

право выполнения работ и уголовной ответственности.

В Приложении № 7 приведена выписка из Уголовного, Трудового кодексов, а также Кодекса об административных правонарушениях в части, касающейся обработки, обеспечения безопасности персональных данных и лицензирования.

10. НЕОБХОДИМОСТЬ ПРИНЯТИЯ ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Это вполне закономерный вопрос, который возникает у любого, кто занялся определением объемов работ по обеспечению законной обработки персональных данных и подсчетом требуемого финансирования. По мнению авторов Памятки, к рассмотрению законодательства касательно вопросов обработки персональных данных, исполнительную и законодательную власть подвигли два серьезных фактора мирового значения. Первый – вступление во Всемирную торговую организацию, которое потребовало (пусть не жестко) принятия международных Конвенций по автоматизированной обработке персональных данных. Естественно, Конвенции не могут быть применимы напрямую к Российскому законодательству, что и повлекло за собой создание собственных законов в этой области права.

Второй – желание оптимизировать систему государственного управления, ее контрольно-надзорных, а также правоприменительных функций, включая предоставление услуг населению с целью защиты конституционных прав и свобод граждан путем создания Системы персонального учета населения Российской Федерации.

Создание такой системы описано в «Концепции создания системы персонального учета населения Российской Федерации», одобренной Распоряжением Правительства Российской Федерации от 09.06.05 г. № 748-р. Основные положения данной Концепции следующие:

Система персонального учета населения Российской Федерации – это система взаимодействия органов государственной власти, органов местного самоуправления, государственных и муниципальных организаций по обмену персональными данными о гражданах Российской Федерации, иностранных гражданах или лицах без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации (далее – граждане), на основе современных информационных технологий в рамках обеспечения конституционных прав граждан, а также предоставления услуг населению в соответствии с законодательством Российской Федерации. В целях повышения эффективности сбора персональных данных и их использования созданы государственные, ведомственные и муниципальные автоматизированные информационные системы учета населения (далее – автоматизированные системы учета).

Действующая в настоящее время государственная система учета населения формировалась в условиях отсутствия единой нормативной правовой базы, а также нескоординированности и несогласованности создания автоматизированных систем учета между собой.

Исходя из изложенного, представляется необходимым обеспечить единый порядок сбора и использования персональных данных, а также создать систему персонального учета на

основе интеграции автоматизированных систем учета в рамках единого информационного пространства. Достижение указанных целей возможно при осуществлении следующих мероприятий:

- введение единого идентификатора персональных данных, обеспечивающего возможность однозначного установления соответствия персональных данных, размещаемых в различных автоматизированных системах учета, конкретному физическому лицу;

- создание государственного регистра населения, содержащего актуальные первичные идентификационные данные граждан и соответствующие им идентификаторы персональных данных;

- интеграция и обеспечение взаимодействия различных автоматизированных систем учета, обеспечивающих сбор, обработку и хранение персональных данных в электронном виде.

Если рассмотреть Федеральный закон «О персональных данных» под таким ракурсом, становится понятно, что его создание является всего лишь одним из этапов реализации положений упомянутой выше Концепции.

ПРИЛОЖЕНИЕ 1

Примерная структура организационно-распорядительной документации

ПРИЛОЖЕНИЕ 2

Перечень и содержание разрабатываемых в организации документов, регламентирующих обработку персональных данных

Положение о персональных данных

Содержание

1. Общие положения.
   1.1. Определение персональных данных.
   1.2. Правовой статус обработки персональных данных.
      1.2.1. Правовое основание обработки персональных данных в организации (виды деятельности по ОКВЭД).
      1.2.2. Правовое основание обработки персональных данных средствами автоматизации (Уведомление о намерении осуществлять обработку персональных данных).
   1.3. Документы, которыми руководствуется организация в вопросах обращения с персональными данными.
2. Персональные данные.
   2.1. Цели обработки персональных данных.
   2.2. Круг субъектов, персональные данные которых подлежат обработке.
   2.3. Состав персональных данных, необходимый для обработки.
   2.4. Источники получения персональных данных.
   2.5. Сроки хранения и сроки обработки данных в каждом информационном ресурсе.
   2.6. Способы обработки персональных данных.
3. Учет персональных данных.
   3.1. Носители персональных данных.
   3.2. Порядок выделения содержащих персональные данные документов и информации (их особой маркировки на бумажных и электронных носителях).
   3.3. Порядок ведения отдельного учета и отслеживания доступа к персональным данным.
      3.3.1. Порядок документирования информации, содержащей персональные данные.
      3.3.2. Порядок оформления документов, содержащих персональные данные.
      3.3.3. Порядок учета документов, содержащих персональные данные.
      3.3.4. Порядок организации документооборота персональных данных.
      3.3.5. Порядок классификации.
      3.3.6. Порядок систематизации документов, содержащих персональные данные.
      3.3.7. Порядок подготовки документов, содержащих персональные данные для передачи их в архив.

3.3.8. Порядок подготовки документов, содержащих персональные данные для их уничтожения.

3.3.9. Определение режима хранения документов, содержащих персональные данные.

3.3.10. Порядок обращения с документами, содержащими персональные данные.

3.3.11. Порядок проверки наличия документов, содержащих персональные данные.

4. Персонал.

4.1. Требования к персоналу.

4.2. Порядок допуска персонала к обработке персональных данных.

4.3. Перечень должностных лиц, имеющих доступ к персональным данным.

4.4. Перечень должностных лиц, имеющих право относить данные к персональным, принимать решение об их обезличивании, осуществлять другие функции по определению и изменению статуса и класса персональных данных.

4.5. Должностные обязанности (в соответствии с «Квалификационным справочником должностей руководителей, специалистов и других служащих», утвержденным Постановлением Минтруда РФ № 37, 21.08.98 г.).

4.6. Обучение и повышение квалификации, повышение осведомленности персонала, осуществляющего обработку персональных данных.

4.7. Ответственность персонала, осуществляющего обработку персональных данных.

5. Порядок взаимодействия с субъектами персональных данных.

5.1. Права и обязанности.

5.1.1. Обязанности субъекта персональных данных.

5.1.2. Права субъекта персональных данных.

5.1.3. Обязанности Оператора.

5.1.4. Полномочия Оператора.

5.2. Юридические последствия, возникающие при нарушении конфиденциальности персональных данных.

5.3. Порядок реагирования на обращения субъектов персональных данных.

5.4. Возможные варианты ответов и действий персонала при обращениях субъектов персональных данных.

5.5. Сроки реагирования на обращения субъектов персональных данных.

5.6. Ответственность персонала и оператора при нарушениях конфиденциальности персональных данных.

6. Определение технических и программных средств обработки персональных данных.

6.1. Определение требований к техническим средствам обработки персональных данных.

6.2. Определение требований к программным средствам обработки персональных данных.

7. Порядок защиты персональных данных (ссылка на «Требования по обеспечению безопасности персональных данных при обработке в ИСПДн»).
   7.1. Направления защиты персональных данных.
   7.2. Санкции и последствия нарушений политики безопасности в отношении персональных данных.
8. Порядок контроля за соблюдением требований по обращению и защите персональных данных.
   8.1. Порядок внутреннего контроля за соблюдением требований по обращению и защите персональных данных.
   8.2. Порядок внешнего контроля за соблюдением требований по обращению и защите персональных данных.
9. Формы: приказ о создании комиссии по классификации; акт о классификации; приказ о вводе в эксплуатацию; приказ о создании должности уполномоченного по защите персональных данных; получения согласия на обработку; заявка-запрос (обращение) о предоставлении информации по обращению; уведомление о... ; акт об уничтожении; уведомление об исправлении; приказ о допуске персонала к обработке персональных данных; перечень сведений, отнесенных к ПДн; другие документы.
10. Должностные инструкции персонала, допущенного к обработке ПДн (требования, что знать, что уметь, обязанности).

Содержание организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн

Содержание

1. Общие положения.
   1.1. Назначение положения... (и на основе чего разработано).
   1.2. Нормативная и методическая документация (НМД) по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн.
2. Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн.
   2.1. Перечень мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн.
   2.2. Необходимость создания СЗПДн.
   2.3. Стадии создания СЗПДн.
      2.3.1. Предпроектная стадия, включающая в себя предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание.
      2.3.2. Стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн.
      2.3.3. Стадия ввода в действие СЗПДн, включающая в себя опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.
   2.4. ОРД, разрабатываемая на предприятии.
      2.4.1. Перечень ОРД, разрабатываемой на предприятии.
      2.4.2. Требования к содержанию ОРД.
3. Решение вопросов управления обеспечением безопасности ПДн в динамике обстановки и контроля эффективности защиты.
4. Формы: технический паспорт и т. д.

Требования по обеспечению безопасности ПДн при обработке в ИСПДн

Содержание

1. Общие положения.
   1.1. Назначение требований... (и на основе чего разработано).
   1.2. НМД по обеспечению безопасности ПДн при их обработке в ИСПДн.
2. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн.
   2.1. Функциональные требования к информационной системе при обработке персональных данных.
   2.2. Содержание мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах.
3. Порядок организации обеспечения безопасности ПДн в ИСПДн (Решение основных вопросов обеспечения защиты ПДн должно предусматривать подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения).
4. Порядок защиты ПДн (подробно).
   4.1. Принципы защиты ПДн.
   4.2. Организационно-распорядительные меры по защите ПДн.
   4.3. Меры по защите ПДн.
      4.3.1. Требования к подбору персонала.
      4.3.2. Требования по защите от несанкционированного физического доступа к элементам ИСПДн.
      4.3.3. Требования по пожарной защите ПДн.
      4.3.4. Требования по защите от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН).
      4.3.5. Требования по защите от перехвата при передаче по проводным (кабельным) линиям связи.
      4.3.6. Требования по защите от угроз несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).
      4.3.7. Требования по защите от воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы (например, подачи фазы на нулевой провод на подстанции).
      4.3.8. Требования по защите от непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т. п.) характера.

Вопросы, которые необходимо отразить
в специальном технологическом регламенте:

1. Учет машинных носителей информации, содержащих персональные данные.
2. Порядок хранения машинных носителей информации, содержащих персональные данные.
3. Порядок обращения с машинными носителями информации, содержащими персональные данные (съемными, несъемными).
4. Порядок уничтожения машинных носителей информации, содержащих персональные данные.
5. Порядок присвоения и изменения степени конфиденциальности (класса персональных данных) вновь создаваемых электронных документов и массивов информации, содержащих персональные данные.
6. Порядок обезличивания электронных документов и массивов информации, содержащих персональные данные.
7. Порядок учета электронных документов и массивов информации, содержащих персональные данные.
8. Порядок передачи электронных документов и массивов информации, содержащих персональные данные.
9. Порядок учета принимаемых электронных документов и массивов информации, содержащих персональные данные.
10. Порядок уничтожения электронных документов и массивов информации, содержащих персональные данные.
11. Порядок распечатки документов, содержащих персональные данные.
12. Порядок учета, хранения, обращения, уничтожения распечатанных документов, содержащих персональные данные.
13. Порядок обращения с электронными и распечатанными носителями персональных данных при чрезвычайных ситуациях (наводнение, пожар, отключение электропитания, теракт, вооруженное нападение, неадекватные действия клиентов, действия вирусов (атаки), отказы оборудования, переезды, нестыковки ключевой документации, введение военного положения).
14. Порядок обращения с электронными носителями персональных данных, средствами автоматизации, их содержащих при техническом обслуживании и ремонте.

Вариант образца № 1

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО работника,

паспортные данные

Заявление о согласии работника
на обработку персональных данных

Я (ФИО работника), даю согласие на обработку моих персональных данных:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- семейное, социальное положение;
- образование;
- профессия;
- доходы, полученные мной в данном учреждении,
- _____

для передачи в налоговую инспекцию по форме 2-НДФЛ и органы ПФР индивидуальных сведений о начисленных страховых взносах на обязательное пенсионное страхование и данных о трудовом стаже.

Передача персональных данных разрешается на срок действия трудового договора.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО работника)*

Вариант образца № 2

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО работника,

паспортные данные

Заявление о согласии работника
на получение/передачу персональных данных от третьей стороны/третьей стороне

Я (ФИО работника), даю согласие на получение/передачу Вами сведений обо мне, содержащих данные о *(перечень персональных данных. Указать, откуда могут быть получены или куда переданы персональные данные).*

С целью *(указать цель обработки персональных данных).*

В форме *(документальной/электронной/устной (по телефону).*

В течение *(указать срок действия согласия).*

Настоящее заявление может быть отозвано мной в письменной форме.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО работника)*

Вариант образца № 3

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО родителя или законного представителя,

паспортные данные

Заявление о согласии

на обработку персональных данных

Я (ФИО родителя или законного представителя), даю согласие на обработку моих персональных данных:

- фамилия, имя, отчество;
- адрес;
- место работы;
- профессия;
- _____

С целью *(указать цель обработки персональных данных).*

В течение *(указать срок действия согласия).*

Настоящее заявление может быть отозвано мной в письменной форме.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО родителя или законного представителя)*

Вариант образца № 4

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО родителя или законного представителя,

паспортные данные

Заявление о согласии

на обработку персональных данных ребенка

Я (ФИО родителя или законного представителя), даю согласие на обработку персональных данных моего ребенка:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- _____

С целью *(указать цель обработки персональных данных).*

В течение *(указать срок действия согласия).*

Настоящее заявление может быть отозвано мной в письменной форме.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО родителя или законного представителя)*

Вариант образца № 5

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО родителя или законного представителя,

паспортные данные

Заявление о согласии

на получение/передачу персональных данных от третьей стороны/третьей стороне

Я (ФИО родителя или законного представителя), даю согласие на получение/передачу Вами сведений обо мне, содержащих данные о *(Перечень персональных данных. Указать, откуда могут быть получены или куда переданы персональные данные).*

С целью *(указать цель обработки персональных данных).*

В форме *(документальной/электронной/устной (по телефону).*

В течение *(указать срок действия согласия).*

Настоящее заявление может быть отозвано мной в письменной форме.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО родителя или законного представителя)*

Вариант образца № 6

Руководителю *(наименование учреждения, адрес):*

_____

ФИО руководителя

ФИО родителя или законного представителя,

паспортные данные

Заявление о согласии
на получение/передачу персональных данных ребенка от третьей стороны/
третьей стороне

Я *(ФИО родителя или законного представителя)*, даю согласие на получения/передачу Вами сведений о моем ребенке, содержащих данные о *(Перечень персональных данных. Указать, откуда могут быть получены или куда переданы персональные данные).*

С целью *(указать цель обработки персональных данных).*

В форме *(документальной/электронной/устной (по телефону).*

В течение *(указать срок действия согласия).*

Настоящее заявление может быть отозвано мной в письменной форме.

Подтверждаю, что ознакомлен с «Положением о персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись *(ФИО родителя или законного представителя)*

Вариант образца № 7

Соглашение о неразглашении персональных данных сотрудников

Я,_____ (паспорт серии _____, номер _____, выданный _____ «____» _____ года), понимаю, что получаю доступ к персональным данным сотрудников (обучающихся, воспитанников, родителей, законных представителей) *(наименование учреждения)*. Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных сотрудников (обучающихся, воспитанников, родителей, законных представителей).

Я понимаю, что разглашение такого рода информации может нанести ущерб сотрудникам (обучающимся, воспитанникам, родителям, законным представителям) *(наименование учреждения),* как прямой, так и косвенный.

В связи с этим, даю обязательство: в работе (сборе, обработке и хранении) с персональными данными сотрудников (обучающихся, воспитанников, родителей, законных представителей) соблюдать все описанные в «Положении о персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения о (об):

- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- характере взаимоотношений в семье;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в органы ФНС;

- подлинниках и копиях приказов по личному составу;
- личных делах и трудовых книжках сотрудников;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.
- _____

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника или их утраты, несу ответственность в соответствии со ст. 90 ТК РФ, п.п. «в» п. 6 ст. 81 ТК РФ.

С «Положением о персональных данных» ознакомлен (а).

Должность

Дата

Подпись (ФИО)

Типовая форма Акта классификации ИСПДн

УТВЕРЖДАЮ
Руководитель учреждения
Подпись
Дата

АКТ
классификации информационной системы персональных данных

В соответствии с Приказом ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20 и Приказом от "___"_____ № ____ комиссия в составе председателя: _____ и членов: _____ произвела классификацию информационной системы персональных данных *Название ИСПДн* и установила нижеследующее:

1. В информационной системе персональных данных (ИСПДн) обрабатываются персональные данные категории…

2. В ИСПДн одновременно обрабатываются данные…

3. По структуре ИСПДн относится к…

4. По наличию подключений к сетям международного информационного обмена (Интернет) информационная система относится к системам…

5. По режиму обработки персональных данных в информационной системе ИСПДн относится к…

6. По разграничению прав доступа пользователей ИСПДн относится к…

7. По зависимости от местонахождения технических средств ИСПДн относится к системам…

8. В соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20, ИСПДн относится к типовым класса…

Подписи комиссии: _____

ПРИЛОЖЕНИЕ 3

Приказ об утверждении образца формы уведомления об обработке ПДн

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ

ПРИКАЗ
от 17 июля 2008 г. № 08

ОБ УТВЕРЖДЕНИИ ОБРАЗЦА
ФОРМЫ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях реализации частей 1, 3 статьи 22, а также части 4 статьи 25 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 31.07.2006 г. № 31 (I ч.), ст. 3451) приказываю:

1. При направлении уведомления об обработке (о намерении осуществлять обработку) персональных данных рекомендуется использовать следующий образец (приложение № 1).

2. Утвердить Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных (приложение № 2).

3. Контроль за исполнением настоящего Приказа возложить на заместителя руководителя Россвязькомнадзора А.А. Романенкова.

Врио руководителя
С.К. Ситников

Не нуждается в государственной регистрации. Письмо Минюста России от 6 августа 2008 г. № 01/7830-АС.

Приложение № 1

к Приказу Россвязькомнадзора

от 17 июля 2008 г. № 08

Образец

Руководителю Управления Федеральной службы
по надзору в сфере связи и массовых
коммуникаций по _____

УВЕДОМЛЕНИЕ
об обработке (о намерении осуществлять обработку)
персональных данных

_____
(наименование (фамилия, имя, отчество), адрес оператора)

руководствуясь _____
(правовое основание обработки персональных данных)
с целью _____
(цель обработки персональных данных)
осуществляет обработку: _____
(категории персональных данных)
_____
принадлежащих: _____
(категории субъектов, персональные данные которых
_____
обрабатываются)
Обработка вышеуказанных персональных данных будет осуществляться путем
_____
(перечень действий с персональными данными, общее описание
_____
используемых оператором способов обработки персональных данных)
_____
(описание мер, которые оператор обязуется осуществлять при обработке
_____
персональных данных, по обеспечению безопасности персональных данных
при их обработке)
Дата начала обработки персональных данных: _____
Срок или условие прекращения обработки персональных данных: _____
_____

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

«___» _____ 200_ г.

Приложение № 2

к Приказу Россвязькомнадзора

от 17 июля 2008 г. № 08

РЕКОМЕНДАЦИИ
ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ
ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее – Уведомление).

2. Уведомление оформляется на бланке оператора, осуществляющего обработку персональных данных, и направляется в территориальный орган Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее – территориальный орган Россвязькомнадзора).

3. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. В поле «наименование (фамилия, имя, отчество), адрес оператора» указывается:

4.1. Для юридических лиц (операторов):

- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;
- наименование филиала(ов), представительства(в) юридического лица (оператора), осуществляющего обработку персональных данных [2];
- место нахождения[3];

---

[2]Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта – согласно справочнику «Коды регионов», утвержденному Приказом ФНС России от 13.10.2006 г. № САЭ-3-04/706@ «Об утверждении формы сведений о доходах физических лиц», зарегистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Россвязькомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств). (Если для каких-либо операторов (с учетом филиалов (представительств)) значения пунктов 5 – 12 отличаются, то для них формируется отдельное уведомление).

[3]Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, а также место нахождения филиала(ов) (представительств) юридического лица, контактная информация (Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, бло-

- индивидуальный номер налогоплательщика (ИНН).

4.2. Для физических лиц:

- фамилия, имя, отчество физического лица (оператора);
- место жительства[4];
- данные документа, удостоверяющего личность; дата его выдачи, наименование органа, выдавшего документ, удостоверяющий личность.

Для индивидуальных предпринимателей:

- фамилия, имя, отчество индивидуального предпринимателя (оператора);
- место жительства[5];
- индивидуальный номер налогоплательщика (ИНН).

4.3. Для государственных, муниципальных органов (операторов):

- полное и сокращенное наименование государственного, муниципального органа;
- наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;
- место нахождения[6];
- индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

5. В поле «цель обработки персональных данных» указываются цели обработки персональных данных (а также их соответствие полномочиям оператора. Под «целью обработки персональных данных» понимаются как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по обработке персональных данных).

6. В поле «категории персональных данных» указываются все категории персональных данных, подлежащих обработке:

кирование, уничтожение персональных данных). При этом необходимо уточнить: обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).).

[4]Указывается место жительства физического лица в соответствии с данными документа, удостоверяющего личность, а в случае расхождения также фактическое место жительства, контактная информация.

[5]Указывается место жительства индивидуального предпринимателя (оператора) в соответствии с данными документа, удостоверяющего личность, и свидетельством о постановке индивидуального предпринимателя на учет в налоговом органе, контактная информация.

[6]Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, контактная информация.

6.1. Персональные данные (любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая необходимая информация).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность).

7. В поле «категории субъектов, персональные данные которых обрабатываются», указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются. Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

8. В поле «правовое основание обработки персональных данных» указываются:

- федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных (Например, ст. 85 – 90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона «Об актах гражданского состояния» и др.);
- номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий).

9. В поле «перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных» указываются действия, совершаемые оператором с персональными данными, а также описание используемых оператором

способов обработки персональных данных:

- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных (При автоматизированной обработке персональных данных либо при смешанной обработке необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица), либо информация передается с использованием Интернета, либо без передачи полученной информации).

10. В поле «описание мер, которые оператор обязуется осуществлять при обработке персональных данных по обеспечению безопасности персональных данных при их обработке», указываются организационные и технические меры, в том числе шифровальные (криптографические) средства, используемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий при их обработке.

11. В поле «дата начала обработки персональных данных» указывается конкретная дата начала совершения действий с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (фактическая дата начала обработки персональных данных).

12. В поле «срок или условие прекращения обработки персональных данных» указывается конкретная дата или основание (условие), наступление которого повлечет за собой прекращение обработки персональных данных.

ПРИЛОЖЕНИЕ 4

Порядок проведения классификации ИСПДн

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)	ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ (ФСБ России)	МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ (Мининформсвязи России)

ПРИКАЗ

«13» февраля 2008 г. г. Москва № 55 / 86 / 20

Об утверждении Порядка проведения классификации информационных систем персональных данных

В соответствии с пунктом 6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, часть II, ст. 6001), **П Р И К А З Ы В А Е М:**

Утвердить прилагаемый Порядок проведения классификации информационных систем персональных данных.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ	ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ	МИНИСТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ
С.И.Григоров	Н.П.Патрушев	Л.Д.Рейман

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 11462
от "03" марта 2008 г.

Утвержден Приказом ФСТЭК России,
ФСБ России,
Мининформсвязи России
от 13 февраля 2008 г. № 55/86/20

ПОРЯДОК
ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий Порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы)[7].

2. Классификация информационных систем проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее – оператор)[8].

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

4. Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

5. При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных – $X_{пд}$;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – $X_{нпд}$;

[7]Абзац первый пункта 1 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 (Собрание законодательства Российской Федерации, 2007, № 48, часть II, ст. 6001) (далее – Положение).

[8]Абзац первый пункта 6 Положения.

- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

6. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{пд}$):

- категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 – обезличенные и (или) общедоступные персональные данные.

7. $X_{нпд}$ может принимать следующие значения:

- 1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- 2 – в информационной системе одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
- 3 – в информационной системе одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

9. По структуре информационные системы подразделяются на:

- автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);
- комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

10. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

11. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

12. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

13. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком на-

ходятся за пределами Российской Федерации.

14. По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

- класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

15. Класс типовой информационной системы определяется в соответствии с таблицей.

$X_{ПД}$ \ $X_{НПД}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

16. По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»[9].

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

[9]Собрание законодательства Российской Федерации, 2007, № 48, часть II, ст. 6001.

18. Результаты классификации информационных систем оформляются соответствующим актом, составленным оператором.

19. Класс информационной системы может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

ПРИЛОЖЕНИЕ 5

Требования к средствам автоматизации

В соответствии с пунктами 3.8.4 и 3.8.5 «Положения по аттестации объектов информатизации по требованиям безопасности информации», утвержденного Председателем Государственной технической комиссии при Президенте России:

3.8.4. «Аттестат соответствия» выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более, чем на 3 года.

3.8.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

По этим причинам рекомендуется не проводить аттестацию средств автоматизации обработки персональных данных, которые в течение срока действия аттестата предполагается заменять на новые, так как это потребует дополнительных финансовых вложений в настройку средств защиты, проведение работ, касающихся анализа изменений и переаттестации, в случае признания их влияющими на защищенность.

Кроме этого, необходимо учитывать требования к ресурсам вычислительной техники с целью обеспечить достаточную скорость работы для выполнения технологических действий, так как, кроме средств выполнения основных задач, на ней будут устанавливаться программные (программно-аппаратные) средства защиты информации (например, от несанкционированного доступа, антивирусное программное обеспечение), которые являются достаточно ресурсоемкими.

Обобщая вышесказанное, можно рекомендовать перед аттестацией обновлять парк средств автоматизации, задействованных в технологическом процессе.

ПРИЛОЖЕНИЕ 6

Особенности неавтоматизированной обработки персональных данных

Утверждено
Постановлением Правительства
Российской Федерации
от 15 сентября 2008 г. № 687.

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

I. Общие положения

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – персональные данные), 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.

2. 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 нее.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

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

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

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

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

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

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. При ведении журналов (реестров, книг), содержащих персональные данные, необходи-

мые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом, составленным оператором, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

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

ПРИЛОЖЕНИЕ 7

Выписка из кодексов Российской Федерации

(Основные положения в части обработки персональных данных)

«ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ»

Федеральный закон № 197-ФЗ от 30.12.2001 г. (с изменениями):

Статья 81. Расторжение трудового договора по инициативе работодателя

Трудовой договор может быть расторгнут работодателем в случаях:

б) однократного грубого нарушения работником трудовых обязанностей:

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника;

11) представления работником работодателю подложных документов при заключении трудового договора.

Глава 14. Защита персональных данных работника

Статья 85. Понятие персональных данных работника. Обработка персональных данных работника

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Обработка персональных данных работника – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работ-

ника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников

Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований настоящего Кодекса и иных федеральных законов.

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

Статья 88. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ)

- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ)

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ).

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работ-

ники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ)

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суде любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

(в ред. Федерального закона от 30.06.2006 г. № 90-ФЗ)

Статья 195. Привлечение к дисциплинарной ответственности руководителя организации, руководителя структурного подразделения организации, их заместителей по требованию представительного органа работников

Работодатель обязан рассмотреть заявление представительного органа работников о нарушении руководителем организации, руководителем структурного подразделения органи-

зации, их заместителями трудового законодательства и иных актов, содержащих нормы трудового права, условий коллективного договора, соглашения и сообщить о результатах его рассмотрения в представительный орган работников.

В случае когда факт нарушения подтвердился, работодатель обязан применить к руководителю организации, руководителю структурного подразделения организации, их заместителям дисциплинарное взыскание вплоть до увольнения.

Статья 237. Возмещение морального вреда, причиненного работнику

Моральный вред, причиненный работнику неправомерными действиями или бездействием работодателя, возмещается работнику в денежной форме в размерах, определяемых соглашением сторон трудового договора.

В случае возникновения спора факт причинения работнику морального вреда и размеры его возмещения определяются судом независимо от подлежащего возмещению имущественного ущерба.

Статья 391. Рассмотрение индивидуальных трудовых споров в судах

Непосредственно в судах рассматриваются индивидуальные трудовые споры по заявлениям:

работника – о восстановлении на работе независимо от оснований прекращения трудового договора, об изменении даты и формулировки причины увольнения, о переводе на другую работу, об оплате за время вынужденного прогула либо о выплате разницы в заработной плате за время выполнения нижеоплачиваемой работы, о неправомерных действиях (бездействии) работодателя при обработке и защите персональных данных работника;

«КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ»

Федеральный закон № 195-ФЗ от 30.12.2001 г. (с изменениями):

Статья 5.27. Нарушение законодательства о труде и об охране труда

1. Нарушение законодательства о труде и об охране труда влечет за собой наложение административного штрафа на должностных лиц в размере от одной тысячи до пяти тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от одной тысячи до пяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на юридических лиц – от тридцати тысяч до пятидесяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

2. Нарушение законодательства о труде и об охране труда должностным лицом, ранее

подвергнутым административному наказанию за аналогичное административное правонарушение, – влечет дисквалификацию на срок от одного года до трех лет.

Статья 5.39. Отказ в предоставлении гражданину информации

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации – влечет наложение административного штрафа на должностных лиц в размере от пятисот до одной тысячи рублей.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) – влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), – влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – влечет наложение административного штрафа на лиц, осуществляющих

предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц – от одной тысячи до одной тысячи пятисот рублей; на юридических лиц – от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), – влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц – от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии – влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, – влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей.

Статья 13.19. Нарушение порядка представления статистической информации

Нарушение должностным лицом, ответственным за представление статистической ин-

формации, необходимой для проведения государственных статистических наблюдений, порядка ее представления, а равно представление недостоверной статистической информации – влечет наложение административного штрафа в размере от трех тысяч до пяти тысяч рублей.

Статья 19.4. Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль)

5. Невыполнение законных требований должностного лица органа, уполномоченного в области экспортного контроля, а равно воспрепятствование осуществлению этим должностным лицом служебных обязанностей – влечет наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц – от пяти тысяч до десяти тысяч рублей.

Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)

1. Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства – влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от одной тысячи до двух тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от десяти тысяч до двадцати тысяч рублей.

2. Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа – влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до десяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от двухсот тысяч до пятисот тысяч рублей.

Статья 19.6. Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения

Непринятие по постановлению (представлению) органа (должностного лица), рассмотревшего дело об административном правонарушении, мер по устранению причин и условий, способствовавших совершению административного правонарушения, – влечет наложение административного штрафа на должностных лиц в размере от трехсот до пятисот рублей.

Статья 19.7. Непредставление сведений (информации)

Непредставление или несвоевременное представление в государственный орган (должно-

стному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных статьями 19.7.1, 19.7.2, 19.7.3, 19.8, 19.19 настоящего Кодекса, – влечет наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.

Статья 19.20. Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии)

1. Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна), – влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до двадцати тысяч рублей.

2. Осуществление деятельности, не связанной с извлечением прибыли, с нарушением требований или условий специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна), – влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

3. Осуществление деятельности, не связанной с извлечением прибыли, с грубым нарушением требований или условий специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна), – влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц – от одной тысячи до одной тысячи пятисот рублей; на юридических лиц – от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Статья 20.25. Неуплата административного штрафа либо самовольное оставление места отбывания административного ареста

1. Неуплата административного штрафа в срок, предусмотренный настоящим Кодексом, – влечет наложение административного штрафа в двукратном размере суммы неуплаченного административного штрафа либо административный арест на срок до пятнадцати суток.

2. Самовольное оставление места отбывания административного ареста – влечет админи-

стративный арест на срок до пятнадцати суток.

Статья 32.2. Исполнение постановления о наложении административного штрафа

1. Административный штраф должен быть уплачен лицом, привлеченным к административной ответственности, не позднее тридцати дней со дня вступления постановления о наложении административного штрафа в законную силу либо со дня истечения срока отсрочки или срока рассрочки, предусмотренных статьей 31.5 настоящего Кодекса.

3. Сумма административного штрафа вносится или перечисляется лицом, привлеченным к административной ответственности, в банк или в иную кредитную организацию, за исключением случаев, предусмотренных частью 1 статьи 32.3 настоящего Кодекса.

(В соответствии с Федеральным законом от 03.06.2009 г. № 121-ФЗ с 1 января 2010 года часть 3 статьи 32.2 будет изложена в новой редакции:

«3. Сумма административного штрафа вносится или перечисляется лицом, привлеченным к административной ответственности, в банк или в иную кредитную организацию либо платежному агенту, осуществляющему деятельность по приему платежей физических лиц, или банковскому платежному агенту, осуществляющему деятельность в соответствии с законодательством о банках и банковской деятельности, за исключением случаев, предусмотренных частью 1 статьи 32.3 настоящего Кодекса».)

5. При отсутствии документа, свидетельствующего об уплате административного штрафа, по истечении тридцати дней со срока, указанного в части 1 настоящей статьи, судья, орган, должностное лицо, вынесшие постановление, направляют соответствующие материалы судебному приставу-исполнителю для взыскания суммы административного штрафа в порядке, предусмотренном федеральным законодательством. Кроме того, должностное лицо федерального органа исполнительной власти, его учреждения, структурного подразделения или территориального органа, а также иного государственного органа, уполномоченного осуществлять производство по делам об административных правонарушениях (за исключением судебного пристава-исполнителя), составляет протокол об административном правонарушении, предусмотренном частью 1 статьи 20.25 настоящего Кодекса, в отношении лица, не уплатившего административный штраф. Копия протокола об административном правонарушении направляется судье в течение трех дней со дня составления указанного протокола.

«УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ»

Федеральный закон № 63-ФЗ от 13.06.1996 г. (с изменениями):

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, состав-

ляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

(Федеральным законом от 22.12.2008 г. № 272-ФЗ с 1 января 2010 года абзац второй части первой статьи 137 данного документа будет дополнен словами: «либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет».)

2. Те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

(Федеральным законом от 22.12.2008 г. № 272-ФЗ с 1 января 2010 года абзац второй части второй статьи 137 данного документа будет дополнен словами: «либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет».)

Статья 140. Отказ в предоставлении гражданину информации

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

Статья 155. Разглашение тайны усыновления (удочерения)

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений, – наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев с лишением права за-

нимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом – наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, – наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, – наказываются лишением свободы на срок до десяти лет.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осуж-

денного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносныхпрограмм для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Статья 292. Служебный подлог

1. Служебный подлог, то есть внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности (при отсутствии признаков преступления, предусмотренного частью первой статьи 292.1 настоящего Кодекса), – наказываются штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на

срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до двух лет.

2. Те же деяния, повлекшие существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 293. Халатность

1. Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло причинение крупного ущерба или существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

2. То же деяние, повлекшее по неосторожности причинение тяжкого вреда здоровью или смерть человека, – наказывается лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяние, предусмотренное частью первой настоящей статьи, повлекшее по неосторожности смерть двух или более лиц, – наказывается лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

ПРИЛОЖЕНИЕ 8

Исходные данные для проведения классификации и выполнения работ по защите персональных данных

1. Полное наименование организации

Пример: Муниципальное общеобразовательное учреждение средняя общеобразовательная школа № XX городского округа Тольятти

2. Адрес и ИНН.

Пример: 445XXX, г. Тольятти, ул. 50 лет Октября, XX; ИНН XXXXXXXXXXX

3. Контактное лицо

(Должность, ФИО полностью, телефон, электронная почта)

Пример: заместитель директора по УВР Иванов Иван Иванович,

тел.: (XXXX) XX-XX-XX, mail@schoolXX.tgl.ru

4. Правовое основание обработки персональных данных

(Устав, Положение – наличие вида деятельности по ОКВЭД; наличие выписки из Реестра Операторов персональных данных).

Пример:

1. Пункт X.X Устава Муниципального общеобразовательного учреждения средней общеобразовательной школы № XX городского округа Тольятти, утвержден Распоряжением мэра городского округа Тольятти XX.XX.XX (далее Устав):

общеобразовательное учреждение имеет право:

- вести обработку данных, включая подготовку и ввод персональных данных учащихся и сотрудников учреждения, в том числе и с применением автоматизированных средств обработки.

2. Пункт X.X Устава:

- предметом деятельности общеобразовательного учреждения является обучение и воспитание обучающихся в процессе реализации общеобразовательных программ общего образования в пределах государственных образовательных стандартов, дополнительных образовательных программ, оказание дополнительных образовательных услуг (на договорной основе), не включенных в перечень основных общеобразовательных программ, определяющих ее статус.

3. Пункт X.X Устава: общеобразовательное учреждение может оказывать следующие платные дополнительные услуги:

- *образовательные:*

  - обучение по дополнительным образовательным программам;

- занятия по углубленному изучению предметов за рамками учебного плана и реализуемых основных и дополнительных общеобразовательных программ;
- репетиторство;
- преподавание специальных курсов, реализующих общеобразовательные (дополнительные) программы;
- работа кружков, секций, где реализуются общеобразовательные (дополнительные) программы;
- создание групп, в которых реализуются развивающие программы, а также программы адаптации детей к условиям школьной жизни;

• *оздоровительные:*
- организация занятий по гимнастике, аэробике, ритмике, баскетболу, лыжам, футболу, гандболу, волейболу;
- создание групп по укреплению здоровья;

• *организационные услуги:*
- организация питания учащихся;
- организация охраны учащихся;
- организация различных мероприятий, в том числе семинаров, конференций, круглых столов,
- организация соревнований, конкурсов;
- организация походов, экскурсий, путешествий, лагерей, слетов и т. д.

5. Наличие документов, регламентирующих работу по обработке ПДн

(Положение (Концепция) о персональных данных, Положение о защите ПДн, Регламент обработки ПДн).

Пример: В МОУ СОШ № XX разработаны и утверждены следующие нормативные документы, регламентирующие обработку персональных данных:

- Положение о персональных данных;
- Общий технологический регламент обработки персональных данных.

6. Наличие Положения о маркировке носителей персональных данных

Пример: В МОУ СОШ № XX разработано и утверждено «Положение о маркировании носителей персональных данных».

7. Перечень собираемых данных

(Наименование всех полей электронной формы базы данных (например, 1С:Зарплата и кадры, поля в АСУ РСО), в которые вводятся персональные данные субъектов).

Пример: См. представленный ниже образец.

фото

Регистрационный номер_____

ФИО (полностью)_____

Дата рождения:_____

Гражданство: *гражданин Российской Федерации, иное* (укажите)_____

Паспортные данные: серия_____ номер_____

Кем выдан_____

Когда выдан_____

Адрес_____

Контактный телефон, (e-mail)_____

Семейное положение_____

Образование_____

Название учебного заведения, курсов	Квалификация, специальность (факультет)	Год поступления	Год окончания	Форма обучения (очная, заочная, вечерняя)

Опыт работы

Место работы (наименование организации)	Занимаемая должность	Основная работа или совмещение	Стаж работы (месяцев, лет)	Ср/мес. зарплата	Причины увольнения

Знание ПК (программы, с которыми Вы работаете; скорость набора текста)_____

_____

Уровень владения иностранными языками (какими)_____

Имеете ли Вы водительские права (категория)_____

8. Объем обрабатываемых персональных данных

(Количество субъектов, персональные данные которых обрабатываются в информационной системе, возможно, за несколько лет).

Пример: В МОУ СОШ № XX имеются следующие информационные системы персональных данных:

- АИС «1С:Зарплата и кадры» – 50 записей о субъектах персональных данных;

- АСУ РСО – 1 500 записей о субъектах персональных данных.

9. Распределенность субъектов персональных данных

(Варианты: персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом; персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования; персональные данные субъектов персональных данных в пределах конкретной организации).

Пример: В МОУ СОШ № XX имеются следующие информационные системы персональных данных:

- АИС «1С:Зарплата и кадры» – данные о работниках МОУ СОШ № XX;
- АСУ РСО – данные об учащихся, их родителях и (или) законных представителях.

10. Заданные оператором характеристики безопасности персональных данных

(Варианты: информационные системы, в которых необходимо обеспечить только конфиденциальность информации или информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных, требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Пример: В автоматизированных информационных системах МОУ СОШ № XX требуется обеспечить следующие характеристики безопасности:

- АИС «1С:Зарплата и кадры» – конфиденциальность, защиту от уничтожения, изменения, блокирования;
- АСУ РСО – конфиденциальность, защиту от уничтожения, изменения, блокирования.

11. Структура (физическая) информационной системы (схема)

(Состав технических средств и систем, предполагаемых к использованию, условия их расположения, топология ЛВС: автономные, локальные информационные системы, распределенные информационные системы; имеются ли подключения ЛВС, в которой обрабатываются персональные данные к другим частям, сегментам ЛВС, где такие данные не обрабатываются).

Пример: В целях удобства использования и наглядности, рекомендуется составить как можно более подробные, поэтажные планы физического расположения средств вычислительной техники и связей между ними. Например, с использованием ПО Microsoft Office Visio.

12. Структура (логическая) информационной системы (схема)

(Конфигурация и логическая топология ИСПДн в целом и ее отдельных компонент, функциональные и технологические связи как внутри этих систем, так и с другими система-

ми различного уровня и назначения, перечень информационных баз, задачи этих баз, их назначение, ресурсы сети, данные из Active Directory по группам безопасности, подразделениям и др.).

Пример: Логическая структура информационной системы может быть представлена при помощи возможностей ПО Microsoft Office Visio. Данное ПО позволяет наглядно представить все упомянутые выше структуры, имеющие отношение к ИСПДн. Примеры отображения таких структур показаны на рис. 1 и 2.

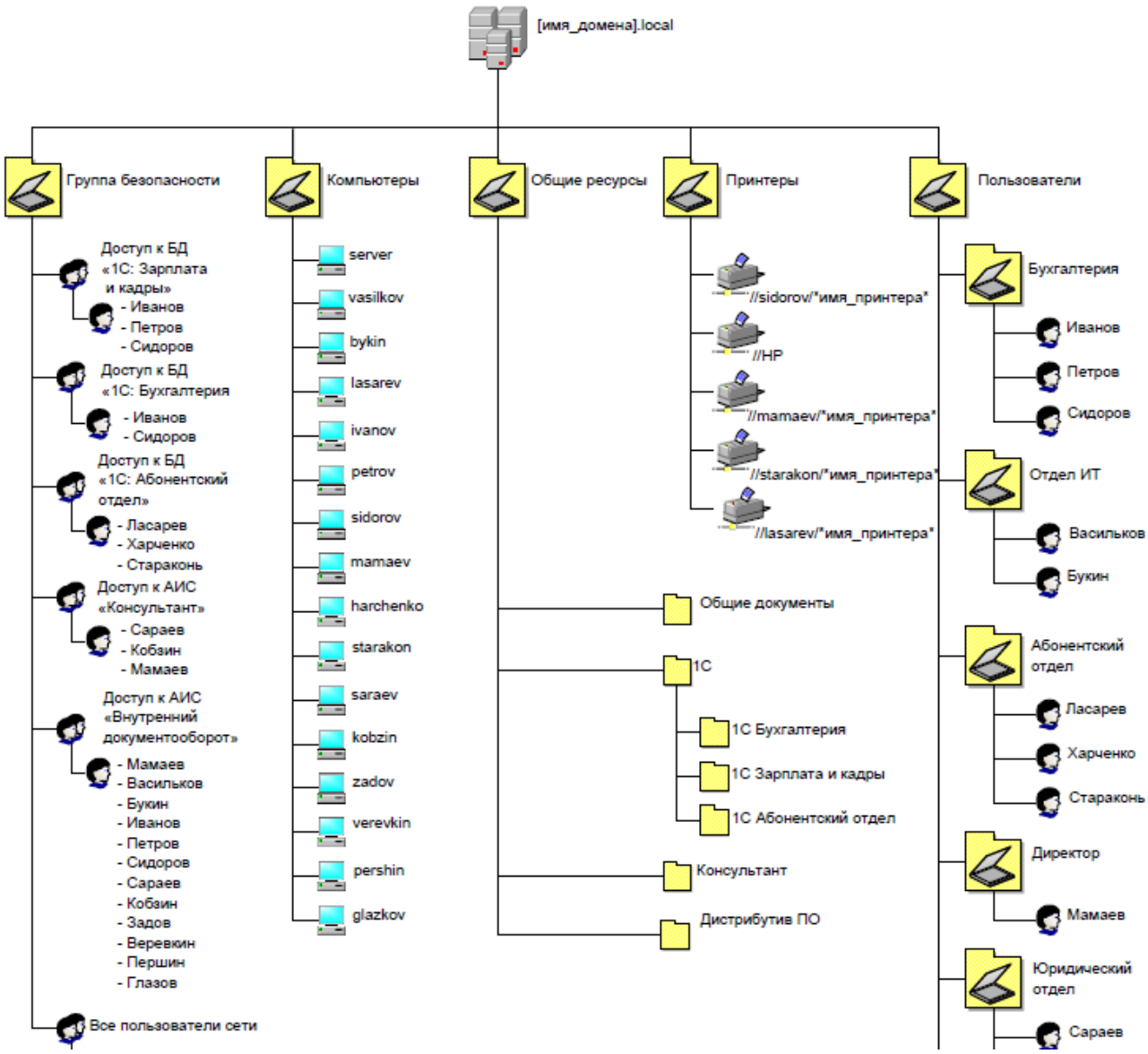

Рис. 1. Логическая структура информационной системы (доменная структура)

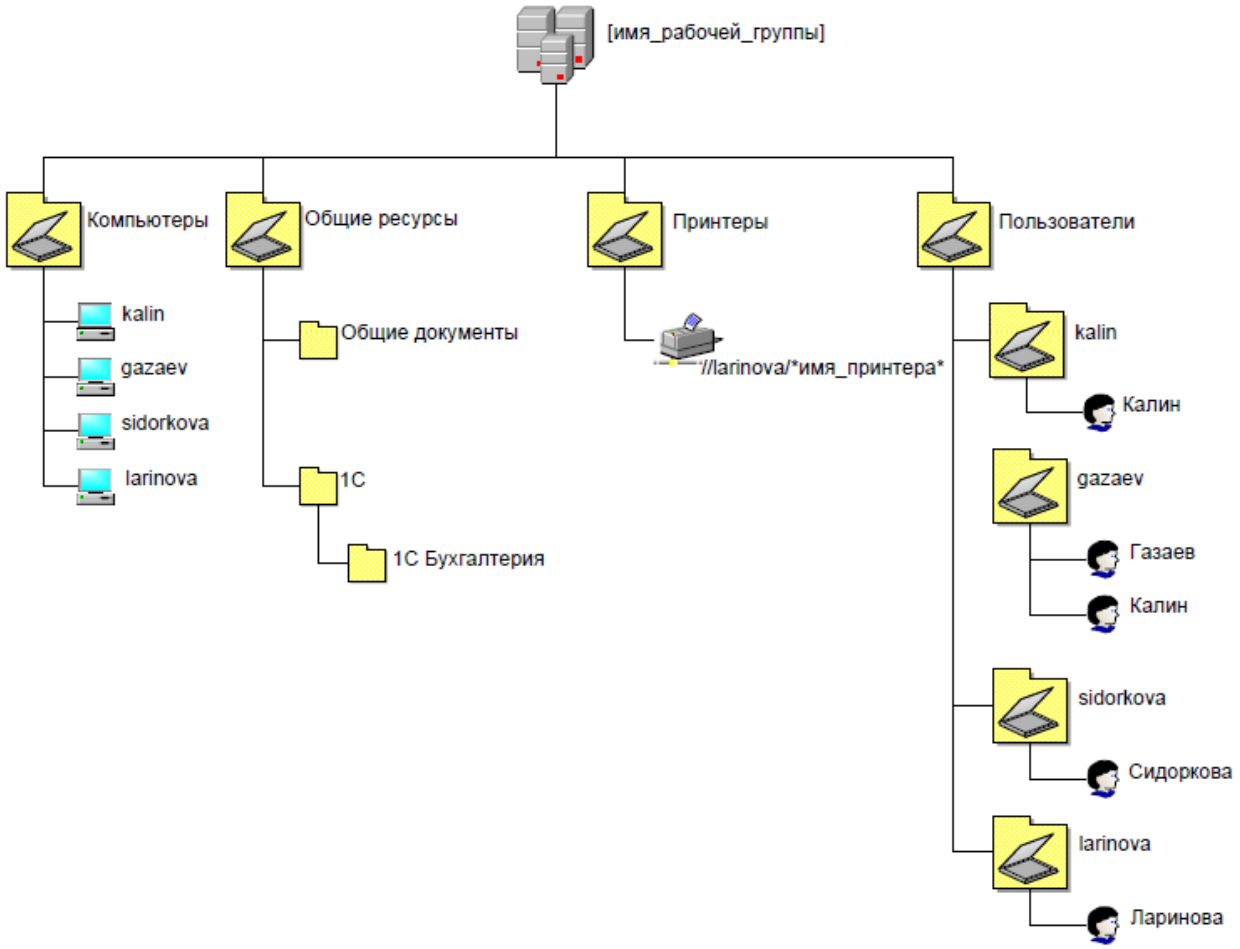

Рис. 2. Логическая структура информационной системы (рабочая группа)

13. Наличие средств инженерно-технической защиты помещений, в которых обрабатываются персональные данные, а также данные, касающиеся пожарной и охранной защиты и сигнализации

Пример: Все помещения МОУ СОШ № XX, в которых обрабатываются персональные данные, имеют железные двери, решетки на окнах первых и последних этажей, во всех помещениях установлена пожарная и охранная сигнализация, имеющая выход на посты круглосуточной охраны.

14. Наличие средств обеспечения гарантированного электропитания систем, в которых обрабатываются персональные данные

Пример: Электропитание всех серверов МОУ СОШ № XX осуществляется через источники бесперебойного питания. Электропитание ПЭВМ осуществляется от промышленной сети без использования источников бесперебойного электропитания.

15. Наличие подключений информационной системы к сетям связи общего пользования (ССОП) и/или к Интернету

(Напрямую или через другие ЛВС, с которыми имеются физические соединения).

Пример: Автоматизированные информационные системы МОУ СОШ № XX:

- АИС «1С:Зарплата и кадры» – не имеет физических соединений с ССОП и Интернетом, имеется прямой канал связи для передачи информации в налоговые органы;
- АСУ РСО – имеет физические соединения с ССОП и Интернетом через внутреннюю сеть учреждения.

16. Режим обработки персональных данных

Режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах: однопользовательские или/и многопользовательские; степень участия персонала в обработке ПДн.

Таблица 1. Правила разграничения доступа информационной системы (доменная структура)

Группы безопасности/Общие ресурсы	**1С:Зарплата и кадры**	**1С:Бухгалтерия**	**Консультант**	**1С:Абонентский отдел**	**Общие документы**	**Дистрибутив ПО**
Доступ к БД «1С:Зарплата и кадры»	полн.					
Доступ к БД «1С:Бухгалтерия»		полн.				
Доступ к АИС «Консультант»			чтение			
Доступ к БД «Абонентский отдел»				полн.		
Доступ к АИС «Внутренний документооборот»					полн.	
Все пользователи						чтение

Пример: Режим обработки АИС «1С:Зарплата и кадры» представлен в табл. 1 и 2.

Таблица 2. Правила разграничения доступа информационной системы (рабочая группа)

Пользователи/Общие ресурсы	**1С:Бухгалтерия**	**Общие документы**
Калин	полн.	полн.
Газаев	полн.	полн.
Сидоркова	полн.	чтение
Ларинова	полн.	полн.

17. Режим разграничения прав доступа пользователей информационной системы

Режимы обработки ПДн в многопользовательских ИСПДн в целом и в отдельных компонентах: без разграничения прав доступа или с разграничением прав доступа; количество со-

трудников всего в системе и за каждым рабочим местом, их пересечение; характер их взаимодействия между собой; права доступа к каждому ресурсу, содержащему персональные данные.

18. Местонахождение технических средств информационной системы

Варианты: все технические средства системы обработки персональных данных находятся в пределах Российской Федерации или все технические средства системы обработки персональных данных частично или целиком находятся за пределами Российской Федерации.

Пример: Все технические средства МОУ СОШ № XX находятся в пределах Российской Федерации.

19. Программное обеспечение

Операционные системы, программное обеспечение, которое обрабатывает и хранит персональные данные, офис, архиватор и другие общесистемные и прикладные программные средства.

Пример: Состав программного обеспечения АРМ АИС «1С:Зарплата и кадры» МОУ СОШ № XX представлен в таблице 3.

20. Наличие сертифицированных (ФСТЭК, ФСБ) средств защиты

От несанкционированного доступа, антивирусы и др.

Пример: В МОУ СОШ № XX не имеется сертифицированных средств защиты от НСД; в АИС «1С:Зарплата и кадры» используется сертифицированный ФСТЭК «АП Континент»; на всех ПЭВМ установлены антивирусные средства DrWeb и Антивирус Касперского, имеющие сертификаты ФСТЭК и ФСБ России.

Таблица 3. Правила разграничения доступа информационной системы (доменная структура)

№ п/п	Назначение программного продукта	Информация о программном продукте		
		Производитель	Наименование	Версия
1	Операционная система	Microsoft	Windows XP	Professional Edition SP3
2	Разработка, модификация текстовых и табличных документов	Microsoft	Office 2003	Professional Edition SP2
3	Программа просмотра файлов pdf	Adobe	Reader	7.0
4	Программа архивации	Александр Рошал	WinRAR	3.51

5	Программа обеспечения совместимости Microsoft Office 2003 с Microsoft Office 2007	Microsoft	Пакет обеспечения совместимости для выпуска 2007 системы Microsoft Office	
6	Набор компонент, позволяющих запускать приложения стандарта NET Framework	Microsoft	Framework	2.0
7		Microsoft	Framework	1.1
8	Клиент СУБД	1С	1С:ЗиК	8.1

21. Наличие администратора (службы)

Ответственного за ЛВС, оборудование, программное обеспечение.

Пример: В МОУ СОШ № XX имеется договор с технической службой ЦИТ, отвечающей за сопровождение ЛВС, серверов, программного обеспечения ПЭВМ.

22. Наличие администратора базы данных

Ответственного за сопровождение баз данных, содержащих сведения о персональных данных.

Пример: Сопровождение баз данных МОУ СОШ № XX осуществляется:

- АИС «1С:Зарплата и кадры» – по договору с сотрудниками ООО «1С-Консалтинг»;
- АСУ РСО – с сотрудниками ЦИТ.

ПРИЛОЖЕНИЕ 9

Сокращения, применяемые при аттестации объектов информатизации

ПО – программное обеспечение;

СВТ – средства вычислительной техники;

АРМ – автоматизированное рабочее место;

СЗИ НСД – средство защиты от несанкционированного доступа;

АС – автоматизированная система;

ОВТ – объект вычислительной техники;

ОИ – объект информатизации;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные;

СЗПДн – система защиты персональных данных;

ОРД – организационно-распорядительная документация.

Подготовлено

в МОУДПОС Центре информационных технологий

445011, г. Тольятти, ул. К. Маркса, 27 а.

Составители

Галина Владимировна Копылова

Сергей Викторович Кокорин

Михаил Владимирович Литвинов

Редактор *С.И. Банюлис*

Верстка *Н.С. Ежова*