1С КОНСАЛТИНГ

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

+CD

- формы документов
- нормативные акты

3 издание

МЕТОДИЧЕСКОЕ ПОСОБИЕ

1С ПАБЛИШИНГ

Персональные данные хранятся и обрабатываются в любой организации, а это значит, что вопросы защиты таких данных актуальны для широкого круга лиц.

К 1 июля 2011 года все информационные системы персональных данных должны быть приведены в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Комплекс необходимых мер по обеспечению безопасности персональных данных включает мероприятия правового, организационного и технического характера.

Предлагаемое пособие содержит пошаговые инструкции и типовые формы документов, наличие которые обязательно при осуществлении мероприятий по защите персональных данных. В отдельном разделе пособия рассмотрены вопросы применения программных продуктов, разработанных фирмой «1С», с учетом требований, предъявляемых законодательством Российской Федерации о защите персональных данных.

К книге прилагается CD, на котором в электронном виде приводятся типовые формы документов, которые могут быть взяты за основу при организации и проведении собственных мероприятий по защите персональных данных.

Пособие подготовлено при участии члена консультативного совета при уполномоченном органе по защите прав субъектов персональных данных Шойдина Ю.Ю. и ведущего специалиста по защите информации ООО «Бюро экспертных решений», к.т.н. Иващук И.Ю.

1С ПАБЛИШИНГ

4 601546 086563

И. Баймакова, А. Новиков, А. Рогачев, А. Хыдыров

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Методическое пособие

3-е издание

Москва ООО «1С-Паблишинг»
2011

УДК 004.056.5
ЬБК 32.973
0-13

Баймакопи И.А., Новиков А.И., Рогачев А.И., Хыдыров А.Х.

О-13 Обеспечение защиты персональных данных. Методическое пособие.
3-е ичд. - М.: ООО «1С-Паблишинг»; 2011. -268 с.: ил.
) I CD-ROM.

ISBN 978-5-9677-1455-9

Персональные данные хранятся и обрабатываются в любой организации, а это значит, что вопросы защиты таких данных актуальны для широкого круга лиц. К 1 июля 2011 года все информационные системы персональных данных должны быть приведены в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Комплекс необходимых мер по обеспечению безопасности персональных данных включает мероприятия правового, организационного и технического характера.

Предлагаемое пособие содержит пошаговые инструкции и типовые формы документов, наличие которые обязательно при осуществлении мероприятий по защите персональных данных. В отдельном разделе пособия рассмотрены вопросы применения программных продуктов, разработанных фирмой «1С», с учетом требований, предъявляемых законодательством Российской Федерации о защите персональных данных.

К книге прилагается CD, на котором в электронном виде приводятся типовые формы документов, которые могут быть взяты за основу при организации и проведении собственных мероприятий по защите персональных данных.

Пособии подготовлено при участии члена консультативного совета при уполномоченном органе по защите прав субъектов персональных данных Шойдина Ю.Ю. и ведущего специалиста по защите информации ООО «Бюро экспертных решений», к.т.н. Иващук И.Ю.

В случае существенных изменений законодательства по защите персональных данных планируется размещать уточняющие материалы к книге на странице http://1 c.ru/szi-news.

ISBN 978-5-9677-1455-9

Содержание

Введение

Проблема защиты персональных данных не является новой. В Конституции Российской Федерации заложены права гражданина о тайне переписки, о личной и семейной тайне, то есть требование о защите персональных данных не ново для российского законодательства.

Особо остро проблема защиты персональных данных встала именно в 2009 - 2010 годах в связи с поэтапным вступлением в действие Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и необходимостью приведения информационных к 01 июля 2011 года в соответствие с требованиями действующего законодательства всеми операторами персональных данных. При этом невыполнение требований закона может повлечь административную и даже уголовную ответственность.

Защита персональных данных актуальна для большинства российских компаний, осуществляющих обработку персональных данных. Ведь под действие закона «О персональных данных» попадают все организации, зарегистрированные в Российской Федерации и осуществляющие обработку персональных данных, независимо от вида отрасли, формы собственности и иных факторов.

Мероприятия по обеспечению безопасности персональных данных сочетают в себе реализацию правовых, организационных и технических мер, причем все они одинаково значимы, а невыполнение одних требований сводит на нет результаты реализации других. При этом именно организационноуправленческая сторона вопроса защиты оператором обрабатываемых персональных данных в большинстве случаев имеет первостепенное значение при соблюдении требований федерального закона. Необходимо понимать, что с целью соблюдения таких требований во всех организациях должен появиться новый, достаточно объемный пласт документации, и организа

ции необходимо решить насколько «хватит сил», чтобы провести все необходимые мероприятия самостоятельно.

Для обеспечения «технической» составляющей, при отсутствии в организации подготовленных должным образом специалистов, необходимо обратиться в специализированные организации, имеющие квалифицированных консультантов по защите ПДн.

Сложность реализации мер по защите персональных данных связана не только с новизной задач, которые необходимо решать, но и с целым рядом проблем, к которым можно отнести следующие:

- отсутствие в штате большинства организаций специалистов по защите информации;
- недостаточность финансовых средств для проведения комплекса работ по построению эффективной системы защиты;
- наличие законодательных пробелов.

Основной задачей данного пособия является оказание практической помощи при организации и проведении мероприятий по защите персональных данных с точки зрения разработки организационно-распорядительной документации. В представленных материалах приведены пошаговые инструкции и типовые формы документов, наличие которые обязательно при осуществлении мероприятий по защите персональных данных.

Кроме того, в отдельном разделе пособия рассмотрены вопросы применения разработанных фирмой «1С» программных продуктов с учетом требований, предъявляемых законодательством Российской Федерации о защите персональных данных.

Надеемся, что данное пособие поможет лицам, не имеющим специальных знаний в области защиты информации и информационных технологий, провести обследование информационной системы персональных данных, оценить «масштаб бедствия», провести необходимые мероприятия и подготовить комплект организационно-распорядительной документации.

Выражаем огромную благодарность за оказание помощи при подготовке настоящего пособия члену консультативного совета при уполномоченном органе по защите прав субъектов персональных данных, члену правления Санкт- Петербургского клуба ИТ-директоров «SPbCIOClub» Шойди- ну Юрию Юрьевичу и ведущему специалисту по защите информацци ООО «Бюро экспертных решений» (Санкт- Петербург), кандидату технических наук Иващук Ирине Юрьевне.

Основные понятия

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

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

Биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (цифровая фотография, отпечатки пальцев, изображение радужной оболочки глаз и другие биометрические персональные данные)[1]

[1] Определение приведено в проекте Соглашения о сотрудничестве в создании государственных информационных систем изготовления, оформления и контроля паспортно- визовых документов нового поколения и дальнейшем их развитии и использовании в государствах-участниках содружества независимых государств, признанного целесообразным к подписанию Распоряжением Правительства РФ от 18.11.2008 № 1654-р.

В документах, рекомендованных Минздравом России для использования в подведомственных учреждениях, дано следующее определение:

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

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Ведение реестра операторов - деятельность Службы, включающая сбор, фиксацию, обработку, хранение и предоставление данных, составляющих систему ведения реестра операторов, осуществляющих обработку персональных данных;

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

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

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

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

Доступ к информации - возможность получения информации и ее использования.

Доступность информации - состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

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

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

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

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

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

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

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

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

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в

отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (п. 1 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства РФ от 15.09.2008 № 687).

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

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

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

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

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

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.

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

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

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, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

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

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

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

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

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных

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

Реестр - перечень, список операторов, осуществляющих обработку персональных данных;

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

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

1)

Определение приведено в документах, рекомендованных Минздравом России для использования в подведомственных учреждениях.

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

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

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенноцифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации.

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

Трансграничная передача персональных данных - передача персональных данных оператором через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

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

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

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Обозначения и сокращения

АВС - антивирусные средства

АРМ - автоматизированное рабочее место

ВТСС - вспомогательные технические средства и системы

ЕГРЮЛ - единый государственный реестр юридических лиц

ИБ - информационная база

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки САЗ - система анализа защищенности СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных СОВ - система обнаружения вторжений ТКУИ - технические каналы утечки информации ТУ - технические условия

УБПДн - угрозы безопасности персональных данных

Основы правового регулирования отношений в сфере защиты персональных данных

1. Развитие законодательства о защите персональных данных в мире

В настоящее время насчитывается более 40 стран, в которых действуют законы, регулирующие порядок защиты неприкосновенности частной жизни и персональной информации. Первый закон о защите персональных данных на национальном уровне был принят в 1973 году в Швеции, затем в 1974 году - в США. В большинстве же стран законы о защите персональных данных принималась в 1998 - 2003 годах.

Особой вехой в развитии законодательства о защите персональных данных в мире явилась Конвенция «О защите физических лиц при автоматизированной обработке персональных данных» ETS-108 (Страсбург, 28 января 1981 г.), которая была принята государствами-членами Совета Европы с целью обеспечения на территории каждой из сторон договора уважения прав и основных свобод каждого человека независимо от его гражданства или места жительства и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой касающихся его персональных данных. Следует учитывать, что положения данной конвенции также применяются к базам персональных данных, которые не проходят автоматической обработки.

В первую очередь необходимо обратить внимание на основные термины, приведенные в названной конвенции:

1. «Данные личного характера» означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных).
2. «Автоматизированная база данных» означает любой набор данных, к которым применяется автоматическая обработка.
3. «Автоматическая обработка» включает следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств: накопление данных, проведение логических или/и арифметических операций с такими данными, их изменение, стирание, восстановление или распространение.

Контролером базы данных является физическое или юридическое лицо, государственный орган, ведомство или любая другая организация, которая в соответствии с национальным правом наделена полномочиями решать, для какой цели создается автоматизированная база данных, какие категории персональных данных будут накапливаться и какие операции с ними будут осуществляться.

Особое внимание в конвенции уделено требованиям, предъявляемым к персональным данным, проходящим автоматическую обработку. В частности предусмотрено, что персональные данные (далее - ПДн):

- должны быть получены и обработаны добросовестным и законным образом;
- должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;
- должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;
- должны быть точными и в случае необходимости обновляться;

- должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

Кроме того, статьей 6 конвенции введены дополнительные требования по отношению к обработке персональных данных о национальной принадлежности, политических взглядах либо религиозных или иных убеждениях, а равно персональные данные, касающиеся здоровья или сексуальной жизни. Определено, что указанные данные могут подвергаться автоматической обработке только в случаях, когда «национальное право предусматривает надлежащие гарантии». Также данное правило применяется к персональным данным, касающимся судимости.

Нормы настоящей конвенции обязывают государства принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или разрушения.

Данная Конвенция и последовавшие за ней несколько Директив Евросоюза сформулировали в общих чертах те задачи, которые национальное законодательство должно решать при регулировании работы с персональными данными:

- защита персональных данных от несанкционированного доступа к ним со стороны других лиц, в том числе представителей государственных органов и служб, не имеющих на то необходимых полномочий;
- обеспечение сохранности, целостности и достоверности данных в процессе работы с ними, в том числе при передаче по каналам связи;
- обеспечение надлежащего правового режима этих данных при работе с ними для различных категорий персональных данных;
- обеспечение контроля над использованием персональных данных со стороны самого гражданина;

- создание специальной независимой структуры, обеспечивающей эффективный контроль за соблюдением прав гражданина на защиту его персональных данных (например, создание должности Уполномоченного по защите персональных данных).

С целью реализации законодательных норм о защите персональных данных и организации порядка работы с ними в государствах, подписавших конвенцию, были созданы специальные государственные структуры (комиссии, агентства или различные управления по защите персональных данных в структуре органов и т. п.). Россия не явилась исключением и 28 декабря 2007 года было создано Управление по защите прав субъектов персональных данных в Российской Федерации в структуре Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор). В составе Федеральной службы функционируют 78 территориальных органов, из них в 19-ти созданы профильные отделы, в остальных управлениях дополнительно введены должности для выполнения функций по осуществлению государственного контроля и надзора за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн.

Дополнительно стоит отметить, что в рамках международной межрегиональной организации СНГ также существует определенный порядок относительно защиты персональных данных. В частности, Межпарламентской ассамблеей государств - участников СНГ 16 октября 1999 г. принят Модельный Закон «О персональных данных», который регулирует вопросы охраны персональных данных в широком смысле и не применительно к трудовым правоотношениям.

Акты международного законодательства в сфере регулирования защиты персональных данных

Таблица 1

№ п/п	Основные законодательные акты
1	**Конвенция Совета Европы от 28 января 1981 года (с изменениями 1999 года) «О защите личности в связи с автоматической обработкой персональных данных» (ратифицирована Федеральным законом от 19 декабря 2005 г. № 160-ФЗ)**
2	**Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных»**
3	**Директива 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций**
4	**Дополнительный протокол к Конвенции «О защите физических лиц при автоматизированной обработке персональных данных, о наблюдательных органах и трансграничной передаче информации (Страсбург, 8 ноября 2001 г.) ETS № 181**

2. Основы законодательства Российской Федерации

В Российской Федерации в основе законодательства о защите персональных данных лежат положения Конституции Российской Федерации о тайне переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, о личной и семейной тайне. Также статьей 24 Конституции Российской Федерации определено, что не допускается без согласия лица сбор, хранение, использование и распространение информации о его частной жизни.

Правовая основа механизма защиты персональных данных формируется по двум направлениям: специализированное законодательство и иное законодательство, которое лишь частично содержит правовые нормы, гарантирующие неприкосновенность частной жизни и регулирующие сферу защиты персональных данных. К специализированному законодательству относятся такие правовые акты как: Федеральный закон от 27.07.2006

№ 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ, закрепляющий принцип неприкосновенности частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (статья 3), Указ Президента РФ от 06.03.1997 № 188, утверждающий «Перечень сведений конфиденциального характера» и другие.

Правовые нормы, регулирующие работу с персональными данными, содержатся также в главе 14 Трудового кодекса РФ «О защите персональных данных работника», в Законе РФ «Об архивном деле в Российской Федерации» от 22.10.2004 г. (ст. 25), в Законе РФ «Об оперативно-розыскной деятельности» (ст. 3, 5, 9, 10, 12, 21) от 12.08.1995 № 144-ФЗ, в Законе РФ от 27.12.1991 №2124-1 «О средствах массовой информации» (ст. 41, 43, 46, 51, 57), в Законе РФ от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования», в соответствии с которым персональные данные содержатся в индивидуальном лицевом счете застрахованного лица, нормы о защите сведений, полученных в ходе всероссийской переписи населения (персональные данные) содержатся в Законе РФ от 25.01.2002 № 8-ФЗ «О всероссийской переписи населения». В соответствии со статьей 84 Налогового кодекса РФ при постановке на учет физических лиц в состав сведений об указанных лицах включаются также их персональные данные.

Наиболее пристальное внимание должно быть обращено на Федеральный закон Российской Федерации «О персональных данных», который был принят в соответствии с Конвенцией Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (ETS № 108, 1981 г.)

Основная цель федерального закона «О персональных данных» —
защита права и свободы человека при обработке его личной информации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну.

Положения Федерального закона «О персональных данных» вступали в силу поэтапно. Начиная с 26 января 2007 года, обработка персональных данных, включенных в информационные системы персональных данных, должна была осуществляться в соответствии с нормами рассматриваемого закона. Например, получение и обработку персональных данных уже в 2007 году необходимо было осуществлять только при наличии согласий субъектов персональных данных. Кроме того уже в 2007 году необходимо было задуматься и начать разработку организационно-распорядительной документации.

С 1 января 2008 года операторы, осуществляющие обработку персональных данных, обязаны направлять уведомление в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор). Соответственно уже в 2008 году следовало провести категорирование персональных данных, классификацию информационной системы, направить уведомление в Роскомнадзор.

Пунктом 3 статьи 25 рассматриваемого закона с учетом изменений, внесенных Федеральным законом от 23.12.2010 № 359-ФЭ, предусмотрено, что информационные системы персональных данных должны быть приведены в соответствие с требованиями этого Федерального закона не позднее 1 июля 2011 года, т. е. Федеральный закон «О персональных данных» окончательно вступает в силу с 1 июля 2011 года. Однако необходимо учитывать, что к 1 июля 2011 года должны быть решены псе вопросы, связанные с технической защитой ИСПДн, а все организационно-распорядительные мероприятия по защите персональных данных должны были быть проведены ранее.

3. Сфера действия федерального закона «О персональных данных»

Федеральным законом «О персональных данных» регулируются отношения, связанные с обработкой персональных данных, осуществляемые 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 (п. 1 статьи 1 Федерального закона «О персональных данных»).

Таким образом, требования Федерального закона «О персональных данных» распространяются на все государственные и коммерческие организации, а также физических лиц, обрабатывающих в своих информационных системах персональные данные физических лиц (сотрудников, клиентов, партнеров и т. п.), независимо от размера и формы собственности.

Говоря об обработке персональных данных, следует уточнить, что в законе речь идет именно о порядке взаимоотношений физического лица и юридического лица (предпринимателя) или иного физического лица, но рассматриваемый закон не затрагивает в настоящее время взаимоотношения между юридическими лицами. Если в рамках выполнения договора между двумя юридическими лицами необходимо передавать персональные данные субъектов ПДн, то, определяя условия такого договора, следует определять условия соблюдения конфиденциальности при организации работы с ПДн и предусматривать мероприятия по защите персональных данных (например, определять условия хранения, допуск лиц и т. п.)

Вместе с тем в законе предусмотрены четыре исключения. И соответствии с пунктом 2 статьи 1 Федерального закона «О персональных данных» действие данного Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
3) обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей (ЕГРИП) сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
4) обработке ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

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.

Основные законодательные акты Российской Федерации в сфере защиты ПДн

Таблица № 2

№ п/п	Законодательный/нормативный правовой акт
1	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»
2	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3	Федеральный закон от 27.12.2004 № 184-ФЗ «О техническом регулировании»
4	Трудовой кодекс Российской Федерации (14 глава)
5	Федеральный закон от 3 декабря 2008 года № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»
6	Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»
7	Постановление Правительства РФ № 781 от 17 ноября 2007 года «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
8	Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
9	Постановление Правительства РФ от 06 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
10	Постановление Правительства РФ от 27 сентября 2007 года № 612 «Об утверждении Правил продажи товаров дистанционным способом»
11	Постановление Правительства РФ от 16 марта 2009 года № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»
12	Распоряжение Правительства РФ от 15 августа 2007 года № 1055-р «Об утверждении Плана подготовки проектов нормативных правовых актов, необходимых для реализации Федерального закона «О персональных данных»
13	Указ Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела

4. Регуляторы в сфере обработки персональных данных

В соответствии с п. 3 ст. 19 Федерального закона «О персональных данных» контроль и надзор за выполнением требований федерального законодательства о защите ПДн осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической шщиты информации, в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в информационных системах персональных данных.

Федеральными органами, регулирующими деятельность в сфере обработки персональных данных (регуляторы), являются:

- Роскомнадзор (Федеральная служба по надзору в сфере связи и массовых коммуникаций) - осуществляет контроль и надзор за соответствием обработки ПДн требованиям законодательства.
- ФСТЭК России (Федеральная служба по техническому и экспортному контролю) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием технических средств.
- ФСБ России (Федеральная служба безопасности РФ) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием криптографических средств защиты информации

Основные «источники поступления» персональных данных, а также сферы влияния регуляторов могут быть представлены в виде следующей схемы.

Поименованные выше три ведомства имеют право проводить проверки операторов ПДн по вопросам, связанным с соблюдением законодательства о защите ПДн, однако основания для проверок различны.

В первую очередь операторов ПДн могут коснуться проверки Роскомнадзора. Данное ведомство проводит проверки:

- по обращению субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки (Федеральный закон от 27.07.2006 № 152-ФЗ);
- проверка сведений, содержащихся в уведомлении об обработке персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ);

- внеплановые проверки по контролю нарушений обязательных требований (Федеральный закон от 26.12.2008 №294-ФЗ).

Для информации

Ежегодно на своем сайте Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций размещает ежегодный отчет о деятельности уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора).

Отчет отражает положение дел в области защиты прав субъектов персональных данных и является основным итоговым документом о деятельности уполномоченного органа. Подготовка такого отчета и его направление Президенту РФ, в Правительство РФ и Федеральное Собрание РФ предусмотрено частью 7 статьи 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Анализ отчетов Роскомнадзора за 2008 и 2009 год показывает значительное повышение активности ведомства в части осуществления контрольных функций (см. таблицу № 3).

Таблица № 3

	2009	**2008**
Проведено проверок за 2009 год	432	76
в т. ч. внеплановых	148 (34%)	40 (53%)
Получено обращений или заявлений граждан на действия (бездействие) операторов ПДн	146	465
в т. ч. по результатам рассмотрения обращений проведено проверок	40 (27%)	31 (6,7%)
Выдано предписаний об устранении выявленных нарушений	557	19
Составлено протоколов об административных правонарушениях	54	11
Направлены материалы проверок в органы прокуратуры	86	24
Вынесены постановления о привлечении операторов к административной ответственности	30	2
Общая сумма штрафов, наложенных на операторов ПДн	78 000 руб.	5 500 руб.

Как нетрудно увидеть, количество проводимых контрольных мероприятий существенно увеличилось, при этом в разы больше выписано предписаний об устранении выявленных нарушений и направлено материалов проверок в органы прокуратуры.

К числу наиболее «популярных» нарушений законодательства о защите персональных данных отнесены:

- **несоответствие сведений, указанных в уведомлении об обработке ПДн, фактической деятельности;**
- **обработка данных без согласия субъектов ПДн;**
- **несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, требованиям законодательства РФ в области ПДн;**
- **избыточность обрабатываемых ПДн применительно к целям обработки.**

Наибольшее количество нарушений в 2009 году, как и в 2008 году, наблюдается у кредитных организаций, операторов связи, организаций жилищно-коммунального хозяйства.

Подробно с отчетом Роскомнадзора за 2009 год можно ознакомиться по ссылке: http://www.rsoc.ru/docs/20090529113450vC.doc.

ФСТЭК России может проводить проверки по следующим основаниям:

- надзор за деятельностью лицензиата ФСТЭК России (Постановление Правительства РФ от 15.08.2006 № 504);
- по обращению Роскомнадзора (Федеральный закон от 27.07.2006 № 152-ФЗ);
- внеплановые проверки по контролю нарушений обязательных требований (Федеральный закон от 26.12.2008 №294-ФЗ).

Основаниями для проведения проверок ФСБ России являются:

- контроль за соблюдением правил пользования средств криптографической защиты информации (Приказ ФСБ России от 9.02.2005 № 66 № ПКЗ-2005);

- надзор за деятельностью лицензиата ФСБ России (Постановление Правительства РФ от 29.12.2007 № 957);
- внеплановые проверки по контролю нарушений обязательных требований (Федеральный закон от 26.12.2008 №294-ФЗ);
- по обращению Роскомнадзора (Федеральный закон от 27.07.2006 № 152-ФЗ).

Права и обязанности Роскомнадзора

Полномочия уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора) определены главой 5 Федерального закона «О персональных данных». В частности, ч. 2 ст. 23 данного закона предусмотрено, что уполномоченный орган по защите прав субъектов ПДн рассматривает обращения субъекта ПДн о соответствии содержания ПДн и способов их обработки целям их обработки и принимает соответствующее решение.

Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) имеет право:

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

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

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;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

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

В соответствии с ч. 5 ст. 23 Федерального закона «О персональных данных» уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

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

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

Типовое положение о территориальном органе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций утверждено Приказом Роскомнадзора от 07.04.2009 № 51.

В частности, п. 9.1.5 данного положения предусмотрено, что территориальный орган осуществляет в установленном порядке государственный контроль и надзор за деятельностью юридических лиц, индивидуальных предпринимателей и физических лиц за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Дополнительно стоит отметить, что при Роскомнадзоре создан на общественных началах консультативных совет, возможность создания которого, предусмотрена п. 9 ст. 23 рассматриваемого федерального закона. Данной нормой отмечено, что порядок формирования и порядок деятельности такого совета определяются уполномоченным органом по защите прав субъектов персональных данных.

Особенности проведения проверок Роскомнадзором

Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (далее - Регламент) утвержден Приказом Министерства связи и массовых коммуникаций РФ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 01.12.2009 №630 (зарегистрировано в Минюсте РФ 28.01.2010 № 16095).

Рассматриваемым регламентом определены следующие административные процедуры:

- принятие решений о проведении проверок;
- проведение проверок;
- оформление результатов и принятие мер по результатам проверок.

В целях осуществления контроля (надзора) за соответствием обработки ПДн требованиям законодательства РФ в области ПДн Регламентом предусмотрено проведение плановых и внеплановых проверок.

Плановые проверки проводятся как в отношении операторов, включенных в реестр операторов, осуществляющих обработку ПДн, так и в отношении операторов, не включенных в Реестр, но осуществляющих обработку ПДн.

В соответствии с пунктом 22 Регламента основанием для включения плановой проверки в План является начало осуществления Оператором деятельности по обработке персональных данных, а также истечение трех лет со дня:

- государственной регистрации Оператора в качестве юридического лица, индивидуального предпринимателя;

- окончания проведения последней плановой проверки Оператора.

Внеплановые проверки проводятся по следующим основаниям (п. 27):

- истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства РФ в области ПДн;
- поступление в Службу (Роскомнадзор) или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:
  - возникновение угрозы причинения вреда жизни, здоровью граждан;
  - причинение вреда жизни, здоровью граждан.

В ходе проведения проверки Служба или ее территориальный орган осуществляют рассмотрение документов Оператора, а также исследование (обследование) информационной системы персональных данных в части, касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

Для операторов ПДн следует обратить особое внимание на те документы, которые будут рассматриваться в ходе проведения проверки, К таким документам в соответствии с п. 64.1 Регламента относятся:

- уведомление об обработке персональных данных;
- документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства РФ в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Службу или ее территориальный орган;

- документы, подтверждающие выполнение Оператором предписаний об устранении ранее выявленных нарушений законодательства РФ в области персональных данных;
- письменное согласие субъекта персональных данных на обработку его персональных данных;
- документы, подтверждающих соблюдение требований законодательства Российской Федерации при обработке специальных категорий и биометрических персональных данных;
- документы, подтверждающие уничтожение Оператором персональных данных субъектов персональных данных по достижении цели обработки;
- локальные акты Оператора, регламентирующие порядок и условия обработки персональных данных.

Дополнительно

В утвержденном Регламенте конкретный перечень документов не приведен. Вместе с тем в проекте данного документа был приведен следующий примерный перечень запрашиваемых документов:

1. Учредительные документы Оператора ПДн;

2. Копия уведомления об обработке ПДн;

3. Положение о порядке обработки ПДн;

4. Положение о подразделении, осуществляющем функции по организации защиты ПДн;

5. Должностные инструкции лиц, имеющих доступ к ПДн;

6. План мероприятий по защите ПДн;

7. План внутренних проверок состояния защиты ПДн;

8. Приказ о назначении ответственных лиц по работе с ПДн;

9. Типовые формы документов, предполагающие или допускающие содержание ПДн;

10. Журналы, реестры, книги, содержащие ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится Оператор или в иных аналогичных целях;

11. Договоры с субъектами ПДн;

12. Лицензии на виды деятельности, в рамках которых осуществляется обработка ПДн;

13. Выписка из ЕГРЮЛ, содержащая актуальные данные на момент проведения мероприятия по контролю (надзору);

14. Приказы об утверждении мест хранения материальных ПДн;

15. Письменное согласие субъектов ПДн на обработку их ПДн (типовая форма);

16. Распечатки электронных шаблонов полей, содержащие ПДн;

17. Справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка ПДн;

18. Заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности ПДн при их обработке (проверяется только наличие данных документов);

19. Приказ о создании комиссии и акты проведения классификации информационных систем ПДн (проверяется только наличие данных документов);

20. Журналы (книги) учета обращений граждан (субъектов персональных данных);

21. Акт об уничтожении персональных данных субъекта (ов) персональных данных (в случае достижения цели обработки);

22. Иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных.

Плановые и внеплановые проверки проводятся в форме документарной или выездной проверки. Форма проведения определения Службой или ее территориальным органом самостоятельно. Рассмотрим основные отличия.

Документарная проверка, в отличие от выездной, проводится по месту нахождения Службы или ее территориального органа. Предметом документарной проверки являются сведения,

содержащиеся в документах Оператора, устанавливающих их организационно-правовую форму, права и обязанности, документы, используемые при осуществлении деятельности по обработке персональных данных и связанные с исполнением обязательных требований, установленных нормативными правовыми актами в области персональных данных, исполнением предписаний Службы или ее территориального органа. Т. е. в ходе документарной проверки в основном изучаются документы, находящиеся в распоряжении проверяющих.

Если же достоверность сведений, содержащихся в документах, вызывает обоснованные сомнения либо эти данные не позволяют оценить исполнение Оператором требований, установленных нормативными правовыми актами, то проверяющие вправе направить мотивированный запрос о предоставлении необходимых для проверки документов. Оператор ПДн обязан представить необходимые документы в течение 10 рабочих дней со дня получения запроса.

ВНИМАНИЕ!

Необходимые документы предоставляются в виде копий, заверенных печатью (при ее наличии) и подписью руководителя или иного уполномоченного представителя Оператора.

Не допускается требовать нотариального удостоверения копий документов.

(п. 67.6 и п. 67.7 Регламента)

Если при проведении документарной проверки выявлены ошибки и (или) противоречия или несоответствия в представленных документах, то Оператору может быть направлено требование о предоставлении в течение 10 рабочих дней необходимых пояснений в письменной форме.

Если в результате проведенных мероприятий с учетом дополнительно представленных документов и пояснений будут выявлены признаки нарушений обязательных требований, установленных нормативными правовыми актами в области персональных данных, то должностные органы Службы или ее территориального органа вправе провести выездную проверку.

Таким образом, выявление нарушений в ходе проведения документальной проверки является одним из оснований для проведения выездной проверки. Также решение о проведении выездной проверки может быть принято в случаях, если Оператор не представил запрашиваемые документы в установленные законодательством сроки, т. е. в течение 10 рабочих дней.

Целью проведения выездной проверки является проверка полноты и достоверности сведений, содержащихся в уведомлении об обработке ПДн, а также в иных документах, имеющихся в распоряжении Службы или ее территориального органа.

Выездная проверка проводится на территории/территориях Оператора. Операторы обязаны предоставить должностным лицами регулятора возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, а также обеспечить доступ проверяющих в здания, строения, сооружения, помещения и оборудованию, используемому Оператором для обработки ПДн. Следует учитывать, что должностные лица Службы или ее территориального органа не вправе изымать оригиналы документов.

ВНИМАНИЕ!

Должностные лица Роскомнадзора не вправе изымать оригиналы документов.

По результатам проведения проверки составляется акт проверки. Требования к оформлению акта проверки содержатся в пункте 75 Регламента. Пунктом 83 Регламента предусмотрено, что в случае выявления нарушений Оператору вместе с актом выдается предписание об устранении нарушений.

Напомним, что формы применяемых документов (приказа, акта, журнала учета проверок) при осуществлении государственного контроля (надзора) утверждены Приказом от 30.04.2009 № 141.

Каковы возможные результаты проведения проверок?

1. Выдача предписания об устранении выявленного нарушения и осуществление контроля за его исполнением.
2. Выявление административного правонарушения и, соответственно, составление протокола об административном правонарушении, направление протокола с материалами проверки в суд либо в прокуратуру.
3. Выявление уголовно наказуемого деяния и, соответственно, направление материалов проверки в органы прокуратуры, другие правоохранительные органы для рассмотрения вопроса о возбуждении уголовного дела.

Дополнительно может быть рекомендовано обратить внимание на блок-схемы, приведенные в приложениях № 2-4 к рассматриваемому Регламенту, в том числе на блок-схему административной процедуры о принятии решения о проведении проверок, блок-схему административной процедуры проведения проверок, блок-схему административной процедуры оформления результатов и принятия мер по результатам проверок.

С целью упрощения изучения Регламента предлагаем следующую справочную информацию в отношении проведения государственного контроля органами Роскомнадзора:

Таблица № 4

Количественный состав участников проверки	**Не менее двух должностных лиц, в том числе должностное лицо, отвечающее за вопросы правового обеспечения (п- 17)**
Основание проведения проверки	**Приказ руководителя Службы или руководителя территориального органа**
Срок уведомления оператора о начале проведения плановой проверки	**Не позднее чем в течение трех рабочих дней до начала проведения проверки (п. 23)**
Срок уведомления оператора о начале проведения внеплановой проверки	**Не позднее чем за 24 часа до начала ее проведения (п. 29)**
Порядок предварительного уведомления о начале проведения плановой проверки	**Направление оператору копии приказа руководителя (заместителя) службы или его территориального органа (п. 23)**
Порядок предварительного уведомления о начале проведения внеплановой проверки	**Любым доступным способом (п. 29)**
Срок проведения проверки	**20 рабочих дней (продление возможно на срок не более 20 рабочих дней) (п. 31 и п. 32)**
Срок представления требуемых документов	**10 рабочих дней**
Срок представления пояснений	**10 рабочих дней**

Основные нормативные правовые акты регуляторов в сфере защиты ПДн

Таблица № 5

№ п/п	Нормативные правовые акты
1	Приказ ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»
2	Приказ Министерства связи и массовых коммуникаций РФ от 30.01.2010 № 18 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»

№ п/п	Нормативные правовые акты
3	Приказ Федеральной службы по надзору в сфере связи и массовых коммуникаций от 17.07.2008 №08 «Об утверждении образца формы уведомления об обработке персональных данных»
4	Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
5	Решение ФСТЭК России от 05.03.2010[4]
6	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 15.02.2008 г.
7	«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 14.02.2008 г.
8	«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144
9	«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 обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622[5]
10	Приказ Мининформсвязи от 01.12.2009 № 630 «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных»

4 Данным решением первого заместителя директора ФСТЭК России отменены два документа:
— Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.
— Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.

Права субъекта персональных данных

Необходимо понимать, что требования Федерального закона № 152-ФЗ «О персональных данных» направлены в первую очередь на защиту субъекта персональных данных и его прав, а не на защиту персональных данных непосредственно.

При обработке персональных данных с должной степенью внимания необходимо учитывать права субъекта персональных данных, т. е. того физического лица, чьи данные обрабатываются.

Субъектом персональных данных является любое физическое лицо и именно человек вправе решать когда, кому и какие данные он предоставляет, а также он вправе проконтролировать как (каким образом) обрабатываются и кому передаются его персональные данные.

данных или его законным представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту ПДн и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

Особое внимание необходимо обратить на ограничения в части принятия решений на основании исключительно автоматизированной обработки ПДн, содержащиеся в ст. 16 Федерального закона «О персональных данных». В частности, предусмотрен запрет на принятие решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих права и законные интересы субъекта ПДн на основании исключительно автоматизированной обработки ПДн. Решение в такой ситуации может быть принято только при наличии соответствующего согласия субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Стоит напомнить, что оператор обязан разъяснить субъекту ПДн «порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов». При наличии возражений субъекта оператор обязан его рассмотреть в течение семи рабочих дней со дня получения и уведомить субъекта ПДн о результатах рассмотрения такого возражения.

Субъект ПД имеет право на получение сведений об операторе и информации, касающейся обработки его ПД, на доступ к своим ПД, на обжалование действий или бездействия оператора, а также на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

С учетом изложенного в организационно-распорядительных документах следует разработать порядок обеспечения возможности своевременно по запросу предоставлять информацию о персональных данных его законному владельцу - субъекту ПДн, а также в уполномоченный орган по защите прав субъектов ПДн.

Обязанности оператора персональных данных

Правам субъектов ЙДн корреспондируют обязанности операторов ПДн. Например, законом «О персональных данных» предусмотрено, что субъект ПДн имеет право получить сведения о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных. Соответственно, оператор обязан субъекту ПДн представить такую информацию.

В соответствии с определением, приведенным в ст. 3 Федерального закона «О персональных данных»:

ОПЕРАТОР - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Таким образом, исходя из данного определения, Федеральный закон «О персональных данных» касается всех лиц, осуществляющих обработку ПДн, ни для каких организаций, предпринимателей либо иных лиц каких-либо исключений не сделано.

ВНИМАНИЕ!

Любая организация или физическое лицо, в том числе предприниматель, осуществляющее обработку данных субъектов персональных данных является оператором персональных данных

Часть 1 ст. 7 Федерального закона «О персональных данных» обязывает операторов и третьих лиц, получающих доступ к персональным данным, обеспечивать конфиденциальность таких данных.

Напомним, что под конфиденциальностью информации понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее правообладателя.

От оператора ПДн требуется обеспечить состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т. е. сохранение в тайне от субъекта, не имеющего полномочий на ознакомление с ней, целостности и доступности информации при ее обработке техническими средствами, т. е. безопасность информации.

Таким образом, под информационной безопасностью понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

С учетом вышеизложенного предпринимаемые оператором ПДн меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного доступа, т. е. обеспечение того состояния информации, при котором доступ к ней осуществляют только субъекты, имеющего право);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Федеральным законом «О персональных данных» обязанность обеспечения конфиденциальности не распространяется:

1) на обезличенные персональные данные;
2) общедоступные персональные данные[7].

В соответствии с ч. 1 ст. 18 Федерального закона «О персональных данных» при сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную ч. 4 ст. 14 данного федерального закона, в том числе содержащую:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2) способы обработки персональных данных, применяемые оператором;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

7
Понятие «общедоступные персональные данные» подробно рассмотрено в главе «Организация и проведение мероприятий по защите персональных данных».

5) сроки обработки персональных данных, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

С учетом изложенного может быть рекомендовано разработать и закрепить во внутренних нормативных актах порядок предоставления такой информации субъектам ПДн.

В ряде случаев обязанность предоставления ПДн субъектом предусмотрена тем или иным федеральным законом. В таких случаях оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Также необходимо учитывать, что обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта ПДн (ст. 15 Федерального закона «О персональных данных»). Аналогичный порядок предусмотрен при обработке ПДн в целях политической агитации.

Если ПДн были представлены оператору не от субъекта ПДн (исключение составляют случаи предоставления данных на основании федерального закона, или если ПДн являются общедоступными), то оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных.

Данное требование предусмотрено ч. 3 ст. 18 Федерального закона «О персональных данных».

Отдельная статья Федерального закона «О персональных данных» уделена обязанностям оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных.

В соответствии с п. 1 ст. 21 Федерального закона «О персональных данных» предусмотрено временное блокирование ПДн, относящихся к соответствующему субъекту ПДн, на период проверки в случае выявления недостоверных ПДн или неправомерных действий с ними оператора при обращении или по запросу субъекта ПДн или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование. Причем такое блокирование осуществляется с момента такого обращения или получения такого запроса.

При подтверждении факта недостоверности ПДн оператор обязан уточнить ПДн и снять их блокирование, а в случае выявления неправомерных действия с ПДн в течение трех рабочих дней (с даты выявления неправомерности действий с ПДн) уничтожить ПДн. Кроме того оператор обязан прекратить обработку ПДн и уничтожить соответствующие ПДн в срок не превышающий 3-х рабочих дней в случае отзыва субъектом ПДн согласия на обработку своих ПДн, а также в случае если цели обработки ПДн были достигнуты. Об устранении допущенных нарушений или об уничтожении ПДн оператор обязан уведомить субъекта ПДн (его законного представителя), а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

В соответствии со ст. 19 Федерального закона «О персональных данных» *«оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».*

Таким образом, оператор ПДн обязан выполнить ряд обязательных требований в случае осуществления обработки ПДн. При этом необходимо исходить из системного подхода, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн с позиции комплексного применения тех-

Организация и проведение мероприятий по защите персональных данных

Как отмечалось выше, оператором персональных данных будет являться любая организация, любой предприниматель, осуществляющие обработку персональных данных. Несомненно, перечень мероприятий по защите персональных данных будет отличаться в различных организациях в зависимости от категории обрабатываемой информации, способа обработки сведений персонального характера и т. п. Например, минимальные требования будут предъявлены к тем организациям, которые передадут обработку данных специализированным организациям, имеющим соответствующие технические возможности и опыт в построении системы защиты ПДн (аутсорсинг). А для организаций, самостоятельно осуществляющих обработку сведений, например, медицинского характера (о состоянии здоровья), или избирательным комиссиям придется затратить на защиту персональных данных максимум сил и средств, в том числе финансовых.

Вместе с тем, как показывает практика, в целях минимизации расходов по защите персональных данных особо важно четко продумать и спланировать те меры, которые будут необходимы и достаточны в целях соблюдения законодательства о защите персональных данных.

На первый взгляд может показаться, что с выполнением мероприятий по защите ПДн своими силами не справиться, ведь в большинстве организаций нет не только службы безопасности, но даже специалиста по защите информации, а в ряде случае нет юриста, который обладает специальными знаниями в данной сфере. Как быть в такой ситуации, кто должен организовывать и проводить работу по защите персональных данных?

Но не зря русская поговорка гласит: «Глаза боятся, а руки делают». Попробуем разобраться, что необходимо осуществить, какими силами и средствами можно выполнить задуманное. Разумеется, что без четкого руководства не обойтись, в связи с чем, в настоящем пособии мы предлагаем практические пошаговые рекомендации по организации защиты ПДн.

Основные задачи и принципы построения системы защиты персональных данных

Система защиты персональных данных (далее - СЗПДн) представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

В соответствии с п. 1.2 Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного Приказом ФСТЭК России от 05.02.2010 №58 (регистрация в Минюсте РФ 19.02.2010, регистрационный № 16456) определено, что к методам и способам защиты информации в информационных системах относятся:

- методы и способы защиты информации, обрабатываемые техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий;

- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий.

Дополнительно стоит обратить внимание, что п. 1.3 рассматриваемого документа предусмотрено, что для выбора и реализации методов и способов защиты информации в ИСПДн оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных, либо может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Для достижения безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только пользователи, имеющие соответствующие право пользования);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

  к информации, циркулирующей в ИСПДн;

  средствам вычислительной техники ИСПДн;

аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

При построении СЗПДн необходимо учитывать такие основополагающие принципы как законность, системность, своевременность, комплексность, непрерывность, обязательность

контроля и т. п. Кроме того особое внимание при построении СЗПДн следует уделить вопросам снижения и оптимизации финансовых и трудовых затрат при приведении ИСПДн в соответствии с требованиями Федерального закона «О персональных данных».

Перечень объектов защиты персональных данных

Объектами защиты являются информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Объекты защиты включают:

1. Обрабатываемую информацию (сведения персонального характера).
2. Информационные технологии, используемые при обработке персональных данных.
3. Программно-технические средства обработки.
4. Средства защиты ПДн.
5. Каналы информационного обмена и телекоммуникации.
6. Объекты и помещения, в которых размещены компоненты ИСПДн.

Этапы построения системы защиты персональных данных

Мероприятия по организации защиты ПДн, обрабатываемых в ИСПДн, состоят из нескольких этапов:

- предварительный этап - стадия предпроектного обследования;
- классификация ИСПДн;
- разработка технического задания;
- стадия проектирования и создания системы защиты ПДн в составе ИСПДн;
- стадия ввода в действие ИСПДн и ее оценка соответствия требованиям безопасности информации.

Проведение предпроектного обследования и классификации ИСПДн обязательно для всех операторов ПДн. Для многих организаций именно данный этап может составлять до 90% всей необходимой работы.

Основными целями предпроектного обследования являются:

- установление необходимости обработки ПДн и ИСПДн;
- определение перечня ПДн, обрабатываемых в организации, объемов таких данных и целей их обработки, а также ситуаций (бизнес-процессов), при которых осуществляется обработка ПДн, определяются источники получения ПДн, оценка законности обработки ПДн и наличие согласия субъектов на обработку ПДн;
- определение режима обработки ПДн в ИСПДн;
- определение перечня лиц и степени участия персонала в обработке ПДн;
- определение конфигурации и топологии ИСПДн, физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения;
- определение технических средств и систем, используемых в ИСПДн, условий их расположения;
- иные факторы, которые могут оказать в дальнейшем влияние на организацию защиты ПДн.

С учетом проведенного предпроектного обследования устанавливается необходимость и проводятся следующие мероприятия:

1. Инвентаризация/обследование информационных системы ПДн, созданных/существующих в организации.
2. Формирование перечня подразделений и сотрудников, участвующих в обработке ПДн в рамках служебной деятельности (определение лиц, имеющих доступ к данным).

3. Проведение предварительного категорирования ПДн и классификации ИСПДн.
4. Разработка схемы документооборота, предусматривающей получение согласия субъектов ПДн.
5. Контроль и корректировка договорных отношений с субъектами.
6. Определение типа ИСПДн (типовая или специальная).
7. Формирование актуальной модели угроз в отношении каждой ИСПДн и разработка на основе модели угроз системы защиты ПДн.
8. Анализ возможности по выработке мер, направленных на снижение категорий обрабатываемых ПДн и в необходимых случаях проведение уточнения классов ИСПДн, составление и утверждение акта классификации ИСПДн.
9. Подготовка технического задания (ТЗ) по созданию требуемой системы защиты с учетом присвоенного класса защиты.
10. Проектировка и внедрение системы защиты ПДн, в т. ч. выполнение требований по инженерно- технической защите помещений, пожарной безопасности, охране, электропитанию и заземлению, санитарные и экологические требования.
11. При необходимости, определенной методическими документами ФСТЭК России и ФСБ России, получение необходимых лицензий.
12. Разработка пакета внутренних организационно-распорядительных документов, регламентирующих обработку ПДн, в том числе установление сроков хранения данных, а также условий прекращения об-работки ПДн.

В соответствии с определением, приведенным в ст. 3 Федерального закона «О персональных данных»:

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.

Кроме того, можно напомнить, что ранее понятие персональных данных было введено Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». Согласно данному акту к персональным данным относятся сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Несомненно, персональные данные есть в каждой организации. Наиболее наглядно область размещения ПДн можно продемонстрировать с помощью следующего рисунка.

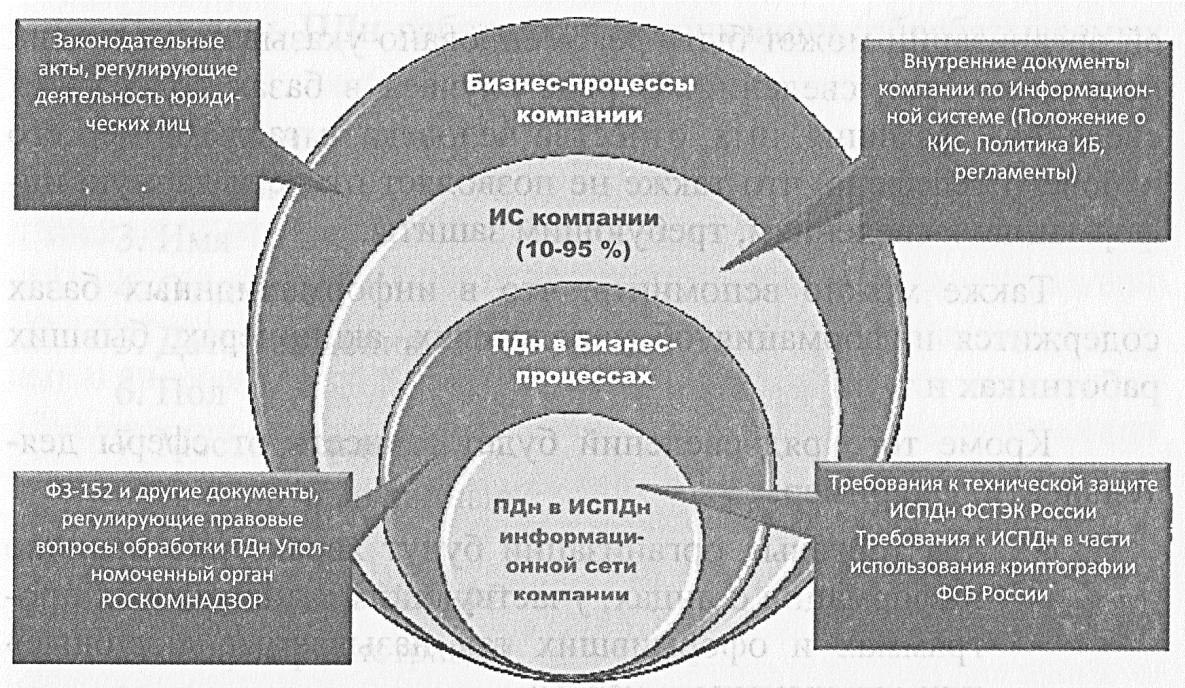


Рис. 2 «Область размещения персональных данных»

Какие же персональные данные обрабатывают в большинстве организаций?

В первую очередь к таким данным относятся ПДн работника - информация, которая необходима работодателю, чтобы заключить трудовой договор, заполнить личную карточку № Т-2. К таким сведения могут быть отнесены паспортные данные, семейное положение, сведения об образовании, номер страхового свидетельства обязательного пенсионного страхования, сведения о трудовой деятельности.

Во вторую очередь в информационных базах многих организаций содержатся сведения о контактных лицах контрагентов (фамилии, имена, отчества, должности в организациях, телефоны, адреса и т. п.). Говоря о данной категории сведений, стоит напомнить, что данные о руководителе другой организации можно найти в сети Интернет или в распространяемых базах данных, соответственно такие сведения могут быть отнесены к общедоступным. Получение согласия лица на обработку сведений, а также защита таких персональных данных не требуются. При внесении такой категории данных в базу сво

ей организации может быть рекомендовано указывать источник получения этих сведений. В ряде случаев в базах содержатся сведения - фамилия, имя, отчество человека, а также номер его рабочего телефона, что также не позволяет отнести данную информацию к сведениям, требующим защиты.

Также можно вспомнить, что в информационных базах содержится информация об учредителях, акционерах, бывших работниках и т. п.

Кроме того ряд сведений будет зависеть от сферы деятельности. Например:

- для торговых организаций будут характерно наличие информации о лицах, участвующих в дисконтных программах и оформивших так называемые «клубные» или «дисконтные» карты;
- у операторов связи будет информация о своих пользователях, а в жилищно-коммунальных службах - о жильцах;
- в медицинских центрах - о состоянии здоровья людей, проходивших лечение и обследования;
- в туристических фирмах - сведения о туристах;
- в образовательных учреждениях - о воспитанниках, учащихся, студентах, преподавателях и т. п.

Также в ряде организаций могут храниться дополнительные персональные данные, связанные с наличием заболеваний у работников при наличии вредных производств, сведения, полученные подразделениями безопасности, данные службы охраны
о посетителях и т. п.

Результатом проведенного исследования является полный перечень ПДн, обрабатываемых в ИСПДн организации. В случае обработки данных работников организации примером такого перечня может служить:

Перечень ПДн работников организации, обрабатываемых в ИСПДн:

1. Табельный номер
2. Фамилия
3. Имя
4. Отчество
5. Дата рождения
6. Пол
7. Место рождения
8. Паспортные данные
9. ИНН
10. Страховой № ПФР
11. Адрес регистрации
12. Адрес проживания
13. Контактные телефоны
14. Инвалидность
15. Вид договора
16. Подразделение
17. Должность
18. Стаж работы
19. Оклад

Если же в силу деятельности организации осуществляется обработка персональных данных ее клиентов, например, для учета выданных дисконтных карт, то данный перечень можно представить в следующем виде.

Перечень ПДн клиентов организации, обрабатываемых в ИСПДн:

1. Фамилия
2. Имя
3. Отчество
4. Дата рождения
5. Пол
6. Контактные телефоны
7. Номер дисконтной карты

8. Сумма накоплений на дисконтной карте

9. Размер предоставляемой скидки по дисконтной карте

Перечень требуемых мероприятий по защите персональных данных во многом зависит от категории обрабатываемых данных. Совместным приказом ФСТЭК России, ФСБ России и Роскомнадзора от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» установлены 4 категории персональных данных:

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

ПДн, отнесенные к категории 1, признаются специальной категорией ПДн. Обработка таких данных допускает только в случаях, предусмотренных ч. 2 ст. 10 Федерального закона «О персональных данных», в том числе, если:

1) субъект ПДн дал согласие в письменной форме на обработку своих ПДн;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта ПДн и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта ПДн невозможно;

4) обработка ПДн осуществляется в медико-ирофилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг ири условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка ПДн членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия в письменной форме субъектов ПДн;

6) обработка ПДн необходима в связи с осуществлением правосудия;

7) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

С учетом определенных выше ограничений осуществляется также обработка биометрических ПДн, т. е. сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные). Например, биометрические данные содержатся в «новых» загранпаспортах, получаемых российскими гражданами.

В соответствии с п. 4 ст. 19 Федерального закона «О персональных данных» «использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним,

уничтожения, изменения, блокирования, копирования, распространения». Стоит отметить, что обработка специальной категории ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных определены постановлением Правительства РФ от 06.07.2008 № 512. В частности предусмотрено, что материальный носитель - к которым относится машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность, должен обеспечивать:

- защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;
- возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими персональными данными;
- возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;
- невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

Кроме того, Федеральным законом «О персональных данных» определена еще одна категория - общедоступные ПДн - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных дан-

пых или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Общедоступные источники ПДн (в том числе справочники, адресные книги) могут создаваться в целях информационного обеспечения (ст. 8 Федерального закона «О персональных данных»). 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. Можно порекомендовать во избежание возможных споров «документировать» факты получения таких сведений, а также получать подтверждение, что у «источника» имеются требуемые законодательством письменные согласия. Требования, предъявляемые к защите таких ПДн, минимальны.

Например, фамилия, имя, отчество руководителя организации могут рассматриваться в качестве общедоступных и не
I юдлежащих защите персональных данных по следующим основаниям:

1) В соответствии с п. 1 ст. 5 Федерального закона от 08.08.2001 № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» (далее - Федеральный закон № 129-ФЗ) в ЕГРЮЛ содержатся сведения и документы
   о компании, в том числе фамилия, имя, отчество должность лица, имеющего право без доверенности действовать от ее имени, а также его паспортные данные и т. д.
2) Согласно п. 1 ст. 6 Федерального закона № 129-ФЗ содержащиеся в государственных реестрах сведения и документы являются открытыми и общедоступными, за исключением сведений, доступ к которым ограничен в соответствии с абзацем вторым настоящего пункта (в том числе к паспортным данным, банковским счетам и т. п.). Информация о фамилии, имени,

отчестве руководителя организации является открытой и общедоступной.

3) В соответствии с пп. 2 п. 2 ст. 7 Федерального закона № 152-ФЗ обеспечение конфиденциальности общедоступных персональных данных не требуется.

Определение цели и способов обработки ПДн

Следующим этапом обследования является определение целей и способов обработки ПДн.

Среди наиболее часто встречающихся целей обработки ПДн без учета отраслевой специфики можно выделить: трудовые отношения с работниками; оформление пропусков для входа на территорию предприятия; договоры бытового подряда, оформление дисконтных карт и т. п.

Под обработкой персональных данных понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

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

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

Уничтожение персональных данных - действия, в ре- 1ультате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные ноет ели персональных данных;

Обработка персональных данных может осуществляться с использованием средств автоматизации или без использования Іа к их средств. Необходимо отметить, что во многих организациях могут сочетаться автоматизированная и «неавтоматизированная» обработка персональных данных, так называемая смешанная обработка. При этом сочетание двух режимов обработки данных позволит оптимизировать организацию защиты персональных данных и существенно сократить расходы на нее.

Рассмотрим стандартную ситуацию.

В любой организации содержатся данные о бывших работниках, срок хранения таких сведений составляет 75 лет. При этом при большой «текучке» кадров сведений о «бывших работниках» может быть существенно больше, чем количество работников в настоящее время. Уничтожение записей в ин-<!)ормационной базе и хранение карточек формы Т-2 на бумажных носителях (в распечатанном виде) поможет уменьшить количество сведений о субъектах, обрабатываемых в ИСПДн, так как от количества субъектов, в отношении которых обрабатываются ПДн, непосредственно зависит класс ИСПДн, а соответственно и требования по защите ПДн. Данное обстоятельство особенно важно, если в базе обрабатываются данные в отношении субъектов ПДн нескольких организаций.

Перечень лиц, допущенных к обработке информации

При организации защиты информации особое внимание должно быть уделено максимально четкому определению пе

речня лиц - сотрудников организации, принимающих участие в обработке персональных данных или имеющих к ним доступ, т. е. разграничению прав доступа в зависимости от должностных обязанностей, а также вида персональных данных. Ведь чем меньше лиц имеет доступ к персональным данным, тем меньше вероятность утечки информации.

При проведении мероприятий по защите персональных данных следует определить категорию лиц - сотрудников организации, допущенных к обработке ПДн, в зависимости от их должностных обязанностей.

Условно можно выделить четыре основные категории:

1. Администратор ИСПДн - лицо, владеющее полной информацией о системном и прикладном программном обеспечении ИСПДн, обладающее правами конфигурирования и администрирования ИСПДн, которое имеет доступ ко всем данным и техническим средствам обработки информации.
2. Программист-разработчик ИСПДн (в данном случае речь может идти о сотруднике сторонней организации, осуществляющем сопровождение ИСПДн). Данное лицо обладает информацией о программных способах обработки информации в ИСПДн, а также о технических средствах, применяемые для обработки и защиты ПДн, обрабатываемых в ИСПДн.
3. Лица, осуществляющие обработку ПДн (операторы), т. е. имеющие право доступа к сведениям, отнесенным к ПДн, а также возможность внесения изменений в данную категорию сведений (например, редактирование ранее заявленных данных, добавление новых учетных записей, удаление и т. п.);
4. Лица, имеющие доступ только к чтению данных (просмотр данных, отбор и группировка по заданному критерию и т. д.), содержащихся в ИСПДн без возможности внесения каких-либо изменений (операторы).

Кроме того, доступ сотрудников к информации может и должен различаться в зависимости от задач, выполняемых подразделением.

Таблица № 6

Вид информации	Подразделение
(ведения о сотрудниках	Администрация Кадровое подразделение Бухгалтерия
Сведения о кандидатах на вакантные должности	Кадровое подразделение
И нформация о посетителях	Служба безопасности
Сведения о контактных лицах контрагентов (CRM-системы)	Отдел продаж
Информация о потенциальных клиентах	Отдел продаж
Данные учредителей и прочее	Юридический отдел
Приказы по личному составу	Канцелярия
Доверенности (например, на получение материальных ценностей)	Канцелярия (или АХО)

Конкретные права пользователей и отнесение их к той или иной категории подлежат определению при проведении обследования ИСПДн.

При предоставлении тех или иных полномочий целесообразно исходить из принципа «минимизации полномочий», который предусматривает, что доступ к ПДн предоставляется только в том случае и в том объеме, которые необходимы для выполнения должностных обязанностей сотрудника.

Предоставленные полномочия в дальнейшем должны быть закреплены в организационно-распорядительных документах.

Срок хранения информации

Другим вопросом, имеющим отношение к документации оператора персональных данных, является вопрос о сроках хранения персональных данных. В отношении персональных данных можно говорить о трех способах определения срока хранения информации, который может быть определен:

1) нормативным правовым актом;

2) достижением цели обработки данных;

3) явным указанием в согласии.

Наиболее простая ситуация имеет место, если срок хранения установлен в согласии субъекта. В такой ситуации стоит лишь помнить, что субъект ПДн не может указать срок меньший, чем предусмотрен нормативным правовым актом, устанавливающим срок хранения информации.

Например, Перечнем типовых управленческих документов, образующихся в деятельности организаций с указанием сроков хранения, утвержденным руководителем Федеральной архивной службы России от 06 октября 2000 года, установлены следующие сроки хранения документов в части расчетов с работниками организации:

- ***лицевые счета рабочих и служащих (форма Т-2) - 75 лет;***
- ***расчетные (расчетно-платежные) ведомости - 5 лет;***
- ***книги учета депонированной заработной платы, журналы регистрации исполнительных листов - 5 лет;***

• исполнительные листы - до минования надобности;

- ***справки, представляемые в бухгалтерию на оплату учебных отпусков, получения льгот по налогам и другие - до минования надобности;***
- ***договоры, соглашения (хозяйственные, операционные, трудовые и другие) - 5 лет.***

В зависимости от сферы деятельности необходимо анализировать законодательные и нормативные правовые отрасли, определяющие сроки хранения документов, содержащих персональные данные.

Например, п. 12 Правил взаимодействия операторов связи *с* уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденных
I Установлением Правительства РФ от 27.08.2005 № 538, предусмотрено, что оператор связи обязан хранить информацию об абонентах оператора связи и оказанных им услугам в течение грех лет.

Наиболее сложная ситуация может иметь место в случае установления срока хранения «по достижению цели обработки информации».

Например, физическое лицо заключает договор бытового подряда. Логично предположить, что цель обработки информации будет достигнута когда будет выполнен договор и заказчик (физическое лицо) примет результаты работ. Однако в ряде случаев может быть предусмотрена гарантия на определенный срок, т. е. договор продолжает действовать и после выполнения работ и в течение срока гарантийного обслуживания. По истечении этого срока информация о физическом лице должна быть удалена. Однако некоторые организации предпочтут сведения не уничтожать (например, в целях предоставления скидок при заключении следующих договоров или направления рекламной информации). В такой ситуации по окончании договора необходимо будет получить согласие у субъекта ПДн и предусмотреть новый срок обработки данных.

Таким образом, в локальных актах по организации необходимо определить сроки хранения информации. Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых ПДн подлежат уничтожению.

Итоговым документом/документами данного этапа должен быть утвержденный перечень обрабатываемых ПДн с ука-

занием цели обработки, режима обработки, объема информации, сроков хранения, а также лиц, допущенных к обработке сведений персонального характера.

Проведение предварительного анализа информационных ресурсов организации позволит получить информацию, необходимую для определения дальнейших шагов по выполнению требований Федерального закона «О персональных данных».

2. Особенности обработки ПДн без использования средств автоматизации

Особенности обработки ПДн, осуществляемой без использования средств автоматизации, утверждены соответствующим Постановлением Правительства РФ от 15.09.2008 г. № 687.

Пунктом 1 Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации, утвержденного указанным выше Постановлением, предусмотрено: ***«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».***

При этом отмечено, что 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.

Стоит отметить, что порядок обработки данных и в данном случае должен быть определен локальными правовыми актами организации с учетом требований поименованного выше Положения.

Какие требования данного положения необходимо учитывать:

- ПДн при их обработке 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) (п. 4 Положения);
- не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы (п. 5 Положения);
- для обработки различных категорий персональных данных, для каждой категории персональных данных должен использоваться отдельный материальный носитель (п. 5 Положения);
- обязательное раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях (п. 14 Положения);
- в отношении каждой категории ПДн можно определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- лица, осуществляющие обработку ПДн (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, а также локальными правовыми актами организации (при их наличии).

Пункт 8 данного положения посвящен порядку ведения журналов (реестров, книг), содержащих ПДн, необходимых для однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях.

При ведении такого журнала должны соблюдаться следующие условия:

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

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.

3. Получение согласия у субъекта ПДн на обработку его данных

Часто ли мы сталкиваемся с предоставлением своих персональных данных? Ответ может удивить: практически ежедневно. Например, совершая покупку в магазине, вам предлагают оформить дисконтную карту, для заполнения которой необходимо указать определенные сведения, в том числе фамилию, имя, отчество, дату рождения, а также адрес места жительства, адрес электронной почты, телефон и т. д. В другом месте при посещении бизнес-центра у вас могут потребовать паспорт для прохода на территорию и внести сведения в компьютер. Необходимо ли в этих случаях получать ваше согласие на их обработку? Постараемся ответить на эти вопросы.

В соответствии со ст. 9 Федерального закона № 152-ФЗ субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

Предоставление данных может быть обязательным и добровольным. Например, обязательное предоставление данных предусмотрено федеральными законами (напр. Трудовым кодексом РФ (ст. 65), Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования») в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (перечень приведен в п. 2 ст. 9 Федерального закона «О персональных данных».

В большинстве же случаев мы предоставляем персональные данные в добровольном порядке. При этом в ряде случаев получение согласия субъектов ПДн на обработку ПДн не требуется.

В соответствии с п. 2 ст. 6 Федерального закона № 152-ФЗ без получения согласия субъекта ПДн может осуществляться обработка персональных данных в следующих случаях:

- на основании федерального законодательства;
- в целях исполнения договора с субъектом персональных данных;
- в статистических или научных целях;
- для защиты жизни, здоровья субъекта персональных данных;
- для доставки почтовых отправлений организациями почтовой связи;
- в ходе профессиональной деятельности журналиста, ученого и т. д.

Кроме того, следует принимать во внимание, что обеспечение конфиденциальности ПДн не требуется в отношении общедоступных ПДн. Общедоступные источники ПДн (в том числе справочники, адресные книги и т. п.) могут создаваться в целях информационного обеспечения. В такие источники могут включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПДн.

Вместе с тем применять приведенные выше исключения необходимо с «должной степенью осмотрительности», так как на оператора возлагается обязанность представить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными.

В соответствии с п. 4 ст. 9 Федерального закона № 152-ФЗ согласие субъекта ПДн на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес опера- гора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва;

7) собственноручную подпись субъекта персональных данных.

Таким образом, уже в настоящее время при организации документооборота необходимо предусмотреть получение разрешения у субъектов ПДн на обработку данных.

Нетрудно заметить, что в самом согласии субъекта ПДн уже содержатся ПДн. В отношении таких данных необходимо учитывать положения п. 5 рассматриваемой статьи, который гласит: ***«для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется».***

В соответствии с ч. 6 ст. 9 Федерального закона «О персональных данных» в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных, а в случае субъекта ПДн согласие на

обработку его ПДн дают в письменной форме наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

Отдельно необходимо остановиться на получении согласия в форме электронного документа. Данные изменения внесены Федеральным законом от 27.07.2010 № 227-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об организации предоставления государственных и муниципальных услуг».

Внесенными изменениями предусмотрено, что «равнозначным содержащему собственноручную подпись письменному согласию субъекта персональных данных на бумажном носителе признается согласие в форме электронного документа, подписанного электронной цифровой подписью или в случаях, предусмотренных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами, иным аналогом собственноручной подписи».

Порядок получения согласия субъекта персональных данных в форме электронного документа на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, определяется Правительством Российской Федерации.

С учетом выше изложенного, необходимо организовать документооборот таким образом, чтобы имелась возможность получать разрешение (согласие) у человека (субъекта персональных данных) на обработку его данных, при этом необходимо четко указать в каких целях данная обработка осуществляется, а также в течение какого времени правомерно хранить полученные сведения. Также в ряде случаев может понадобиться форма «отзыва согласия».

Оператору персональных данных целесообразно разработать и утвердить список должностных лиц в организации (у предпринимателя), уполномоченных в получении персональных данных субъектов ПДн, а также определить порядок реагирования на обращения субъектов ПДн, предусмотреть возможные варианты ответов и действий, установить сроки реагирования, а также ответственных за соблюдение установленного порядка. Такой порядок следует «закрепить» в организационнораспорядительных документах организации. Например, могут быть разработаны «Правила получения согласия у субъекта персональных данных», «Положение о порядке и сроках подготовки ответов на обращения субъектов персональных данных» и иные аналогичные документы (приказы, инструкции, процедуры). В качестве необходимых документов в организации следует разработать и использовать журналы учета получения согласий, а также журналы обращений субъектов персональных данных.

Могут быть предложены следующие образцы документов.

Пример № 1

Согласие на обработку персональных данных

№ _____ « _____ » _____ 20___ г.

_____ именуемый в дальнейшем «Субъект персональных данных» разрешает _____ _____ , в лице ответственного за обработку персональных данных _____ далее «Оператор», обработку персональных данных, приведенных в пункте 3 настоящего согласия на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение следующих действий: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», в следующих целях:

- в целях исполнения трудового договора;
- для обеспечения личной безопасности, защиты жизни и здоровья работника;
- в целях ведения финансово-хозяйственной деятельности организации;
- иное (необходимо точное указание целей).

2. Перечень персональных данных, передаваемых Оператору на обработку (нужное подчеркнуть):

- дата и место рождения;
- биографические сведения;
- сведения об образовании (образовательное учреждение, время обучения, присвоенная квалификация);
- сведения о местах работы (город, название организации, должность, сроки работы);
- сведения о семейном положении, детях (фамилия, имя, отчество, дата рождения);
- сведения о месте регистрации, проживании;
- контактная информация;
- паспортные данные;
- сведения о постановке на налоговый учет (ИНН);
- сведения о регистрации в Пенсионном фонде (номер страхового свидетельства);
- сведения об открытых банковских счетах;
- иное (необходимо точное указание).

3. В соответствии с пунктом 4 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных.

4 Срок действия данного согласия устанавливается на период:

с _____ по _____

(>поратор вправе осуществлять следующие действия с указанными выше персональными данными (нужное подчеркнуть):

- **сбор;**
- **систематизацию;**
- **накопление;**
- **хранение;**
- **уточнение (обновление, изменение);**
- **использование;**
- **распространение/передачу[9];**
- **блокирование;**
- **уничтожение;**
- **иное (необходимо точное указание).**

Г» Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Данные об операторе персональных данных:
Наименование организации _____;
Адрес оператора _____ ;
Ответственный за обработку ПДн _____

Субъект персональных данных:
Фамилия, имя, отчество _____
Адрес

Паспортные данные _____ выдан _____

_____ / _____
Подпись ФИО

t)

Необходимо конкретизировать, какое распространение - внешнее (наиример, передача сведений в банк, страховую компанию и т. п.), внутреннее, размещение в Интернете.

Пример № 2

Согласие на обработку персональных данных (в случае получения данных у третьих лиц/передачи данных третьим лицам)

Руководителю
ООО « _____ **»**

от _____
фамилия, инициалы заявителя

должность

структурное подразделение

Не возражаю против _____ **Вами сведений обо мне,**
получения/сообщения
содержащих данные о/в отношении _____

перечень персональных данных
полученных/переданных

указать откуда могут быть получены или куда переданы персональные данные **с целью**

указать цель обработки персональных данных
В форме _____
документальной / электронной
В течение _____
указать срок действия согласия

Настоящее заявление может быть отозвано мной в письменной форме

Подпись заявителя Дата

Отзыв согласия на обработку персональных данных

Руководителю
ООО « _____ »

от _____
фамилия, инициалы заявителя

Настоящим во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я _____

(фамилия, инициалы заявителя)
паспорт _____ выдан _____ ,
зарегистрированный _____

отзываю у ООО « _____ » свое согласие на обработку моих персональных данных, представленных в целях _____

Прошу прекратить обработку моих персональных данных в срок, не превышающий трех рабочих дней с даты поступления настоящего отзыва.

(подпись, фамилия, инициалы заявителя)

Дата

ЖУРНАЛ УЧЕТА СОГЛАСИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Дата, № согласия	Субъект ПДн	Перечень ПДн, на обработку которых дается согласие	Цель обработки ПДн	Срок, в течение которого действует согласие	Подпись лица, получившего согласие

ЖУРНАЛ УЧЕТА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ О ВЫПОЛНЕНИИ ИХ ЗАКОННЫХ ПРАВ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ[10]

№ п/п	Дата, № и реквизит запроса	Запрашивающее лицо	Состав запрашиваемых данных	Требуемая информация и цель ее получения	Отметка о предоставлении или отказе в предоставлении информации	Дата передачи отказа в пре-доставлении информации	Причина отказа	Подпись запрашивающего лица	Подпись ответственного сотрудника	Место хранения информации

10 „

В ряде случаев может также вестись журнал учета передачи персональных данных по аналогичной форме. В данном журнале следует отражать факты передачи персональных данных по запросам государственных органов.

4. Уведомление Роскомнадзора

Начиная с 2008 года после утверждения формы уведомления у операторов, осуществляющих обработку персональных данных, появилась новая обязанность в части направления уведомление в уполномоченный орган по защите прав субъектов персональных данных.

В соответствии с п. 1 ст. 22 Федерального закона «О персональных данных» оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по шщите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Порядок ведения реестра операторов, осуществляющих обработку ПДн, внесения, изменения, исключения сведений, а также предоставления выписок из реестра утвержден Приказом Министерства связи и массовых коммуникаций РФ от
30.01.2010 № 18 «Об утверждении административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных» (зарегистрировано в Минюсте РФ 24.03.2010 № 16717).

В реестре содержатся следующие сведения об Операторах персональных данных:

1. регистрационный номер;
2. наименование (фамилия, имя, отчество), адрес Оператора;
3. адреса филиалов (представительств) Оператора, осуществляющих обработку персональных данных (при наличии);
4. дата направления уведомления;
5. цель обработки персональных данных;
6. категории персональных данных;

7. категории субъектов, персональные данные которых обрабатываются;
8. правовое основание обработки персональных данных;
9. перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;
10. описание мер, которые Оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
11. дата начала обработки персональных данных;
12. срок или условие прекращения обработки персональных данных;
13. дата и основание внесения сведений об Операторе в Реестр;
14. дата и основание внесения изменения сведений об Операторе из Реестра;
15. дата и основание исключения сведений об Операторе из Реестра.

Соответственно, исходя из перечня данных сведений формируется и форма уведомления, направляемого в Роском- надзор.

По состоянию на 1 февраля 2011 года в реестре зарегистрировано более 170 тыс. операторов ПДн. Вместе с тем в качестве оператора ПДн может быть рассмотрено практически любое юридическое лицо, а в ряде случаев и физические лица.

В представленном отчете за 2009 год Роскомнадзор акцентирует внимание на том, что общая прогнозная численность операторов составляет 5-7 млн, т. е. доля зарегистрированных операторов от общей прогнозной численности (на конец 2009 года) составляет менее 2 %.

В отчете особо отмечается, что ***«существует группа операторов, среди которых бытует ошибочное мнение о том, что факт непредставления уведомления об обработке ПДн исключает возможность проверки Уполномоченным органом»,*** в свя- ш с чем уполномоченным органом принято решение о внедрении практических механизмов повышения эффективности дея- юльности по формированию Реестра, в том числе в части реали- ищии мер по привлечению к административной ответственно-
11и Операторов, осуществляющих обработку ПДн без уведом- исния уполномоченного органа.

Также стоит обратить внимание, что 54 протокола об административных правонарушениях, направленных в суд, были составлены по фактам непредставления или несвоевременного представления в уполномоченный орган уведомления об обработке ПДн, непредставления сведений об изменении информации, содержащейся в уведомлении, а также непредставления либо несвоевременного представления информации на запрос уполномоченного органа.

Регистрация в реестре осуществляется в территориальных подразделениях Роскомнадзора, которые созданы практически ко всех субъектах Российской Федерации.

Организаций, для которых сделаны исключения, перечислены в п. 2 ст. 22 Федерального закона № 152-ФЗ. Операторы без уведомления Роскомнадзора вправе осуществлять 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) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

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

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

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

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

Анализ данного перечня исключений показывает, что практически каждая организация должна направить уведомление в Роскомнадзор, так как в архиве любой организации можно найти сведения о бывших сотрудниках.

Форма уведомления утверждена Приказом Федеральной службы по надзору в сфере связи и массовых коммуникаций Министерства связи и массовых коммуникаций Российской Феи-рации от 17.07.2008 № 08.

В соответствии с установленным порядком уведомление тлжно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с шконодательством Российской Федерации и содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых (нарабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персо-нальных данных;

7) описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению ос^опасности персональных данных при их обработке;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных.

Необходимо отметить, что с учетом рекомендаций, подготовленных Роскомнадзором и размещенных на сайте ведомства (www.rsoc.ru) , перечень информации, которую нужно указать при заполнении уведомления более широкий. Например, заполняя поле ***«описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке»*** указывается класс ИСПДн, организационные и технические меры,

применяемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

Далее Роскомнадзор в течение 30 дней вносит сведения в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

Необходимо помнить, что в случае изменения предоставленных сведений оператор обязан уведомить об изменениях уполномоченный орган в течение 10 дней с даты возникновения таких изменений.

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

УВЕДОМЛЕНИЕ[11] 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)

11 _____

и надлежащих: _____

(категории субъектов, ПДн которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем _____

(перечень действий с ПДн, общее описание

используемых оператором способов обработки ПДн)

(описание мер, которые оператор обязуется осуществлять при обработке

персональных данных, по обеспечению безопасности *ПДн при их обработке)*

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных: _____

должность **подпись** **расшифровка подписи**

“ ____ ” _____ 20 _____ г.

[11] Утверждено Приказом Роскомнадзора от 17.07.2008 № 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 Роскомнадзора).

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; место нахождения;
индивидуальный номер налогоплательщика (ИНН).

4.2. Для физических лиц:

фамилия, имя, отчество физического лица (оператора);

местонахождение;

данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ;
ИНН.

4.3. Для государственных, муниципальных органов (операторов):

полное и сокращенное наименование государственного, муниципального органа;

наименование территориального(ых) органа(ов), осуществляющего^) обработку персональных данных; место нахождения;
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) (Примечание № 1).

Примечание № 1: 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:

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, и другие категории персональных данных, обрабатываемые оператором, не указанные в настоящем пункте).

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 (Примечание № 1);

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 (Примечание N 2).

Примечание N 1: Указываются не только соответствующие статьи Федерального закона «О персональных данных", но и статьи иного нормативноправового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных. (Например: ст. ст. 85 - 90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона "Об актах гражданского состояния" и др.)

Примечание № 2: 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 (Примечание N 1).

Примечание № 1: При автоматизированной обработке персональных данных либо 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 сети общего пользования Интернет, 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:

а) класс информационной системы персональных данных оператора (пункт 14 Приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных";

б) организационные и технические меры, применяемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

В случае использования оператором, осуществляющим обработку персональных данных, шифровальных (криптографических) средств указываются следующие сведения:

а) наименование, регистрационные номера и производителей используемых криптографических средств;

б) уровень криптографической защиты персональных данных;

в) уровень специальной защиты от утечки по каналам побочных излучений и наводок;

г) уровень защиты от несанкционированного доступа.

Предоставление данной информации осуществляется в соответствии с Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/5-144.

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 прекращение обработки персональных данных.

5. Инвентаризация/обследование информационных систем ПДн в организации

Основной задачей инвентаризации/обследования информационных систем является выявление ИС, в которых осуществляется обработка персональных данных (например, система бухгалтерского учета, кадровый учет, система взаимоотношений с клиентами, биллинговая система и т. п.).

И Н ФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Если в небольшой организации, скорее всего, создана одна информационная система ПДн, в крупных - таких систем будет несколько, причем обрабатываемые в них данные могут относится к различным категориям.

Как показывает практика внедрение мер по защите ПДн без предварительного анализа и оптимизации процессов обработки ПДн может привести к неоправданному удорожанию системы защиты ПДн. Оптимизация процессов обработки позволяет не только снизить стоимость работ по организации защиты персональных данных, но и повысить эффективность бизнес- процессов Заказчика.

Обследование ИСПДн включает:

- обследование персональных данных обрабатываемых в ИСПДн;
- обследование и анализ ИТ-инфраструктуры ИСПДн;
- изучение и анализ процедур обработки ПДн;

- обследование и анализ применяемых средств защиты информации;
- использование антивирусных программ и т. п.

При проведении обследования может быть рекомендовано составление опросных листов, учитывающих специфику деятельности оператора, проведение анализа полученной информации с целью возможного понижения класса ИСПДн, выявление бизнес-процессов, анализ организационной структуры и т. п.

6. Проведение классификации и присвоение класса информационной системе

Еще одним обязательным мероприятием, которое обязаны осуществить все без исключения операторы информационных систем, является проведение классификации и присвоение класса информационной системе. При проведении классификации необходимо руководствоваться совместным Приказом ФСТЭК РФ (Федеральной службы по техническому и экспортному контролю), ФСБ РФ и Министерства информационных технологий и связи РФ от 13.02.2008 № 55/86/20 (далее - приказ № 55/86/20).

Порядок проведения классификации ИСПДн можно представить в виде следующей схемы.

Рис. 3 Порядок проведения классификации

Ответим на наиболее важные вопросы, возникающие при проведении классификации ИСПДн.

Цель проведения классификации

Установление методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных (п. 3 Порядка, утв. Приказом № 55/86/20).

ВНИМАНИЕ!
Классификация проводится именно в отношении информационной системы, а не программного обеспечения.

Когда проводим?

Классификация информационных систем персональных данных может проводиться:

- на этапе создания информационных систем
- в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) (п. 3 Порядка, утв. Приказом № 55/86/20).

ВНИМАНИЕ!
Все операторы ПДн обязаны провести классификацию ИСПДн до 01 июля 2011 года.

Кто проводит?

В соответствии с п. 2 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 (далее - Приказ ФСТЭК России № 55/8/20) классификация ИСПДн 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.

Т. е. классификация проводится самой организацией. Несомненно, если организация «сомневается в своих силах», то in я проведения классификации следует привлечь стороннюю организацию, специализирующуюся на оказании данных видов услуг.

Какие данные учитываем при проведении классификации типовых ИСПДн?

Категория обрабатываемых в информационной системе ИДн-Хпд

К перечню обрабатываемой информации необходимо подойти с особой тщательностью, ведь от этого напрямую зависит класс информационной систем и, соответственно, сумма расходов на проведение мероприятий по защите ПДн.

В соответствии с Приказом ФСТЭК России № 55/8/20 различают 4 категории данных:

- Обезличенные и (или) общедоступные данные (Х4);
- ПДн, позволяющие идентифицировать субъекта ПДн (Х3);
- ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1 (Х2);
- ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (XI).

Как следует из приведенных выше категорий персональных данных, в случае внесения в информационную систему данных о состоянии здоровья требования, предъявляемые по тщите таких данных, максимальные.

Возьмем для примера сведения, подлежащие учету в программе «1С:Бухгалтерия 8». Например, при внесении записи в справочник «Физические лица» подлежат указанию следующие сведения:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- место рождения;
- паспортные данные физического лица;
- гражданство;
- инвалидность;
- страховой номер свидетельства в ПФР;
- ИНН.

Кроме того, в базе данных будет также содержаться информация об адресе места жительства физического лица, телефоне, должности и другие сведения, в том числе финансового характера.

Данные сведения не содержат информацию, при обработке которой мы должны были бы признать обработку данных относящихся ко 2 или 3 категории. Если обрабатываются данные о состоянии здоровья (например, в медицинских учреждениях), то категории данных будет максимальна, т. е. XI.

В ряде случаев могут возникнуть вопросы по поводу таких сведений как гражданство, инвалидность, беременность. Несмотря на то, что любой человек может дать определение данным терминам, вопросы с точки зрения категорирования персональных данных могут возникнуть.

Например, понятие гражданства. Ведь мы понимаем, что гражданство не является синонимом национальная принадлежности, а вводится только с учетом различных требований по правильному исчислению налогов и взносов, которые различны для резидентов РФ и нерезидентов.

Еще больше сомнения вызывает графа инвалидность. Не может ли данное сведение трактоваться как состояние здоровья? А данный термин в настоящее время в действующем законодательстве не определен. Анализ действующего законодательства показывает, что в настоящее время в нормативных правовых актах, принятых на федеральном уровне, отсутствует четкое оп

ределение термина «состояние здоровья». По мнению авторов, в качестве определения можно рассматривать ст. 31 Закона Российской Федерации от 22.07.1993 № 5487-1 «Основы законодательства Российской Федерации об охране здоровья граждан». В соответствии с рассматриваемой нормой при определении состояния здоровья учитываются сведения о результатах обследования, наличии заболевания, его диагнозе и прогнозе, методах лечения, связанном с ними риске, возможных вариантах медицинского вмешательства, их последствиях и результатах проведенного лечения.

Вместе с тем признание гражданина инвалидом согласно соответствующим правилам, утвержденным Постановлением Правительства РФ от 20.02.2006 № 95, ***«осуществляется при проведении медико-социальной экспертизы исходя из комплексной оценки состояния организма гражданина на основе анализа его клинико-функциональных, социально-бытовых, профессионально-трудовых и психологических данных с использованием классификаций и критериев, утверждаемых Министерством здравоохранения и социального развития Российской Федерации».*** Группа инвалидности - понятие социальное и введено именно с целью классификации людей с отклонениями состояния здоровья с целью оказания им социальной помощи. Цель введения этого понятия и заключается в том, чтобы социальные работники, чиновники не имели информации о состоянии здоровья (диагнозах), но могли оказывать предусмотренную законом социальную помощь таким людям соразмерно состоянию здоровья. Ведь по группе инвалидности нельзя определить диагноз.

Таким образом, говорить, что данные термины синонимичны, некорректно. Данные об инвалидности опять же необходимы для правильного применения налогового законодательства. Аналогично можно говорить и в отношении сведений о нетрудоспособности, учитываемых при начислении пособий по временной нетрудоспособности.

Таким образом, можно говорить, что персональные данные, вводимые в «1С:Бухгалтерию 8», соответствуют классу К2. Необходимо учитывать, что в случае дополнения базы дополнительными реквизитами организация рискует понизить класс и соответственно будет обязана повысить требования по защите этой информации.

Дополнительно стоит отметить, что в настоящее время нет четкого разграничения между ПДн, относящимися к категории 2 (ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1), и ПДн категории 3 (ПДн, позволяющие идентифицировать субъекта ПДн).

Объем обрабатываемых персональных данных (количество объектов персональных данных, ПДн которых обрабатываются в информационной системе) - Х нпд

Данная характеристика на первый взгляд кажется относительно простой. При определении класса информационной системы ПДн необходимо определить в какой диапазон попадает ИСПДн вашей организации исходя из объема обрабатываемых данных:

- в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации (Х3);
- в информационной системе одновременно обрабатываются персональные данные от 1 ООО 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 (Х2);

- в информационной системе одновременно обрабатываются персональные данные более чем 100 ООО субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом (XI).

При расчете данного показателя стоит учитывать содержащуюся в базе информацию о работниках, бывших работниках, акционерах (учредителях), клиентах, контактных лицах в различных организациях (поставщиках, покупателях) и т. п.

При этом при обработке данных в рамках одной организации (независимо от численности) следует исходить из порядка, предусмотренного для ИСПДн, в которой обрабатываются ПДн не более чем 1 ООО субъектов. Таким образом, в особую «группу риска» попадают те лица, в информационных базах которых содержится информация о деятельности нескольких организаций и соответственно сведения о субъектах ПДн, имеющих отношения к нескольким операторам ПДн, например, информационные базы групп компаний (холдингов).

В данном случае для уменьшения затрат на дальнейшее создание системы защиты ИСПДн можно рекомендовать произвести разделение единой ИСПДн на несколько, в которых будут обрабатываться ПДн субъектов, относящиеся лишь к одной организации, предварительно оценив экономическую целесообразность процесса.

Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе

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

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

Специальные информационные системы - 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).

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.

В данном случае необходимо учитывать, чего оператор больше боится - утечки или искажения/утраты данных, а чего «боится субъект ПДн». Например, платежная система боится больше искажения - деньги не тому заплатят, чем утечки; субъект воинского учета - призывник - может только радоваться, если данные о нем потеряются; и, соответственно, оператор готов больше вкладываться в предотвращение утечки или в сохранность данных от вирусов или «сбоя железа».

Структура информационной системы

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);

f

- 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).

Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена

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

Причем под удаленным доступом, в соответствии с определением, данным в «NIST SP 800-53 Recommended Security Controls for Federal Information Systems» (Национальный институт стандартов и технологий, США), стоит понимать любой доступ к информационной системе организации пользователем (или процессом, действующим от имени пользователя), осуществляемый через внешнюю сеть/сеть общего пользования (например, Интернет).

Режим обработки персональных данных

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

Системы с разграничением прав доступа пользователей информационной системы или без

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

Местонахождение технических средств информационной системы

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 находятся за пределами Российской Федерации.

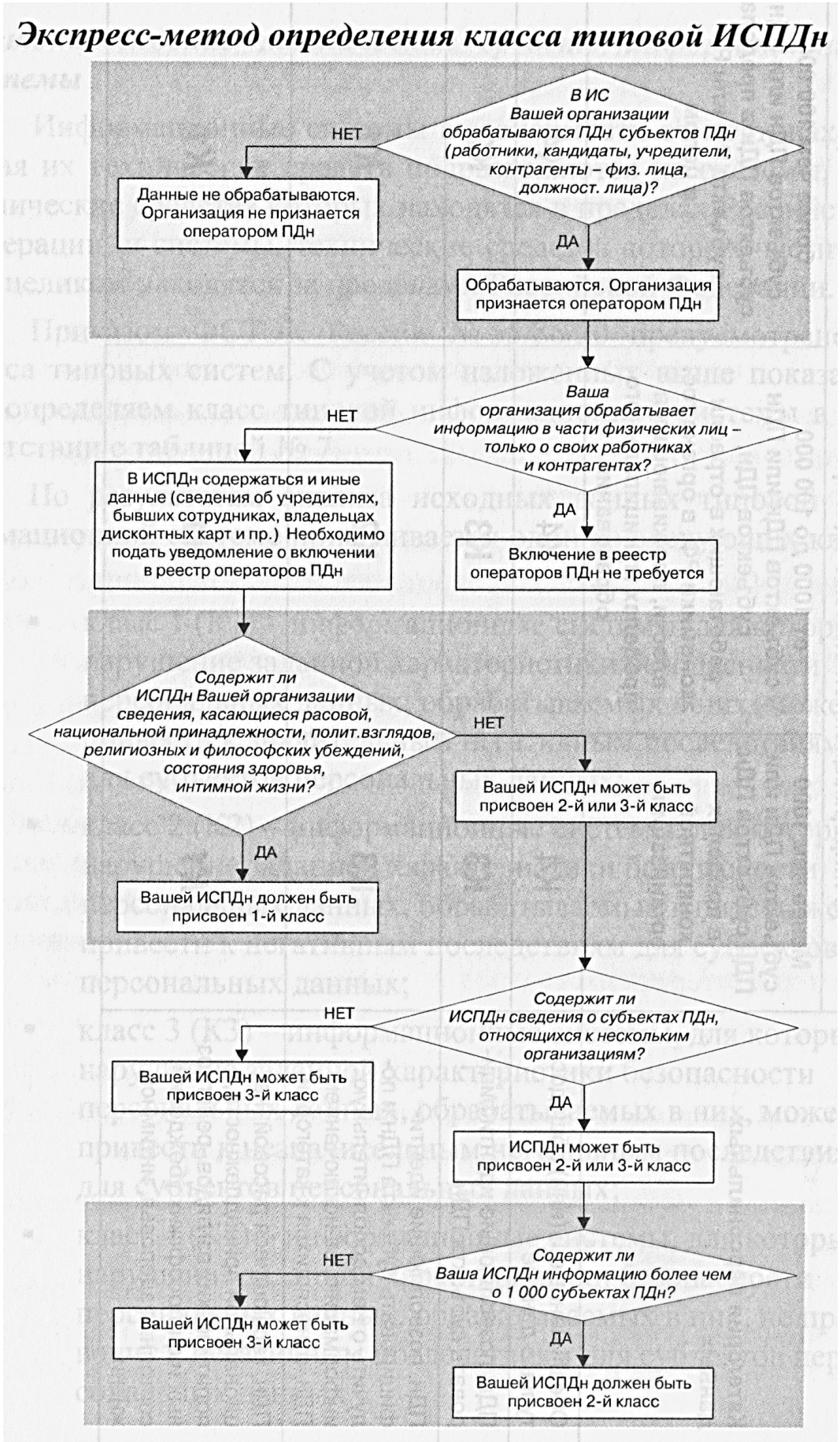
Приказом ФСТЭК России № 55/86/20 предусмотрено 4 класса типовых систем. С учетом изложенных выше показателей определяем класс типовой информационной системы в соответствии с таблицей № 7.

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.

Категория персональных данных	В информационной системе одновременно обрабатываются данные		
	Менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе гос. власти, проживающих в пределах муниципального образования	более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
Обезличенные и (или) общедоступные данные	К4	К4	К4
ПДн, позволяющие идентифицировать субъекта ПДн	К3	К3	К2
ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1	К3	К2	*К1*
ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.	*К1*	*К1*	*К1*

Экспресс-метод определения класса типовой ИСПДн



Для ИСПДн 2 и 3 классов может быть предложено следующее решение д
защиты ПДн.

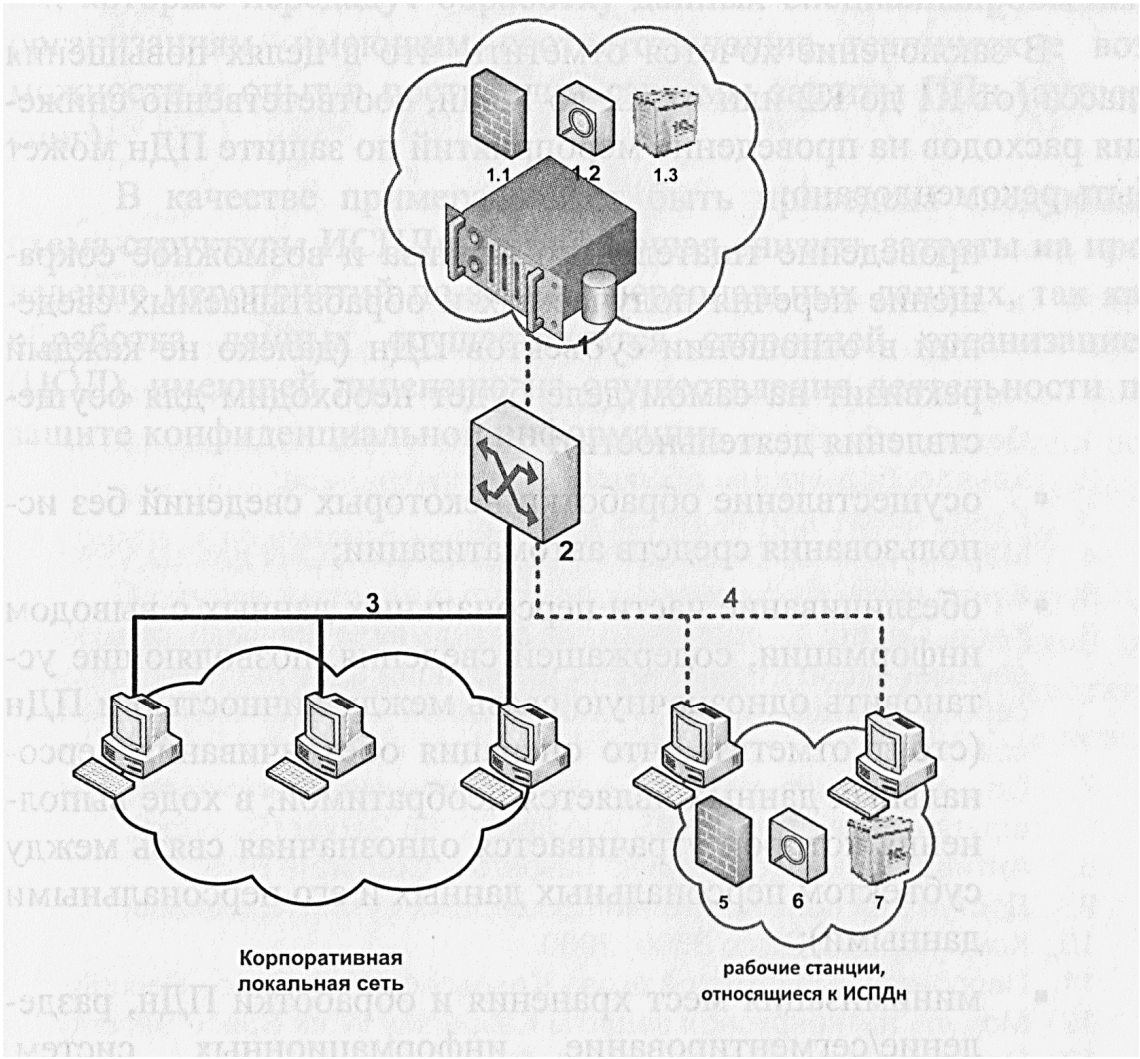


Рис. № 4

1. **Сервер обработки персональных данных:**
   1.1 .Персональный экран Kaspersky Business SpaceSecurity;
   1.2. Модуль антивирусной защиты Kaspersky Business SpaceSecurity;
   1.3. Сервер приложений 1С:Предприятие 8.2.
2. **Коммутаторы поддерживающие VLAN: Cisco 3560, 2960.**
3. **Локальная компьютерная сеть, принадлежащая к виртуальной сети № 1 (закрыт доступ к станциям и серверу обрабатывающим персональные данные).**
4. **Локальная компьютерная сеть, принадлежащая к виртуальной сети № 2.**
5. **Персональный экран Kaspersky Work Space Security.**
6. **Модуль антивирусной защиты Kaspersky Work Space Security.**
7. **Платформа 1С:Предприятие 8.2.**

Меры по снижению расходов на проведение мероприятий по защите ПДн

В заключение хочется отметить, что в целях повышения класса (от К1 до К2 или от К2 до КЗ) и, соответственно снижения расходов на проведение мероприятий по защите ПДн может быть рекомендовано:

- проведение тщательного анализа и возможное сокращение перечня получаемых и обрабатываемых сведений в отношении субъектов ПДн (далеко не каждый реквизит на самом деле будет необходим для осуществления деятельности);
- осуществление обработки некоторых сведений без использования средств автоматизации;
- обезличивание части персональных данных с выводом информации, содержащей сведения, позволяющие установить однозначную связь между личностью и ПДн (стоит отметить, что операция обезличивания персональных данных является необратимой, в ходе выполнения которой утрачивается однозначная связь между субъектом персональных данных и его персональными данными);
- минимизация мест хранения и обработки ПДн, разделение/сегментирование информационных систем, снижение требований к части сегментов;
- сокращение числа сотрудников, имеющих доступ к персональным данным;
- выделение рабочих мест, где используются ПДн в отдельную локальную вычислительную систему и организация защиты только ее;
- отключение ИСПДн от сетей общего пользования;
- обеспечение обмена с другими АРМ с помощью сменных носителей;
- передача по каналам связи только обезличенной информации.

Как отмечалось ранее, минимальные требования по защите персональных данных будут предъявлены ***к*** тем организациям, которые передадут обработку данных специализированным организациям, имеющим соответствующие технические возможности и опыт в построении системы защиты ПДн (аутсорсинг).

В качестве примера может быть приведена следующая схема структуры ИСПДн, позволяющая снизить затраты на проведение мероприятий по защите персональных данных, так как обработка данных осуществляется сторонней организацией (ЦОД), имеющей лицензию на осуществление деятельности по шщите конфиденциальной информации.

Решение для Класса 3 с ЦОД-ом (***1С:Предприятие 8.2 + KAV 6.0)***

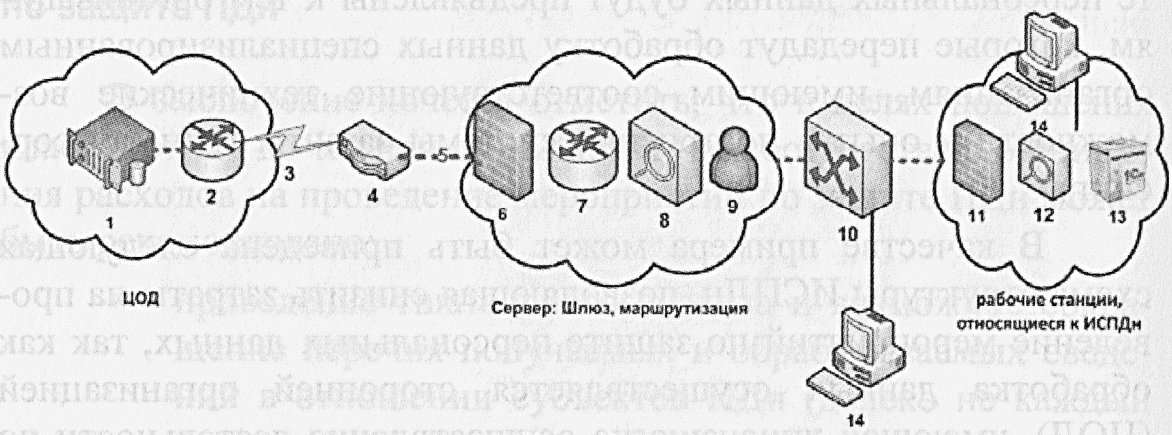


Рис. 5

1. Сервер обработки данных;
2. Каналообразующее оборудование провайдера;
3. Канал связи протокола L3 VPN;
4. Маршрутизатор Cisco 2811 – выделенный VLAN для L3 VPN;
5. Канал связи в офисе;
6. Kerio Control – программный брандмауэр (firewall) обеспечивающий защиту при сетевой трансляции адресов (NAT), прокси сервер, маршрутизация, блокирование нежелательных ресурсов;
7. Служба маршрутизации с настроенными статическими маршрутами средствами MS Windows 2008 Server (Standart);
8. Антивирусный мониторинг Kaspersky Corporate BSS;
9. Доступ для пользователей прошедших аутентификацию;
10. Коммутаторы Cisco 3560, 2960
11. Персональный сетевой экран Kaspersky Work Space Security;
12. Модуль антивирусной защиты Kaspersky Work Space Security;
13. Платформа 1С:Предприятие v.8.2;
14. Компьютеры организации, не работающие в ИСПДН.

По итогам проведения классификации необходимо получить документы, отражающие, что сделано, кем, в какой период, какие данные проанализированы, какой класс присвоен и т. п. То есть результатом данного этапа обследования информационной системы должны быть акт категорирования персональных данных и акт классификации информационной системы ПДн.

В соответствии с п. 19 совместного приказа № 55/86/20 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.

Проводить проверку информационной системы на предмет ее соответствия заявленному классу имеют право ФСТЭК РФ и ФСБ РФ. Если в ходе проверки выяснится, что класс системы занижен, то контролирующий орган потребует принять все меры для обеспечения безопасности, необходимые для реального уровня информационной системы персональных данных.

В случае неправильного определения ИСПДн по результатам проверки ФСТЭК может быть вынесено предписание об устранении выявленных нарушений. Какие-либо более жесткие административные меры могут наступить только в случае невыполнения настоящего предписания.

7. Вид информационной системы

По типу информационные системы делятся на типовые и специальные. Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных, а специальные информационные системы - 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.

Как правило, в информационных системах, которые ведутся с целью кадрового, бухгалтерского, управленческого учета, важно обеспечить не только конфиденциальность, но и защищенность от уничтожения и изменения. Следовательно, подавляющее большинство информационных систем следует рассматривать в качестве специальных.

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.

Для специальных ИСПДн требуется провести работу по моделированию возможных угроз. Формирование Модели угроз безопасности персональных данных является необходимым этапом в создании системы защиты персональных данных согласно пп. 12а Постановления Правительства РФ от 17 ноября 2007 г.

№781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». При этом модель угроз позволит применять именно те контрмеры, которые актуальны для условий использования защищаемой системы.

ФСТЭК России и ФСБ России разработаны следующие методические документы, определяющие порядок формирования модели угроз:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 15.02.2008 г.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 14.02.2008 г.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России, 21.02.2008 г, № 149/54-144.

Методика определения актуальных угроз безопасности предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных:

- государственных или муниципальных ИСПДн;
- ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями (далее - организациями) независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением;
- ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

Исходные данные для определения актуальных угроз формируются на основе перечней источников угроз (опрос), уязвимых звеньев ИС (опрос и сканирование сети) и, наконец, перечня технических каналов утечки (обследование ИС). Порядок определения актуальных угроз безопасности ПД в ИСПДн предусматривает следующие этапы:

- оценка (на основе опроса и анализа) уровня исходной защищенности ИСПДн (высокий, средний, низкий);
- экспертная оценка частоты (вероятности) реализации угрозы (маловероятная, низкая, средняя, высокая);
- определение актуальных угроз (путем исключения неактуальных угроз по определенному алгоритму, описанному в методике).

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз на основе Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного Приказом ФСТЭК России от 05.02.2010 №58 формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

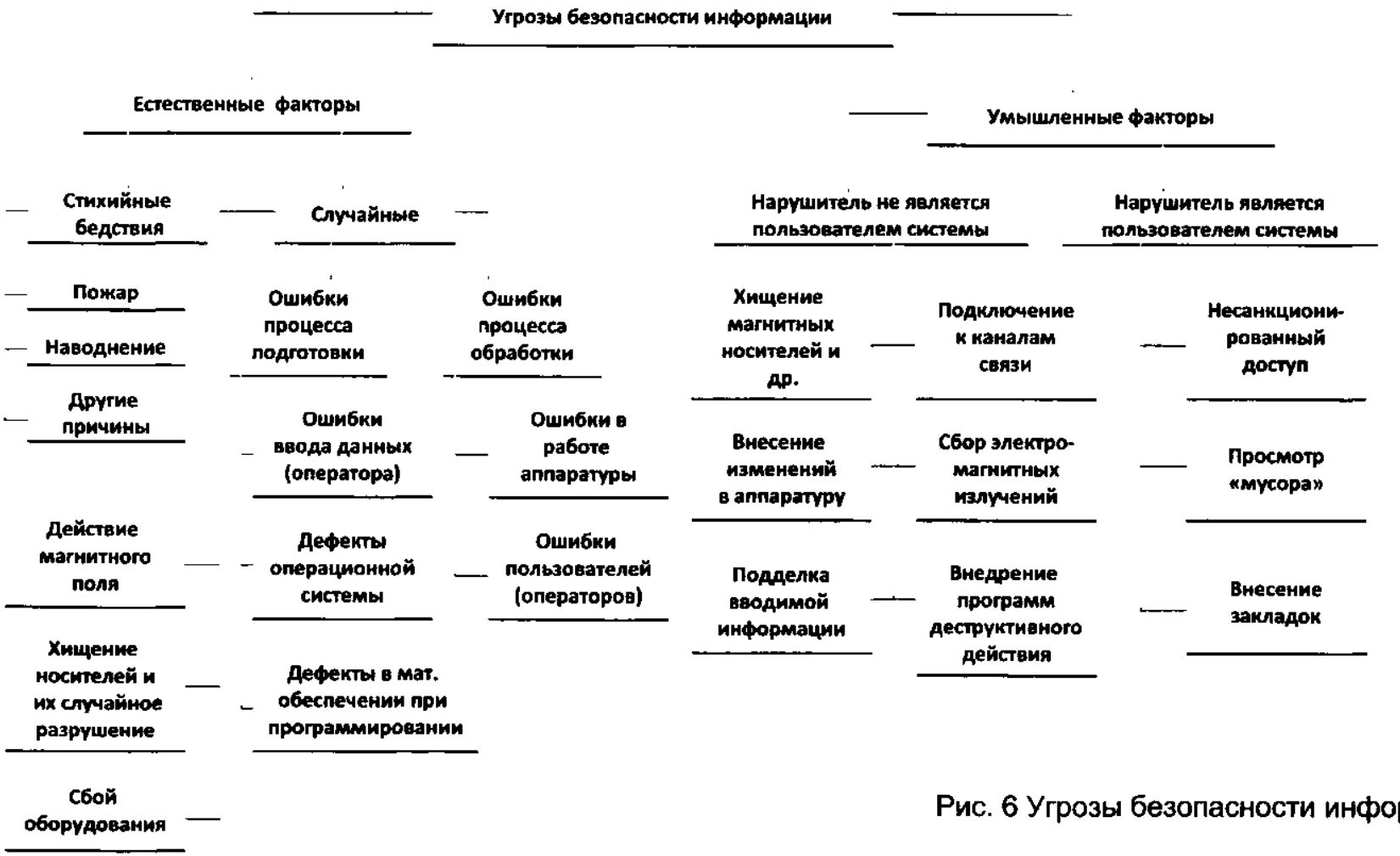


Рис. 6 Угрозы безопасности информации

8. Определение комплекса мероприятий по результатам проведения классификации ИСПДн

Защита персональных данных - это комплекс мер технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

ВНИМАНИЕ!

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе в случае необходимости 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.

(п. 1 ст. 19 Федерального закона «О персональных данных»)

Требования к обеспечению безопасности ПДн при их обработке в информационных системах ПДн, требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне информационных систем ПДн устанавливаются Правительством РФ.

Постановлением Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» определены необходимые мероприятия по защите ПДн. В их число входят: определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз; разработка на основе моде

ли угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз, с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн, и другие мероприятия.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Что важно учесть с юридической точки зрения. Ни закон, ни Положение об обеспечении безопасности ПДн при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 г. №781, не содержат конкретного перечня мероприятий, которые необходимо провести в случае присвоения информационной системе того или иного класса. В данном случае необходимо исходить из требований, определенных Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденного Приказом ФСТЭК России от 05.02.2010 г. № 58 (далее - Приказ ФСТЭК России № 58).

В пункте 1.4 Положения, утвержденного Приказом ФСТЭК России № 58, предусмотрено, что ***«выбор и реализация методов и способов защиты информации в информационной***

системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы».

В соответствии с п. 1.2 Приказа № 58 к методам и способам защиты информации в информационных системах отно- ятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий;
- методы и способы речевой защиты информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий.

Необходимо отметить, что с 15 марта 2010 года отменено применение двух методических документов ФСТЭК России:

- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утвержденные заместителем директором ФСТЭК России от 15 февраля 2008 года (далее - Основные мероприятия);
- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные заместителем директора ФСТЭК России от 15 февраля 2008 года.

Данные изменения связаны с утверждением заместителем директора ФСТЭК решения от 5 марта 2010 года, принятого в связи с принятием Приказа ФСТЭК России № 58.

Несмотря на то, что в целом нормы приказа № 58 дублируют положения Основных мероприятий, существенные различия в этих двух документах все же имеются. Основным отличием, по мнению авторов, является снижение ряда требований и предоставление большей «степени свободы» операторам персональных данных.

Например, в отличие от Основных мероприятий в приказе №58 не определен порядок проведения оценки соответствия ИСПДн требованиям безопасности. Соответственно, проведение обязательной аттестации (сертификации) ИСПДн 1 и 2 класса в настоящее время не предусмотрено. Данное изменение можно рассматривать как положительное, так как отмена аттестации (сертификации) позволит сэкономить операторам персональных данных значительные финансовые ресурсы.

Для информации

Согласно ст. 20 Федерального закона от 27.12.2004 г. № 184-ФЗ «О техническом регулировании» (далее - Федеральный закон «О техническом регулировании») подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Обязательное подтверждение соответствия осуществляется в формах:

- **принятия декларации о соответствии (далее - декларирование соответствия);**
- **обязательной сертификации (аттестации).**

В соответствии с п. 24 ст. Федерального закона «О техническом регулировании» декларирование соответствия осуществляется по одной из следующих схем:

- **принятие декларации о соответствии на основании собственных доказательств;**
- **принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра).**

Пунктом 2 рассматриваемого закона предусмотрено, что *«при декларировании соответствия на основании собственных доказательств заявитель самостоятельно формирует доказательственные материалы в целях подтверждения соответствия продукции требованиям технических регламентов. В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов».*

Требования к порядку оформления декларации соответствия предусмотрены п. 5 Федерального закона «О техническом регулировании». В частности предусмотрено, что декларация оформляется на русском языке и должна содержать:

- **наименование и местонахождение заявителя;**
- **наименование и местонахождение изготовителя;**
- **информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект;**
- **наименование технического регламента, на соответствие требованиям которого подтверждается продукция;**
- **указание на схему декларирования соответствия;**
- **заявление заявителя о безопасности продукции при ее использовании в соответствии с целевым назначением и принятии заявителем мер по обеспечению соответствия продукции требованиям технических регламентов;**
- **сведения о проведенных исследованиях (испытаниях) и измерениях, сертификате системы качества, а также документах, послуживших основанием для подтверждения соответствия продукции требованиям технических регламентов;**
- **срок действия декларации о соответствии;**
- **иные предусмотренные соответствующими техническими регламентами сведения.**

Приказом Министерства промышленности и энергетики Российской Федерации от 22.03.2006 № 54 «Об утверждении формы декларации о соответствии продукции требованиям техническим регламентам» утверждена форма декларации соответствия. Конкретная форма декларации соответствия информационных систем требованиям законодательства о защите персональных данных в настоящее время не установлена.

Общий порядок аттестации регламентирован «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.) В ходе аттестации проводится обследование объекта информатизации по требованиям законодательства и выдается подтверждающий документ (Аттестат соответствия ФСТЭК России).

Процедура сертификации программного обеспечения, являющегося средством защиты информации, ФСТЭК России установлена «Положением о сертификации средств защиты информации по требованиям безопасности информации» (утверждено приказом Гостехкомиссии России от 27 октября 1995 г. № 199). В результате проведения сертификации средств защиты информации на сертифицируемое средство выдается сертификат соответствия по требованиям безопасности информации ФСТЭК России.

На сроке действия декларации соответствия стоит остановиться особо. Федеральным законом о «Техническом регулировании» предусмотрено, что срок действия декларации о соответствии определяется техническим регламентом. Ни требованиями Федерального закона «О персональных данных», ни подзаконными актами не установлены конкретные сроки действия декларации соответствия.

Необходимо учитывать, что в первую очередь срок действия декларации соответствия ограничен временем, в течение которого остаются неизменными определяющие характеристики ИСПДн (условия размещения, состав технических средств, бизнес-процессы, состав обрабатываемых данных и т. п.). Соответственно, внесение каких-либо изменений влечет повторное проведение декларирования соответствия.

Во-вторых, пересмотр декларация соответствия необходимо при внесении изменений в подзаконные акты, а также нормативные правовые документы регуляторов. Можно предположить, что такие изменения на стадии становления законодательства о защите персональных данных будут вноситься нередко.

Кроме того, при определении срока действия декларации соответствия стоит учитывать, что для оператора ПДн организация защиты персональных данных может быть делом новым, рекомендуется для начала установить срок действия декларации соответствия небольшим - скажем полгода или 9 месяцев, чтобы по истечения этого срока по результатам функционирования ИСПДн уточнить комплект организационно-распорядительных документации и набор аргументов, подтверждающих соответствие системы защиты требованиям безопасности.

Таким образом, начиная с 15 марта 2010 года, операторы ПДн вправе самостоятельно выбрать тот способ подтверждения соответствия, который им необходим.

Методы и способы защиты информации от НСД[12]

В соответствии с п. 2.1 Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного Приказом ФСТЭК России № 58, методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

12 Методы и способы речевой защиты информации в рамках данного пособия не рассматриваются.

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Как отмечалось выше, требования, предъявляемые к операторам, зависят от класса ИСПДн, вида информационной системы (распределенная или нераспределенная), условий пользования, разграничений доступа.

Для простоты понимания приведем требования, предъявляемые к операторам ПДн, в соответствии с Методами и способами защиты информации от несанкционированного доступа в зависимости от класса информационной системы, приведенны

ми в Приложении к Положению, утвержденному Приказом ФСТЭК России № 58, в таблице № 8[13].

Как видно из данной таблицы, информационная безопасность в ряде случаев опирается на средства и возможности программного обеспечения, а в ряде случаев на организационнораспорядительные мероприятия (например, порядок хранения защищаемых носителей информации, пропускной режим и т. п.)

Дополнительно в качестве еще одного положительного изменения, внесенного отменой двух документов ФСТЭК России, можно рассматривать отмену требования о необходимости наличия лицензии на осуществление деятельности по технической защите конфиденциальной информации у операторов ИСПДн при осуществлении обработки ПДн в ИСПДн 1, 2 и 3 (распределенные системы) классов.

13
Методы и способы обеспечения безопасного межсетевого взаимодействия, а также вопросы антивирусной защиты в рамках данного пособия не рассматриваются.

Таблица № 8

№ п/п	Требования		Режим пользования		
			Одно-пользователь.	Многопользовательский	
				Права доступа	
				равные	разные
ИСПДн 2 и 3 классов					
1	*В подсистеме управления доступом*				
1.1	Должна осуществляться идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов		*	*	*
2	*В подсистеме регистрации и учета*				
2.1	Должна осуществляться регистрация входа (выхода) субъекта доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются	дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы	*	*	*
		результат попытки входа (успешная или неуспешная)		*	*
		идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа			*
2.2	Должен проводиться умет всех защищаемых носителей информации	с помощью их маркировки и с занесением учетных данных в журнал учета	*	*	
		с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)			*

№ п *In*	Требования		Режим пользования		
			Одно-пользователь.	Многопользовательский	
				Права доступа	
				равные	разные
3	*В подсистеме обеспечения целостности*				
3.1	Должна быть обеспечена целостность программных средств защиты ПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы	по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;	*		
		по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации		*	
		по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации			*

№ п /п	Требования		Режим .0 , 5 I ^ (5 *g* o g Осп	пользования Многополь-зовательский рав ные	Права доступа раз ные
3.2	Должна осуществляться физическая охрана физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации		*	*	*
3.3	Должно проводиться периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа		*	*	*
3.4	Должны быть в наличии средства восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности		*	*	*
Для ИСПДн 1 класса (п. 4.1 - 4.3)					
4	*В подсистеме управления доступом*				
4.1	Должна осуществляться идентификация и проверка подлинности пользователя при входе в систему	по паролю условно-постоянного действия длиной не менее шести буквенноцифровых символов	*		
		по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов		*	*

№ п *In*	Требования		Режим пользования		
			Одно-пользователь.	Многопользовательский	
				Права доступа	
				рав	раз
5.6	Должен обеспечиваться учет всех защищаемых носителей информации	с помощью их маркировки и занесение учетных данных в журнал учета	*		
		с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)		*	*
5.7	Должен быть обеспечен дублирующий учет защищаемых носителей информации		*	*	
5.8	Необходимо обеспечивать очистку (обнуление, обезличивание)освобождаемых областей оперативной памяти информационной системы	и внешних носителей информации	*	*	
		и внешних накопителей			*
6	*В подсистеме обеспечения целостности*				
6.1	необходимо обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов средств защиты информации, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ		*	*	
6.2	Требуется обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения ПДн				*

№ п/п	Требования	Одно-пользователь. $.*	пользования Многопользовательский	Права доступа
			равные	разные
6.3	Должна осуществляться физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания	*	*	
6.4	Должна осуществляться физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая кон-^ троль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации			*
6.5	Необходимо обеспечить периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	*	*	*
6.6	Необходимо обеспечить наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	*	*	*

9. Организационно-распорядительные мероприятия

Безопасность объекта оценки в значительной степени может быть достигнута административными мерами, такими как организационные меры, управление персоналом, физическая защита и процедурный контроль.

Ведь не секрет, что зачастую утечка информации происходит либо из-за целенаправленной работы инсайдеров, либо так называемого «человеческого фактора» - потери портфеля с документами или компьютера, неконтролируемого или плохо контролируемого пропускного режима в организацию, возможности подключения различного оборудования, с помощью которых можно скачать и передать информацию и т. п.

Именно поэтому к проведению организационных мер необходимо отнестись с должной степенью внимания. Оператор при организации обработки персональных данных обязан организовывать и проводить мероприятия:

Правового характера:

- Получение согласия у субъекта ПДн на обработку ПДн;
- Направление уведомления в Роскомнадзор с целью включения в реестр операторов;
- Разработка организационно-распорядительной документации, регламентирующей отношения в информационной сфере.

Организационного характера:

- Проведение категорирования ПДн и классификации информационных систем ПДн;
- Разработка порядка работы с ПДн;

- Доведение до сотрудников порядка работы со сведениями о персональных данных (обучение сотрудников);
- Осуществление мер контроля.

Для некоторых операторов персональных данных проводимые мероприятия будет ближе и понятнее называть мероприятиями организационно-технического характера, к которым можно отнести:

- создание и совершенствование системы обеспечения информационной безопасности;
- разработку, использование и совершенствование СЗИ и методов контроля их эффективности;
- предотвращение перехвата информации по техническим каналам связи;
- разработку порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ;
- контроль за выполнением требований по защите информации;
- сертификацию средств защиты информации;
- лицензирование деятельности организации в области защиты информации;
- аттестацию объектов информатизации на соответствие требованиям безопасности информации.

Режимного характера:

- Организация системы охраны территории, здания, помещений;
- Организация порядка допуска на территорию и в помещения;
- Обеспечение сохранности сменных носителей

Меры организационного характера осуществляются на предприятии независимо от того, нужно ли подавать уведомление в Роскомнадзор или нет, осуществляется ли обработка ПДн с использованием средств автоматизации или без использования таких средств. В каждой организации перечень мероприятий и документов может варьироваться в зависимости от специфики обработки ПДн, организационной структуры и других особенностей конкретного предприятия. Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных - чем выше категория, тем выше требования их защиты.

Особое внимание должно быть уделено разработке организационно-распорядительной документации, которая регламентирует весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Что необходимо зафиксировать в данных документах:

- перечень обрабатываемых данных;
- перечень сотрудников, имеющих право доступа к сведениям персонального характера, вид доступа и т. п.;
- перечень сотрудников, имеющих право получения и обработки ПДн;
- используемое оборудование, СЗИ, антивирусные программы, межсетевые экраны и т. п.;
- порядок учета защищаемых носителей информации;
- контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, в том числе в ночное время;
- определить сроки проведения внутренних проверок защиты ПДн;
- иные требования.

Набор документов в различных организациях может быть разный, среди основных можно выделить:

- Приказ о создании комиссии по защите персональных данных с наделением ее полномочиями по проведению всех мероприятий, касающихся организации защиты персональных данных;
- Положение о персональных данных и их защите;
- Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные;
- Приказ (приказы) о возложении персональной ответственности за защиту персональных данных;
- Договор с субъектом персональных данных, который может содержать отдельное письменное согласие субъекта персональных данных на их обработку, в случаях определенных Федеральным законом № 152-ФЗ;
- Нормативный документ (перечень), аккумулирующий информацию о персональных данных, обрабатываемых оператором (в том числе их категория, объем и сроки хранения)
- Перечень информационных систем, обрабатывающих ПДн;
- Регламент допуска сотрудников к обработке персональных данных;
- Регламент взаимодействия при передаче ПДн третьим лицам;
- Перечень допущенных сотрудников к обработке ПДн;
- Перечень сотрудников, имеющих право ознакомления со сведениями, отнесенными к ПДн;
- Должностные инструкции сотрудников, имеющих отношение к обработке ПДн, в том числе инструкции администраторов безопасности ПДн, инструкции пользователей по работе с ПДн;

- Положение об организации доступа в помещения, где осуществляется обработка ПДн и т. п.

Кроме того, в ряде случаев потребуется вносить изменения в должностные инструкции.

Проведение комплекса технических мероприятий и разработка организационно-распорядительной документации могут оказаться бесполезными, если не будет проведена соответствующая работа с сотрудниками, а также не будут созданы условия, при которых сотрудники будут осознанно соблюдать установленные правила обеспечения защиты персональных данных. Кроме того, важной «составляющей успеха» будет организация эффективного взаимодействия пользователей и сотрудников подразделений информационной безопасности (IT-отделов).

Стоит помнить, что защита ПДн - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн и дальнейший контроль за их выполнением.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т. п.).

10. Техническая защита ПДн

Технические меры защиты информации предполагают использование программно-аппаратных средств защиты информации.

В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн в зависимости от класса информационной системы должны быть реализованы следующие мероприятия:

- установлены средства защиты информации от несанкционированного доступа (НСД) (системы разграничения доступа к информации; антивирусная защита; межсетевые экраны; средства блокировки устройств ввода-вывода информации, криптографические средства и т. п.);
- установлены средства защиты информации от утечки по техническим каналам (использование экранированных кабелей; установка высокочастотных фильтров на линии связи; установка активных систем зашумления и т. д.)

В соответствии с пунктом 2.1 Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58, методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение; резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Мероприятия по защите ПДн реализуются в рамках подсистем: управление доступом, регистрации и учета, обеспечения целостности, криптографической защиты, обнаружения вторжений.

Кроме того, в ИСПДн должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения. Данное требование является обязательным для средств защиты информации, интегрированных в ИСПДн класса К1, причем про

граммное и программно-аппаратное обеспечение должно соответствовать 4 уровню контроля отсутствия недекларированных возможностей.

Проводить мероприятия по технической защите ПДн необходимо либо своими силами либо исключительно силами организаций, имеющих лицензию ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации. Перечень таких организаций размещен на сайте ФСТЭК РФ - http://www.fstec.ru/_razd/_lico.htm.

Особо необходимо оговорить использование криптографических (шифровальных) средств защиты информации и предоставления услуг по шифрованию ПД при их обработке в информационной системе. Данный порядок определяет ФСБ России. Целесообразность их применения выясняется на этапе построения частной модели угроз. Если они признаются необходимыми, то применяемые средства криптографической защиты информации (СКЗИ) должны соответствовать требованиям российского законодательства.

Применение СКЗИ представляется очевидным в следующих ситуациях:

- наличие территориально распределенных систем, где в качестве транспорта для передачи персональных данных служат глобальные информационные сети (Internet) и сети связи общего пользования, в которых невозможно обеспечить контроль оператора персональных данных за доступом к передаваемой информации (на транзитных узлах Интернет, телефонных станциях при использовании коммутируемого доступа и т. п.);
- вынос за пределы контролируемой территории мобильных устройств обработки персональных данных, в том числе используемых для удаленного доступа к ИСПДн (ноутбуки, КПК и т. п.);

- применение многопользовательских систем персональных данных первого класса, где разграничение доступа обеспечивается исключительно шифрованием информации на дисках и средствами управления криптографическими ключами.

С перечнем средств защиты информации, не содержащей сведений, составляющих государственную тайну (Перечень средств ФСБ России), можно ознакомиться по ссылке http://www.fsb.ru/fsb/supplement/contact/lsz/perechen.htm.

Следует обратить внимание, что Федеральным законом от 27.12.2009 № 3б3-ФЗ внесены изменения в статью 19 Федерального закона «О персональных данных» в части использования шифровальных (криптографических) средств. В частности, предусматривается не обязательность, а возможность применения СКЗИ.

Также необходимо учитывать, что принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защищенности. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Кроме того, механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе пользователей.

Разработка комплекта организационно-распорядительных документов

1. Приказ о создании комиссии по проведению категорирования персональных данных и проведению инвентаризации/обследования информационных систем

В целях реализации мероприятий по защите персональных данных в первую очередь необходимо организовать руководство вопросами организации защиты персональных данных как на период приведения предпроектных и проектных работ, так и в дальнейшем в ходе повседневной эксплуатации информационной системы ПДн.

Таким образом, первым документом, подлежащим принятию в организации, должен быть приказ о проведении анализа обрабатываемых ПДн и обследования информационных систем.

В данном документе необходимо определить круг лиц, ответственных за проведение «предварительного этапа» организации защиты ПДн, конкретные задачи, а также сроки их исполнения. При этом члены комиссии должны быть наделены полномочиями по проведению мероприятий по организации защиты ПДн.

Основными целями данной работы будут являться:

- определение категорий ПДн, целей их обработки, режима обработки, наличия согласия, а также оценка целесообразности получения ПДн;
- выявление бизнес-процессов, при осуществлении которых обрабатываются персональные данные;
- проведение обследования существующих ИСПДн.

- определение подразделений и сотрудников, обрабатывающих ПДн;
- подготовка плана мероприятий по организации и защите ПДн.

Могут быть предложены следующие формы документов.

Общество с ограниченной ответственностью
« _____ »

ПРИКАЗ №_____

I _____ от _____

С) создании комиссии по организации и проведению работ по защите персональных данных

В целях проведения мероприятий по организации защиты персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ

1. Назначить комиссию в составе:
- председатель комиссии - должность Ф.И.О.;
- члены комиссии - должность Ф.И.О., должность Ф.И.О.

2. Комиссии:

1) Провести обследование существующих информационных систем (наименование информационных систем). В ходе работы следует определить:
- перечень ПДн, обрабатываемых в ИСПДн, их объем, а также выделить совокупность ПДн, подлежащих защите;
- условия размещения технических средств ИСПДн и доступа к ним;
- определить конфигурацию и топологию ИСПДн, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами;
- определить технические средства и системы, составляющие ИСПДн, используемые общесистемные и прикладные программные средства;
- определить режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах.

Результаты работы представить в виде акта (перечня) категорирования обрабатываемых данных и акта обследования информационных систем (либо перечня информационных систем).

Срок:
Ответственный:

2) Провести классификацию ИСПДн, в том числе:
- определить категорию обрабатываемых ПДн;
- определить (уточнить) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн, разработать модель угроз;
- определить класс ИСПДн;
- уточнить степень участия должностных лиц в обработке ПДн, характер их взаимодействия между собой.

Результаты работы представить в виде акта классификации Срок:
Ответственный:

3) Разработать и представить на утверждение план мероприятий по организации защиты персональных данных. Представить предложения по исполнителям, сумме затрат и сроках исполнения.

Срок:
Ответственный:

Руководитель _____ / _____
Подпись ФИО

Для небольших организаций может быть предложен следующий упрощенный вариант приказа.

Общество с ограниченной ответственностью
« _____ »

ПРИКАЗ № _____

г. _____ от _____

О назначении комиссии по категорированию и классификации объектов информатизации

Для определения категории объекта информатизации _____ в помещении № _____ и класса защищенности АС от несанкционированного доступа к информации

ПРИКАЗЫВАЮ

1. Назначить комиссию в составе:
- председатель комиссии - должность Ф.И.О.;
- члены комиссии - должность Ф.И.О., должность Ф.И.О.

2. Назначенной комиссии провести категорирование персональных данных/объекта информатизации и классификацию информационной системы персональных данных.

Результаты работы представить в виде актов категорирования и классификации. Срок исполнения _____

Руководитель _____ / _____
Подпись ФИО

2. Опросный лист для сбора исходных данных об ИСПДн

Для простоты проведения обследования информационной системы предлагаем следующую форму листа, которую нужно будет 'заполнить для каждой ИСПДн, созданной в организации.

N8	Вопрос	Ответ
1	Описание ИСПДн	
1.1	Название ИСПДн	
1.2	Характеристики ИСПДн, включая: перечень используемых программных и аппаратных средств; архитектуру ИСПДн; описание принципов функционирования; описание информационных потоков в ИСПДн; ПО рабочих станций и серверов,сетевого оборудования; тип СУБД; прочее.	
1.3	Цель обработки ПДн	
1.4	Операции, которые предполагается осуществлять с ПДн в системе и способы их обработки	
1.5	Количество субъектов персональных данных, информация о которых будет обрабатываться в системе	
1.6	Какая информация о субъектах ПДн обрабатывается в системе?	
1.7	Какие категории лиц выступают в качестве субъектов ПДн?	

№	Вопрос	Ответ
1.8	Время начала, срок хранения и обработки информации о субъектах ПДн в системе, условия прекращения обработки информации о субъектах ПДн	
1.9	Структура ИСПДн	□ - Автономные (не подключенные к иным ИС) технические и программные средства □ - АРМ, объединенные в ИС средствами связи без использования удаленного доступа □ - АРМ, объединенные в ИС средствами связи с использованием удаленного доступа
1.10	Осуществляется ли передача ПДн за границу РФ?	□ -Да □ - Нет
1.11	Имеет ли сеть, в которой функционирует ИСПДн, сопряжение с внешними, в т. ч. публичными, сетями?	
1.12	Характеристика ИСПДн с точки зрения распределения ролей и полномочий пользователей	□ - Однопользовательская □ - Многопользовательская с равными правами □ - Многопользовательская с разными правами
1.13	Какие аспекты обеспечения ИБ в отношении ПДн требуется обеспечить	□ - Конфиденциальность □ - Целостность □ - Доступность
1.14	Технические средства, входящие в состав ИСПДн, находятся в границах РФ или за ее пределами (указать где)?	□ - В границах РФ □ - За пределами границы РФ
1.15	Имеет ли компания лицензию на техническую защиту конфиденциальной информации?	□ -Да □ - Нет
1.16	Какая организационно-распорядительная и нормативная документация по ИБ (в т. ч. по защите ПДн) уже разработана в Компании?	

№	Вопрос	Ответ
2	Материальный состав и расположение компонент ИСПДн	
2.1	Количество и наименование объектов, на которых предполагается хранить или обрабатывать ПДн	
2.2	В состав организации фактически входит одно или несколько юридических лиц, в рамках которых осуществляется обработка ПДн?	
2.3	Состав и суммарное количество рабочих станций ИСПДн	
2.4	Суммарное количество пользователей ИСПДн	
2.5	Состав и суммарное количество серверов ИСПДн	
2.6	Состав и суммарное количество единиц сетевого оборудования	
2.7	Состав и суммарное количество технических СЗИ	
3	Прочее	
3.1	Перечень лиц, принимавших участие в заполнении пунктов опросного листа	

3. Акт категорирования персональных данных (перечень персональных данных)

Необходимо внимательно проанализировать, какие данные обрабатываются в организации, целесообразность их получения и обработки. Причем следует учитывать как данные, обрабатываемые автоматизированным способом (например, в отношении сотрудников), так и данные которые обрабатываются без использования средств автоматизации (например, в отношении посетителей). Тщательная подготовка перечня персональ

ных данных позволит операторам осознать слабые места во взаимодействии с субъектами ПД.

Для примера перечень персональных данных, которые могут быть учтены в типовой конфигурации ПП «1С:Зарплата и управление персоналом 8»:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- место рождения;
- паспортные данные физического лица;
- дата регистрации по месту жительства,
- гражданство;
- инвалидность;
- страховой номер свидетельства в ПФР;
- ИНН;
- предшествующие места работы;
- общий стаж;
- страховой стаж;
- непрерывный стаж;
- северный стаж;
- вычеты по НДФЛ:
  - на ребенка,
  - на ребенка-инвалида,
  - на ребенка единственному родителю,
- воинский учет;
- состояние в браке;
- семья:
  - мать, отец, жена,
  - дети;
- языки;
- учеба:
  - вид образования (высшее, среднее),
  - учебное заведение,

специальность, диплом,

серия, номер, год окончания,

квалификация по диплому;

- профессия;
- награды;
- информация о добровольном и обязательном страховании;
- даты приема на работу и кадровых перемещений;
- суммы зарплаты;
- сведения о прохождении аттестации (оценки), данные о компетенциях работника;
- сведения об отпусках;
- сведения о социальных льготах;
- исполнительные листы, отчет по исполнительным листам всего предприятия:

месяц,

сумма

удержания,

почтовый сбор,

контрагент:

- его банковский номер,
- адрес,
- телефон.

Данные сведения могут быть отнесены к категории сведений, позволяющих идентифицировать субъекта и получить о нем дополнительную информацию. По каждой позиции или группе позиций необходимо определить цели обработки и период хранения. Аналогичным образом проводится анализ по каждой категории физических лиц (учредители, бывшие сотрудники, контрагенты, контактные лица контрагентов, кандидаты на работу и т. п.)

Соответственно итогом проведенной работы будет являться Перечень персональных данных, обрабатываемых в организации/у индивидуального предпринимателя.

Утверждено

Руководитель ООО « _____ »

« _____ » _____ 20.... г.

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в

ООО « _____»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149- ФЗ «Об информации, информационных технологиях и о защите информации», другими нормативными правовыми документами по вопросам использования и защиты информационных ресурсов и приказом руководителя ООО «_____ » от _____ № _____ комиссией по организации и проведению работ по защите персональных данных определен перечень персональных данных, обрабатываемых в ООО « _____ ».

В ходе проведенного обследования установлено, что в ООО « _____ » обрабатываются следующие персональные данные:

№ п/п	Вид ПДн	Категория ПДн в соответствии с Приказом № 55/86/20	Вид обработки	Срок хранения	Цель обработки	Наименование ИСПДн, в которой обра-батываются пер-сональные данные
1.	Данные о работниках, в том числе фамилия, имя, отчество, дата и место рождения, пол,паспортные данные, гражданство, ИНН, страховой номер в ПФР					

№ п/п	Вид ПДн	Категория ПДн в соответствии с Приказом № 55/86/20	Вид обработки	Срок хранения	Цель обработки	Наименование ИСПДн, в которой обрабатываются персональные данные
2.	Лица, связанные с сотрудниками[14]					
3.	Акционеры/учредители					
4.	Контрагенты					
5.	Потенциальные клиенты					
6.	Иные лица					

1.4. Перечень может пересматриваться по мере необходимости в соответствии с установленным порядком.

Председатель комиссии _____ / _____

Подпись **ФИО**

[14] Дети, в отношении которых выплачиваются алименты, бывшие жены и т. п.

4. Перечень информационных систем

Следующим документом, который целесообразно подготовить, является перечень созданных в организации информационных систем персональных данных и входящих в них подсистем.

Дополнительно к перечню информационных систем необходимо нарисовать схему размещения (мест размещения) технических средств и устройств, используемых в автоматизированной информационной системе. Может быть предложена следующая форма документа.

Утверждено
Руководитель

« » 20091т

ПЕРЕЧЕНЬ

Информационных систем персональных данных, созданных в

№ п\п	Наименование ИСПДн	Место расположения	Максимальная категория обрабатываемых данных	Объем сведений персонального характера, содержащихся в ИСПДн

Настоящий перечень может пересматриваться по мере необходимости в соответствии *с* установленным порядком.

Председатель комиссии _____ / _____
Подпись **ФИО**

5. Акт классификации информационной системы, обрабатывающей ПДн

В акте классификации необходимо указать все информационные системы, созданные в организации, в которых содержатся ПДн.

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

Акт классификации ИСПДН может иметь следующую форму.

Утверждаю Руководитель предприятия

"____ " _____ г.

АКТ

классификации информационной системы персональных данных

Комиссия, в соответствии с приказом от _____ № _____ в составе:
председатель:
члены комиссии:
провела классификацию информационной системы _____ и установила:

Выявленные определяющие признаки классификации типовой информационной системы:
- наивысшая категория обрабатываемых персональных данных _____ ;
- количество обрабатываемых субъектов персональных данных (диапазон);
- в информационной системы обрабатываются данные _____ (наименование одного или нескольких операторов ИСПДн);
- структура системы (автономная, локальная, распределенная);
- наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных (однопользовательский или многопользовательский);
- режим разграничения прав доступа пользователей информационной системы (без разграничения прав доступа или с разграничением прав);
- местонахождение технических средств информационной системы (в пределах Российской Федерации, частично или целиком за пределами Российской Федерации).

Комиссия, на основании определяющих признаков классификации и в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»,

РЕШИЛА:

присвоить информационной системе _____, обрабатывающей персональные данные, класс _____(К1, К2, К3, К4 или специальный)

Председатель комиссии

Члены комиссии

6. План мероприятий по защите персональных данных

Данный документ должен быть составлен с целью четкого определения тех работ, которые надлежит осуществить в организации с учетом полученных результатов проведенного обследования информационных систем.

Утверждаю
Руководитель ООО « _____ »

" ____"_____ " ___ "г.

ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО « _____»

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание

Председатель комиссии Члены комиссии

7. Положение о защите персональных данных

Положение о защите персональных данных - это внутренний, локальный нормативный акт, который регламентирует порядок получения, использования и хранения персональных данных сотрудников компании. Унифицированной формы данный документ не имеет, но он должен быть составлен в соответствии с требованиями Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 г., а также Трудового кодекса РФ. В Положении необходимо определить:

- цель и задачи организации в области защиты персональных данных;
- понятие и состав персональных данных;
- порядок их сбора, обработки, использования и передачи;
- на каких носителях (электронных, бумажных) и где они хранятся;
- права субъекта ПДн с целью обеспечения защиты своих данных;
- обязанности оператора ПДн
- ответственность работодателя за несанкционированный доступ и разглашение конфиденциальной информации о человеке:
- перечень лиц/подразделений, имеющих доступ к персональным данным (приложение к положению).

После согласования и утверждения руководством фирмы Положения необходимо ввести его в действие приказом руководителя организации, а затем с документом ознакомить всех сотрудников под роспись. Факт ознакомления может быть зафиксирован либо в листе согласования, либо подтвержден распиской сотрудника.

Далее в необходимых случаях следует составить «Инструкцию по обработке и защите ПД», описывающую порядок обработки ПД в соответствии с бизнес-процессами оператора.

Эти и ряд других подобных документов позволят формализовать обработку ПД и минимизировать связанные с этим риски.

Данным документом следует конкретно определить организационные и технические условия охраны персональных данных субъектов ПДн от их неправомерного использования и распространения, например:

1) запретить подсоединение автоматизированных систем обработки персональных данных к локальной сети организации и Интернет;

2) снабдить все компьютеры, на которых обрабатываются персональные данные, средствами защиты от несанкционированного доступа;

3) хранить дела, папки с документами, картотеки, учетные журналы и книги учета в металлических запирающихся шкафах;

4) «дробить данные» о персональных данных субъектов ПДн между работниками и не допускать разглашения полученных знаний каждым из работников;

5) проводить регулярные проверки функционирования системы защиты ПДн.

Утверждаю
Руководитель ООО « _____ »

" ___ " _____"____"г.

ПОЛОЖЕНИЕ по обработке и защите персональных данных

город год

I. Общие положения

1.1. Настоящее Положение по обработке и защите персональных данных (далее - Положение) Организации (ООО « _____ ») разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», иными нормативными правовыми актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения - определение порядка обработки персональных данных в Организации; обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Организации и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Все работники Организации должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных в отношении персональных данных работников организации снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Организации, если иное не определено законом.

1.6. Контроль за соблюдением настоящего Положения осуществляет

II. Основные понятия и состав персональных данных

Для целей настоящего Положения используются следующие основные понятия и определения:

- ***«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;**
- ***«оператор»*** **- государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;**
- ***«субъект»*** **- субъект персональных данных;**
- ***«обработка персональных данных»*** **- действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распро-**

странение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- ***«конфиденциальность персональных данных»*** **- обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;**
- ***«распространение персональных данных»*** **- действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;**
- ***«использование персональных данных»*** **- действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;**
- ***«блокирование персональных данных»*** **- временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;**
- ***«уничтожение персональных данных»*** **- действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;**
- ***«обезличивание персональных данных»*** **- действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;**
- ***«информационная система персональных данных»*** **- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;**
- ***«конфиденциальность персональных данных»*** **- обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;**
- ***«трансграничная передача персональных данных»*** **- передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;**
- ***«общедоступные персональные данные»*** **- персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.**

- ***«информация»*** **- сведения (сообщения, данные) независимо от формы их представления;**
- ***«доступ к информации»*** **- возможность получения информации и ее использования:**
- ***«документированная информация»*** **- зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.**

III. Цели и задачи обработки персональных данных

3.1. В соответствии с разделом 2 настоящего Положения оператором, организующим и осуществляющим обработку персональных данных, является ООО « ».

3.2. К персональным данным относятся:

3.2.1 Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта.

3.2.2. Сведения о месте жительства субъекта.

3.2.3. Информация, содержащаяся в трудовой книжке работника.

3.2.4. Сведения об образовании, квалификации или наличии специальной подготовки.

3.2.5. Сведения о заработной плате работников.

3.2.6. Иные сведения[15].

3.3. Обработка персональных данных осуществляется с целью содействия субъектам персональных данных в _____

—

3.4. Обработка персональных данных осуществляется:

- без использования средств автоматизации (в части)[17];

- с использованием автоматизированной информационной системы « _____ » (в части_____)[18];

[15] Необходимо указать конкретные виды, сведений персонального характера, хранение и обработка которых осуществляется в организации.

[16] В данном пункте необходимо наиболее четко и подробно отразить в каких целях осуществляется обработку ПДн. Например, с целью содействия субъектам ПДн в осуществлении трудовой деятельности, обеспечения личной безопасности, исполнения договорных обязательств и т. п.

[17] Необходимо указать какие сведения обрабатываются без использования средств автоматизации

[18] Необходимо указать какие сведения обрабатываются с использованием средств автоматизации в ИСПДн.

3.5. Обработка персональных данных в автоматизированной информационной системе « _____ » осуществляется для решения следующих задач:

1) _____ ;
2) _____ ;
3) _____ ;[19]

3.6. При принятии решений, затрагивающего интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

IV. Субъекты персональных данных

4.1. В соответствии с разделом 2 настоящего Положения к субъектам персональных данных относятся следующие категории физических лиц:

- **работники Организации;**
- **кандидаты для приема на работу;**
- **контрагенты;**
- **учредители;**[20]

4.2. Все персональные данные субъекта персональных данных оператору следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Организации должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих *получению персональных* данных и последствиях отказа дать письменное согласие на их получение.

4.3. Организация не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

4.4. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и дает согласие на их обработку. Обработка указанных персональных данных возможна только с их согласия, либо без их согласия в следующих случаях:

[19] Указать конкретные задачи для решения которых осуществляется обработка ПДн. Например, учет кадрового состава, бухгалтерский учет и контроль за финансовохозяйственной деятельностью организации и исполнением финансовых обязательств по заключенным договорам и т. п. Данный перечень будут напрямую связан с целями, указанными в согласии на предоставление ПДн.

[20] Указать иные категории субъектов ПДн, актуальные для организации.

- **обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;**
- **обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;**
- **обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;**
- **обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;**
- **обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;**
- **обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;**
- **осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.**

4.5. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

4.6. Согласие на обработку персональных данных оформляется в письменном виде[21].

Письменное согласие на обработку своих персональных данных должно включать в себя:

- **фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;**
- **наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;**
- **цель обработки персональных данных;**
- **перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;**

[21] Форма листа согласия может являться приложением к настоящему Положению.

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

4.7. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора.

4.8. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные следует получать от его законных представителей.

4.9. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

4.10. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя руководителя организации[2].

4.11. Субъект персональных данных имеет право на получение следующей информации:

- **сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;**
- **перечень обрабатываемых персональных данных и источник их получения;**
- **сроки обработки персональных данных, в том числе сроки их хранения;**
- **сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.**

4.12. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

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

4.14. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении

12

Может быть указано иное лицо, имеющее соответствующие полномочия от руководителя организации.

письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя руководителя организации или уполномоченного руководителем лицо.
4.15. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

V. Состав персональных данных, обрабатываемых с использованием автоматизированной системы

5.1. Состав персональных данных, обрабатываемых с использованием автоматизированной системы Организации, определяется настоящим Положением и соответствует целям и задачам сбора, обработки и использования персональных данных в соответствии с разделом 3 настоящего Положения.
5.2. Перечень персональных данных автоматизированной информационной системы Организации зависит от категории субъекта персональных данных и утверждается руководителем Организации.

VI. Порядок сбора, хранения и использования персональных данных

6.1. Субъекты персональных данных при получении от них согласия на обработку персональных данных в автоматизированной информационной системе должны быть ознакомлены с перечнем собираемых и используемых сведений, с целями и задачами сбора, хранения и использования персональных данных.
6.2. Персональные данные субъектов персональных данных могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
6.3. Порядок хранения анкет и иных документов, содержащих информацию персонального характера, а также согласий на обработку персональных данных определяются «Положением о порядке хранения информации персонального характера на бумажных носителях».
6.4. Ввод персональных данных в автоматизированную систему Организации осуществляется работником, имеющим доступ к работе с персональными данными, и в соответствии с его должностными обязанностями. На бумажном носителе информации, содержащей персональные данные (анкеты, личные листки и др.) работник, осуществляющий ввод данных, оставляет отметку о дате ввода информации и о лице, осуществившем ее ввод.
6.5. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированной информационной системы, несут ответственность за достоверность и полноту введенной информации.
6.6. При работе с программными средствами автоматизированной информационной системы Организации, реализующими функции просмотра и редактирования персональных данных, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующих должностных обязанностей.
6.7. Хранение персональных данных в автоматизированной информационной системе Организации осуществляется на серверах Организации с использованием специализированного программного обеспечения, отвечающего требованиям безопасности.

6.8. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечению установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении.
6.9. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.
6.10. Хранение резервных и технологических копий баз данных автоматизированной информационной системы, содержащих информацию персонального характера, осуществляется на серверах организации и сменных носителях, доступ к которым ограничен.
6.11. Вынос резервных и технологических копий баз данных автоматизированной информационной системы, содержащих информацию персонального характера, из организации запрещен. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки автоматизированной информационной системы.
6.12. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя или уполномоченного им лица.

VII. Особенности предоставления доступа к персональным данным

7.1. Доступ сотрудников к персональным данным, содержащимся как в автоматизированной информационной системы организации, так и на бумажных носителях осуществляется с письменного согласия руководителя организации или уполномоченного им лица (допуск).
7.2. Сотрудник, получивший допуск к персональным данным, должен быть ознакомлен с настоящим Положением.
7.3. При получении доступа к персональным данным сотрудники подписывают Обязательство о неразглашении персональных данных.
7.4. Доступ к автоматизированной информационной системе Организации разграничен политикой безопасности системы, реализуемой с использованием технических и организационных мероприятий.
7.5. Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в автоматизированной информационной системе. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.
Запрещается использование для доступа к автоматизированной информационной системе Организации учетных записей других пользователей.
7.6. Созданием, удалением и изменением учетных записей пользователей автоматизированной информационной системы занимаются уполномоченные администраторы в соответствии с должностными обязанностями.
7.7. При получении доступа к персональным данным сотрудники подписывают Обязательство о неразглашении персональных данных.
7.8. Право доступа к персональным данным субъектов персональных данных в части их касающейся имеют:

- генеральный директор Организации;
- заместитель генерального директора по безопасности;

- **сотрудники бухгалтерии;**
- **сотрудники службы персонала;**
- **сотрудники отдела по экономической безопасности;**
- **сотрудники канцелярии (информация о фактическом месте проживания и контактные телефоны работников);**
- **руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения)**
- [23].

VIII. Порядок передачи информации, содержащей персональные данные

8.1. В соответствии с законодательством Российской Федерации персональные данные Организации могут быть переданы правоохранительным, судебным органам и другим учреждениям в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, а также в случаях, установленных федеральным законом.
8.2. Запрещается сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия. Обработка персональных данных субъектов персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.
8.3. Передача информации третьей стороне возможна только при письменном согласии работников.

IX. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

9.1. Нарушение требований настоящего Положения может повлечь гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.
9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

[23] Необходимо указать должности или подразделения, сотрудники которых имеют доступ к субъектам ПДн, а также конкретизировать к какой категории данных предоставлен доступ.

Общество с ограниченной ответственностью
«_____ »

ПРИКАЗ № _____

г. _____ от _____

Об утверждении Положения
«Об обработке и защите персональных данных»

В целях обеспечения защиты прав и свобод человека и в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Положение «Об обработке и защите персональных данных»;.

2. Положение «Об обработке и защите персональных данных» ввести в действие с « » _____ 20 _____ года.

3. _____ ознакомить всех работников с настоящим приказом под роспись.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель _____ / _____
Подпись ФИО

ЛИСТ ОЗНАКОМЛЕНИЙ

с Положением об обработке и защите персональных данных ООО « _____ », утвержденным приказом от _____№ _____

ознакомлены:

№ п/п	Фамилия	Подразделение	Должность	Дата	Подпись

8. Приказы о допуске

Завершающим этапом разработки организационно-распорядительной документации является издание приказов, определяющих:

- перечень сведений, содержащих персональные данные и обрабатываемые автоматизированным способом;
- перечень сведений, содержащих персональные данные и обрабатываемые без использования средств автоматизации;
- перечень сотрудников, имеющих доступ к сведениям, содержащие персональные данные, в том числе «с правом записи» (т. е. правом внесения изменений, дополнений и уточнений сведений, содержащихся в ИСПДн) и без «права записи»;
- подразделение/лица, ответственные за защиту персональных данных.

Общество с ограниченной ответственностью
«_____ »

ПРИКАЗ № _____

г. _____ от_____

Об утверждении перечней персональных данных и перечней групп должностей, допущенных к обработке персональных данных

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом РФ и другими нормативными правовыми документами по вопросам использования и защиты информационных ресурсов, содержащих персональные данные,

ПРИКАЗЫВАЮ:

1. Утвердить Перечень персональных данных, обрабатываемых в информационной системе/информационных системах с использованием средств автоматизации;

2. Утвердить Перечень персональных данных, обрабатываемых без использования средств автоматизации.

4. Перечень сотрудников, имеющих доступ к персональным данным.

3. Перечень предназначен для работников ООО « _____», выполнение должностных обязанностей которых связано с использованием сведений персонального характера.

4. Ознакомить с настоящим перечнем работников ООО « _____ » в части их касающейся

Руководитель _____ / _____
Подпись **ФИО**

Утверждено

Руководитель ООО « _____ »

« _____ » _____ 20.... г.

ПЕРЕЧЕНЬ
групп должностей предприятия, имеющих доступ к документам, содержащим информацию о персональных данных

1. **Управление**
   - 1.1. **Заместитель руководителя**
   - 1.2. **Помощник руководителя**
   - 1.3. _____
2. **Бухгалтерия**
   - 2.1. **Главный бухгалтер**
   - 2.2. **Заместитель главного бухгалтера**
   - 2.3. **Бухгалтер**
   - 2.4. _____
3. **Отдел кадров**
   - 3.1. **Начальник отдела кадров;**
   - 3.2. **Сотрудник**
4. **Информационные технологии**
   - 4.1. **Директор по ИТ**
   - 4.2. **Администратор баз данных**
   - 4.3. _____
5. **Юридическая группа**
   - 5.1. **Руководитель группы**
   - 5.2. **Юрисконсульт**
   - 5.3. _____
6. **Отдел продаж**
   - 6.1. **Начальник отдела**
   - 6.2. **Менеджер по продажам**

Утверждено

Руководитель ООО «_____ »

«_____» _____ 20.... г.

ПЕРЕЧЕНЬ
групп должностей предприятия, имеющих доступ к документам, содержащим информацию о персональных данных

Подразделение/должность	Вид сведений, к которым предоставлен допуск
Управление	
Руководитель	Без ограничений
Заместитель руководителя	Без ограничений
Помощник руководителя	Без ограничений
Бухгалтерия	
Главный бухгалтер	Без ограничений
Заместитель главного бухгалтера	Без ограничений
Бухгалтер по учету труда и заработной платы	В части сведений о персональных данных сотрудников
Отдел продаж	
Начальник отдела	В части персональных данных покупателей, поставщиков
Менеджер по продажам	В части персональных данных покупателей, держателей дисконтных карт

I

Общество с ограниченной ответственностью
« _____ »

ПРИКАЗ №_____

г._____ от _____

Об утверждении лиц, ответственных
за защиту информации, содержащей персональные данные

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом РФ и другими нормативными правовыми документами по вопросам использования и защиты информационных ресурсов, содержащих персональные данные,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за осуществление мероприятий по защите персональных данных в ООО « _____ » _____;

2. Ответственными по подразделениям/отделам назначаются:

- по отделу кадров _____ ;

- по отделу продаж _____;

3. Указанные лица несут персональную ответственность за работу по защите персональных данных в организации.

4. Ознакомить с настоящим приказом работников ООО «_____» в части их касающейся.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель _____ / _____
Подпись **ФИО**

ДОГОВОР О КОНФИДЕНЦИАЛЬНОСТИ

г. _____ 20 _____ г.

1. Организация _____ в лице _____ действующего на основании _____ , именуемое в дальнейшем «Организация», и гражданин _____ , именуемый в дальнейшем «Работник», заключили настоящий договор о нижеследующем.

2. Работник принимает на себя следующие обязательства:
   - 2.1. Не разглашать сведения о персональных данных (сведения персонального характера), которые будут ему доверены или станут известны в ходе выполнения своих должностных обязанностей;
   - 2.2. Не передавать третьим лицам и не раскрывать публично сведения персонального характер, без письменного согласия администрации организации;
   - 2.3. Выполнять относящиеся к работнику требования приказов, инструкций и положений по обеспечению сохранности сведений персонального характера;
   - 2.4. Не использовать полученную информацию, в том числе персональные данные о физических лицах (субъектах персональных данных), для занятия другой деятельностью, которая в качестве конкурентного действия может нанести ущерб организации;
   - 2.5. В случае попытки посторонних лиц получить от работника сведения персонального характера в отношении иных лиц, незамедлительно известить об этом руководство организации;
   - 2.6. Незамедлительно сообщать руководству организации об утрате или недостаче носителей информации, содержащих сведения персонального характера, удостоверений, пропусков, ключей от помещений организации, сейфов, печатей и о других фактах, которые могут привести к разглашению данных сведений, а также о причинах и условиях возможной утечки информации;
   - 2.7. В случае увольнения все носители информации, содержащие персональные данные (документы, диски, дискеты, распечатки, кино- и фотоматериалы, изделия и др.), которые находились в распоряжении работника в связи с выполнением им служебных обязанностей во время работы в организации, передать руководству организации.
   - 2.8. Уволившийся работник обязан в течение трёх лет не разглашать и не использовать для себя или других лиц персональные данные о физических лицах (субъектах персональных данных).
   - 2.9. Невыполнение работником взятых на себя по данному договору обязательств может повлечь наступление гражданской, административной, уголовной либо иной ответственности.

3. К сведениям, содержащим персональные данные (сведения персонального характера) в целях настоящего договора относятся:
   3.1. Данные о сотрудниках организации;
   3.2. Данные о клиентах-физических лицах;
   3.3. иные[24].
4. Работник и организация принимают на себя обязательства не разглашать сведения о заработной плате работников, за исключением случаев, предусмотренных законодательством.
5. Организация должна произвести инструктаж работника относительно системы хранения сведений персонального характера и другой конфиденциальной информации.
6. Данный договор имеет силу, как в случае наличия трудового договора между организацией и работником, так и в случае, когда работник представляет субподрядную организацию, имеющую договорные отношения с организацией.
7. Данный договор является бессрочным.
8. Данный договор подписан в двух экземплярах: один экземпляр хранится в организации, другой экземпляр хранится у работника.

Адреса сторон и подписи:

Работник:	Организация:
Паспорт (серия, номер), выдан _____ (кем, когда)	Адрес:
Инструктаж по системе хранения информации, содержащей персональные данные, и другой конфиденциальной информации прошел	
(Подпись)	(Подпись)

[24] Необходимо указать конкретные категории данных в зависимости от специфики работы организации и обрабатываемых персональных данных.

10. Декларация соответствия

ДЕКЛАРАЦИЯ О СООТВЕТСТВИИ

(Наименование организации-изготовителя, фамилия, имя, отчество индивидуального предпринимателя, принявших декларацию о соответствии)

(Сведения о регистрации организации или индивидуального предпринимателя: наименование регистрирующего органа, дата регистрации, регистрационный номер)

(адрес, телефон, факс)

в лице _____

(Фамилия, имя, отчество руководителя организации, от имени которой принимается декларация)

заявляет, что _____

(Наименование, тип, марка продукции, на которую распространяется декларация, код ОК 005-93 и (или) ТН ВЭД СНГ)

(Сведения о серийном выпуске или партии (номер партии, номера изделий, реквизиты договора, накладная, наименование изготовителя и т. п.))

соответствует требованиям

(Обозначение нормативных документов, соответствие которым подтверждено данной декларацией с указанием пунктов, содержащих требования для данной продукции)

Декларация принята на основании _____

1. Акта классификации ИСПДн от _____ **,** _____

2. Сертификата соответствия (программное обеспечение ...)

3. Сертификата соответствия (антивирусная программа ...)

4. Сертификата соответствия (межсетевой экран ...)

(Информация о документах, являющихся основанием для принятия декларации)

Дата принятия декларации **Декларация о соответствии действительна до**

М.П.

(Подпись) **(Инициалы, фамилия)**

Сведения о регистрации декларации о соответствии

(Наименование и адрес органа по сертификации, зарегистрировавшего декларацию) (Дата регистрации и регистрационный номер декларации)

М.П.

(Подпись) **(Инициалы, фамилия руководителя органа по сертификации)**

11. Правила учета и хранения носителей информации, содержащей персональные данные

Требования об обязательности учета всех защищаемых носителей информации, в том числе с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку) предусмотрен Приказом ФСТЭК России № 58. Данное требование предусмотрено для всех классов информационных систем персональных данных.

Кроме того, требование об учете всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку) предусмотрен Руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация»

В любой организации следует в обязательном порядке предусмотреть правила копирования информации, а также организовать порядок учета и хранения сменный носителей. Следует завести соответствующие журналы, в которых будет зафиксирована информация о конкретных пользователях тех или иных носителей. Так же следует предусмотреть формы актов на уничтожение носителей информации и проводить периодические контрольные проверки с целью установления фактического наличия сменных носителей, содержащих персональные данных, в организации.

Может быть предложена следующая форма журнала учета носителей:

Журнал учета защищаемых носителей информации

Учетный номер	Дата регистрации	Вид носителя	Краткое содержание информации	Максимальная категория ПДн	ФИО лиц, получившего носитель	Дата получения и подпись	Дата возврата и подпись ответственного лица	Отметка об уничто-жении/ передаче носителя

Экз. № _____

АКТ
НА СПИСАНИЕ И УНИЧТОЖЕНИЕ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

ООО « _____»

Мы, нижеподписавшиеся:

1. _____ ;
(должность, фамилия и инициалы)
2. _____ ;
(должность, фамилия и инициалы)
3. _____ ;
(должность, фамилия и инициалы)

составили настоящий акт в том, что перечисленные в нем электронные носители информации подлежат уничтожению как утратившие практическое значение и непригодные для перезаписи:

No. п/п	Вид носителя информации	Учетный номер носителя	Дата поступления	Краткое содержание информации

Всего подлежит списанию и уничтожению _____ (_____) наименований электронных носителей информации
" ___"_____ 20 __ г.

Подписи: 1.
2.
3.

Правильность произведенных записей в акте проверил:

(подпись)

Электронные носители информации перед уничтожением сверили с записяг в акте и полностью уничтожили путем

- - 20 -

Подписи: 1.
..... 2.
3.

Акт составлен в _____ экз.

12. Иные документы

Было бы неправильно говорить, что представленный перечень документов является исчерпывающим. В данном случае определен минимально необходимый «комплект документов», имеющий непосредственное прямое отношение к защите сведений персонального характера и разрабатываемых исключительно в связи с выполнением требований Федерального закона «О персональных данных».

Вместе с тем во многих организациях, особенно в тех, которые обрабатывают значительные массивы персональных данных, целесообразно разработать более «узкие», «специализированные» документы, отражающие порядок действий именно с учетом специфики данной организации, категории персональных данных, режима обработки и т. п.

Кроме того, в большинстве организаций будут разработаны или существуют документы об обеспечении сохранности информации, содержащих коммерческую тайну, о порядке документооборота, о пропускном режиме. Такие документы также надлежит проанализировать и в необходимых случаях внести соответствующие изменения с учетом требований законодательства по защите персональных данных.

К таким документам можно отнести:

- Правила хранения информации, представленной в электронном виде;
- Положение о пропускном режиме на территории/помещениях организации;
- Политика информационной безопасности;
- Положение о коммерческой тайне;
- Положение об информационной сети организации;
- Регламент учета информационных ресурсов;
- Должностные инструкции сотрудников, в том числе администратора безопасности ПДн и пользователя;
- Должностной регламент специалиста по обеспечению безопасности информации;

- Инструкция на случай возникновения внештатной ситуации;
- Рекомендации по использованию программных и аппаратных средств защиты информации;
- иные.

Перечень таких документов в различных организациях будет существенно отличаться. Разрабатывать/перерабатывать данные документы необходимо исключительно во взаимодействии с соответствующим подразделением - ИТ-службой, службой охраны и т. п.

Кроме того, пунктом 4 статьи 6 Федерального закона «О персональных данных предусмотрено, что «в случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке».

Соответственно, заключая договор, в ходе которого осуществляется допуск иных лиц к сведениям персонального характера, обязательным пунктом договора должно быть обеспечение конфиденциальности персональных данных. Например, такая ситуация может иметь место при проведении проверки организации аудиторской фирмой.

Формирование модели угроз

Работы по формированию модели угроз безопасности персональных данных, при их обработке в информационных системах персональных данных с использованием средств автоматизации проводятся в соответствии с основными документами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее - Положение);
- Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462) (далее - Порядок);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.).

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных (Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных).

Пункт 2 Положения «Безопасность персональных данных при их обработке в информационных системах» обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Мероприятия, предусмотренные Положением (п. 12) по обеспечению безопасности ПДн при их обработке в информационных системах включают в себя:

1. выявление угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
7. учет лиц, допущенных к работе с персональными данными в информационной системе;
8. контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
10. описание системы защиты персональных данных.

В Положении (п. 12) отмечено, что необходимым элементом разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных (далее - модель угроз). Далее, в Порядке (п. 16) отмечено, что модель угроз необходима для определения класса специальной информационной системы.

Модель угроз формируется и утверждается оператором в соответствии с методическими документами, разработанными 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», в том числе:

- Методический документ ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Методический документ ФСТЭК России. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Методический документ ФСБ России. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Модель угроз может быть пересмотрена:

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

1. Схема формирования модели угроз

При формировании модели угроз необходимо учитывать что:

- Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, понимаемая как комплекс организационно-технических мероприятий.
- При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее - прямая угроза), так и угрозы, создающие условия для появления прямых угроз, иначе - косвенных угроз.
- Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.
- Никакая система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗПДн не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

При формировании модели угроз необходимо последовательно осуществить следующие шаги:

1. проанализировав источники угроз безопасности и уязвимости элементов ИСПДн, сформировать перечень угроз безопасности персональных данных;
2. описать ИСПДн, указав структуру технических средств и программного обеспечения;
3. определить категории пользователей ИСПДн;
4. определить тип ИСПДн;

5. определить исходный уровень защищенности ИСПДн;
6. определить вероятность реализации угроз в ИСПДн ;
7. определить возможность реализации угроз в ИСПДн
8. оценить опасность угроз;
9. определить перечень актуальных угроз в ИСПДн.

После прохождения всех шагов будет сформирована частная модель угроз. Частная модель угроз составляется для каждой выявленной ИСПДн и оформляется в виде документа Модель угроз безопасности персональных данных.

2. Характеристики безопасности ПДн

Характеристиками безопасности ПДн в контексте нормативных документов являются требования обеспечения конфиденциальности, защиты от уничтожения, изменения, блокирования и другие требования безопасности в отношении ПДн.

Оператор ПДн должен задать требования обеспечения безопасности в отношении обрабатываемых им ПДн.

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

- Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.
- Специальные информационные системы - 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).

К специальным информационным системам должны быть отнесены:

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

3. Перечень угроз

Перечень угроз, уязвимостей и технических каналов утечки информации формируется в соответствии с требованиями руководящих документов ФСТЭК России, при необходимости может быть использован ГОСТ Р 51275-2006.

Определение угроз безопасности персональных данных осуществляется на основе утвержденной ФСТЭК России "Базовой модели угроз безопасности персональных данных". Полный перечень факторов, действующих на безопасность информации, в целях обоснования угроз безопасности информации и требований по ее защите, определен ГОСТ Р 51275-2006.

Состав и содержание угроз безопасности персональных данных (УБПДн) определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн обрабатываемым в ИСПДн.

Как правило, ИСПДн учреждения представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Составляющими ИСПДн являются:

- персональные данные, обрабатываемые в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;

- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
- программные средства (операционные системы, системы управления базами данных и т. п.);
- средства защиты информации (СЗИ), включая СКЗИ;
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т. п.) (далее - ВТСС);
- документация на СКЗИ (если имеются), технические и программные компоненты ИСПДн;

При составлении перечня следует учитывать, что о наличии угрозы свидетельствует наличие источников угрозы и уязвимых звеньев, что может быть использовано для реализации угрозы. Формируя на основе опроса перечень источников угроз ПДн, на основе опроса и сетевого сканирования перечень уязвимых звеньев ИСПДн, а также по данным обследования ИСПДн - перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании дальнейшего анализа этого перечня формируется перечень актуальных угроз безопасности ПДн.

Типовые модели угроз

В зависимости от целей и содержания обработки ПДн оператор может осуществлять обработку ПДн в ИСПДн различных типов.

В документе "Базовая модель угроз безопасности персональных данных" приведены типовые модели угроз безопасности ПДн в зависимости от типа ИСПДн (не нужно путать с понятиями типовая и специальная ИСПДн из приказа ФСТЭК, ФСБ и Мининформсвязи России «Порядок проведения классификации информационных систем персональных данных»).

Выбор типовой модели угроз осуществляется в зависимости от того, имеют ли ИСПДн подключение к сетям общего пользования и (или) сетям международного информационного обмена, а также от их структуры (автономные автоматизированные рабочие места, локальные сети, распределенные ИСПДн с удаленным доступом).

В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации УБПДн и наступления последствий в результате несанкционированного или случайного доступа в "Базовой модели угроз безопасности персональных данных" выделены типовые модели угроз безопасности ИСПДн:

- автоматизированные рабочие места, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

- распределенные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Частные модели угроз

Типовые модели угроз учитывают, в основном, удовлетворение таким характеристикам безопасности как конфиденциальность. В этом смысле следует считать, что типовые модели безопасности соответствуют понятию «типовая ИСПДн». Поэтому при составлении модели угроз специальной ИСПДн перечень угроз безопасности должен быть уточнен (характеристики безопасности - целостность, доступность, защита от уничтожения, блокирования и т. п.).

Если модель угроз ИСПДн не может быть отнесена к типовой, то модель угроз специальной информационной системы разрабатывается с учетом полного списка факторов угроз безопасности ГОСТ Р 51275-2006.

Как в случае типовых моделей угроз, наименьшее количество угроз имеют автоматизированные рабочие места и локальные ИСПДн, не подключенные к сетям общего пользования.

Для каждой угрозы, приведенной в типовой модели и включенной в список угроз при формировании частной модели угроз, следует оценить возможную степень ее реализации. Если она окажется высокой, то это может потребовать применения соответствующих дополнительных технических средств защиты информации.

Возможность реализации угрозы зависит от уровня исходной защищенности ИСПДн и вероятности реализации угрозы.

4. Выявление источников угроз

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

- нарушители;
- носители вредоносной программы;
- аппаратные или программные закладки.

Нарушитель - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из подсетей локальной сети, внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, - внутренние нарушители.

Для ИСПДн, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационным ресурсам ИСПДн, правил выполнения работ и мер по контролю порядка проведения работ.

Угрозы несанкционированного доступа внешних нарушителей к ресурсам ИСПДн реализуются с использованием сетевых протоколов локально вычислительной сети (ЛВС) и протоколов межсетевого взаимодействия. Возможности нарушителей существенно зависят от установленных правил эксплуатации, корректной настройки программно-аппаратного обеспечения ЛВС.

Имеет смысл классифицировать персонал организации по ролевым признакам в отношении к ИСПДн. Типовой состав пользователей ИСПДн может быть представлен в виде таблицы (матрицы доступа).

Матрица доступа в табличной форме отражает права всех групп пользователей ИСПДн на действия с персональными данными. Пользователи ИСПДн выполняют следующие действия (операции): сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, и уничтожение персональных данных.

Как правило, существуют три основные группы пользователей ИСПДн:

- Администраторы ИСПДн, осуществляющие настройку и установку технических средств ИСПДн и обеспечивающие ее бесперебойную работу;
- Разработчики ИСПДн, осуществляющие разработку и поддержку программного обеспечения собственной разработки или стандартных программ, специально доработанных под нужды организации;
- Операторы ИСПДн, осуществляющие текущую работу с персональными данными.

Таблица № 9

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	**Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.**	**сбор систематизация накопление хранение уточнение использование распространение обезличивание блокирование уничтожение**
Разработчик ИСПДн	**Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информаций о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн**	**систематизация накопление хранение уточнение обезличивание блокирование уничтожение**
Оператор ИСПДн	**Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и(или)распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн.**	**сбор систематизация накопление хранение уточнение использование распространение обезличивание**

Состав групп может быть уточнен, например, может быть несколько групп операторов ИСПДн. Одна осуществляет лишь сбор и систематизацию персональных данных, другая - уточнение, использование и распространение, третья - резервное копирование и т. д. В матрице доступа должно быть описание всех

групп, обладающих правами на определенные действия с ПДн. Должен быть уточнен список разрешенных действий каждой из групп.

Должен быть предусмотрен порядок предоставления и прекращения доступа тем или иным пользователям, при наступлении, каких событий (прием и увольнение с работы, инициатива или требование руководителя, службы безопасности и т. п.) и на основании каких документов (политик и инструкций) происходит предоставление и прекращение доступа.

Сотрудники выявленных групп пользователей, должны быть рассмотрены в качестве потенциальных внутренних нарушителей - источников угроз безопасности.

5. Выявление уязвимостей ИСПДн Организационно-территориальная структура предприятия.

Заполняется информация об организационнотерриториальной структуре организации, входящей в защищаемую зону автоматизации, к которой предъявляются требования по защите персональных данных.

Оборудование и системное программное обеспечение

Заполняются сведения об оборудовании и системном программном обеспечении, которое будет применяться (применяется) для решения задач обработки ПДн, к которым предъявляются требования по защите.

Информация заполняется в виде таблицы:

Таблица № 10

Роль	Название	Характеристики оборудования	ОС	Прикладное ПО
Роль выполняемая машиной (например, сервер 1С сервер баз данных, рабочая станция и т. д.)	Название компьютера	Процессор (CPU); Память (RAM); Дисковая подсистема; HDD; Сетевые адаптеры (Lan); Порты	Версия операционной системы, включая релизы и сборки.	Перечень прикладного программного обеспечения (включая информацию о релизах и сборках)

Здесь же должна быть приведена схема технической архитектуры (топология ЛВС), параметры каналов связи.

Если информационная база ИСПДн является распределенной привести:

- схему (топология);
- количество узлов (баз данных) в распределенной информационной базе ИСПДн;
- связь между узлами (показывается на схеме);
- расписание сеансов обмена;
- объектный (функциональный) состав обмена;
- примерный объем передаваемых данных, если возможно определить.

На основании указанных сведений производится определение возможных уязвимостей элементов ИСПДн.

6. Пример перечня угроз

Список УБПДн модельной ИСПДн на основе платформы «1С Предприятие».

Как правило, для таковых систем можно выделить следующие угрозы:

2.5.7. Угрозы перегрузки ТС ИСПДн типа DOS-атак (отказ в обслуживании).

2.5.8. Угрозы удаленного запуска приложений.

2.5.9. Угрозы внедрения по сети вредоносных программ.

Определение УБПДн производится на основании анализа источников угроз безопасности и уязвимостей ИСПДн. Список УБПДн составляется в зависимости от структуры и других характеристик ИСПДн. Так, если ИСПДн не имеет подключения к сетям общего пользования и (или) международного обмена, то угрозы несанкционированного доступа по каналам связи, можно убрать из общего списка угроз.

7. Определение уровня исходной защищенности

Исходная защищенность ИСПДн определяется в соответствии с утвержденной ФСТЭК России "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных". Расчет исходной защищенности ИСПДн осуществляется по таблице, приведенной в "Методике...", в зависимости от ряда показателей, по которым подразделяются ИСПДн.

При задании исходных параметров ИСПДн необходимо учесть, что системы подразделяются по структуре, по наличию подключений к сетям общего пользования, по режиму обработки, по разграничению прав доступа, по местонахождению технических средств:

- По структуре информационные системы подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.
- 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.

- По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.
- По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.
- 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 находятся за пределами Российской Федерации.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице.

Показатели исходной защищенности ИСПДн (пример)

Таблица № 11

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	-	-	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	-	-	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	-	+	-
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	-	+	-
локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования: ИСПДн, имеющая многоточечный выход в сеть общего пользования;	-	-	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	-	+	-
ИСПДн, физически отделенная от сети общего пользования	+	-	-

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск;	+		
запись, удаление, сортировка;	-	+	-
модификация, передача	-	-	+
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	-	+	-
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	-	-	+
ИСПДн с открытым доступом	-	-	+
5. По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	-	-	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн	+		

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т. д.);	+	-	-
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	-
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т. е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	~	—	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая всю базу данных с ПДн;			+
ИСПДн, предоставляющая часть ПДн;	-	+	-
ИСПДн, не предоставляющая никакой информации.	+	-	-

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу).
2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.
3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1, а именно:

- 0 - для высокой степени исходной защищенности;
- 5 - для средней степени исходной защищенности;
- 10 - для низкой степени исходной защищенности.

Пример расчета исходной защищенности для типовой ИСПДн, выполненной в виде типовой конфигурации для платформы «1С:Предприятие 8» с исходными параметрами:

Таблица № 12

Заданные характеристики безопасности персональных данных	Специальная информационная система К персональным данным предъявляется требование целостности и доступности
Структура информационной системы	Локальная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	К сетям общего пользования не подключена
Режим обработки персональных данных	многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничение доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации

Оценка исходной защищенности может быть представлена таблицей № 13:

Таблица № 13

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	высокий
2	По наличию соединения с сетями общего пользования	высокий
3	По встроенным (легальным) операциям с записями баз персональных данных	средний
4	По разграничению доступа к персональным данным	средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	средний
6	По уровню (обезличивания) ПДн	средний
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний
	Уровень защищенности	средний
	Значение Y_1	5

Выполнение расчета уровня исходной защищенности позволяет сделать вывод, что уровень защищенности средний, и значение коэффициента Y1 равно 5.

8. Вероятность реализации угроз

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- ***маловероятно*** - отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- ***низкая вероятность*** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- ***средняя вероятность*** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
- ***высокая вероятность*** - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент V_2, а именно:

- 0 - для маловероятной угрозы;
- 2 - для низкой вероятности угрозы;
- 5 - для средней вероятности угрозы;
- 10 - для высокой вероятности угрозы.

Коэффициент реализуемости угрозы Y будет определяться соотношением

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

9. Реализуемость угроз безопасности

В соответствии с "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" осуществляется расчет возможности реализации угроз и оценка их опасности.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 \le Y \le 0,3$,то возможность реализации угрозы признается низкой;
- если $0,3 < Y \le 0,6$, то возможность реализации угрозы признается средней;
- если $0,6 < Y \le 0,8$, то возможность реализации угрозы признается высокой;
- если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Оценка возможности должна проводиться с учетом того, что в ряде случаев возможности реализации отдельных угроз могут быть более высокими и потребовать дополнительных мер защиты персональных данных. Например, возможность реализации угроз увеличивается, если:

- доступ в помещения не контролируется;
- при обработке персональных данных используются аудио и видео устройства;

- экран монитора может просматриваться посторонними через окно или посетителями как внутренними, так и внешними;
- используются беспроводные устройства, включая беспроводные клавиатуры и мыши;
- легко подбираются, либо плохо охраняются пароли, либо, вообще, отсутствует парольная защита (например для доступа к ресурсам серверов, СУБД, серверов приложений, BIOS рабочих станций);
- используются средства сетевого взаимодействия по электропроводке или беспроводные;
- запуск неразрешенных приложений не контролируется, включая запуск программного обеспечения для мобильных устройств, игр и т. п.

Примечание. В контексте методики определения актуальных угроз факты наличия, отсутствия, достаточности или недостаточности уже принятых в организации мер по обеспечению безопасности необходимо учитывать на этапе определения вероятности реализации угроз безопасности ПДн.

Если в организации существует система мер по обеспечению безопасности, например, контролируется вход сотрудников в рабочие помещения, регламентировано использование программного обеспечения рабочих станций, кабельные линии проложены в каналах, недоступных для внешних подключений, мониторы рабочих станций недоступны для неконтролируемого просмотра и т. д. и т. п. Кроме этого, если в организации утверждены инструкции и правила работы с информацией, то вероятность реализации УБПДн будет ниже. Данные факты должны быть учтены при оценке вероятности реализации и, далее, при определении показателя реализуемости УБПДн.

Ниже приводится таблица определения реализуемости УБПДн некоторой модельной ИСПДн в организации, где на момент формирования модели угроз безопасности уже был принят ряд мер по обеспечению защиты информации. Перечень угроз безопасности для данной ИСПДн был определен выше.

Таблицы определения реализуемости угроз безопасности

Таблица № 14

Угроза безопасности ПДн	Принятые меры по обеспечению безопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
1. Угрозы от утечки по техническим каналам.						
1.1. Угрозы утечки акустической информации	Определен порядок и инструкции Регламентирован технологический процесс на рабочих станциях	Звукоизоляция.	Маловероятно	0	0,25	низкая
1.2. Угрозы утечки видовой информации		Жалюзи на окнах	Маловероятно	0	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН		Генераторы зашумления Генератор шума по цепи электропитания Контур заземления	Маловероятно	0	0,25	низкая
2. Угрозы несанкционированного доступа к информации.						
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
2.1.1. Кража ПЭВМ	Пропускной режим Охрана Инструкция по использованию средств защиты Рабочей станции	Охранная сигнализация Решетки на окна Металлическая дверь Кодовый замок Шифрование данных рабочей станции	Маловероятно	0	0,25	низкая

Угроза безопасности ПДн	Принятые меры по обеспечению безопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
2.1.2. Кража носителей информации	Порядок учета и хранения носителей информации	Охранная сигнализация Решетки на окна Металлическая дверь Сейф и кодовым замком Шифрование данных	Маловероятно	0	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	Инструкция пользователю	Защита доступа к ключам	Маловероятно	0	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации			Маловероятно	0	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Технологический регламент, ответственность за несанкционированный доступ сотрудников	Опечатывание, опломбирование	Маловероятно	0	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Ремонт в организация, имеющих лицензию		Маловероятно	0	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты			Маловероятно	0	0,25	низкая

Угроза безопасности ПДн	Принятые меры по обеспечению безопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционирова доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математи воздействий).						иного ческих
2.2.1. Действия вредоносных программ (вирусов)			Низкая	0	0,35	низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных			Маловероятно	0	0,25	низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей			Маловероятно	0	0,25	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и С ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т п) характ						ЗПДн в ера.
2.3.1. Утрата ключей и атрибутов доступа	Инструкция пользователя и администратора		Низкая	0	0,35	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Настройка средств защиты	Технология резервного копирования	Маловероятно	0	0,25	низкая

Угроза безопасности ПДн	Принятые меры по обеспечению безопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
2.3.3. Непреднамеренное отключение средств защиты	Доступ к установлению режимов работы средств защиты предоставляется только администратору	Инструкция пользователя Инструкция администратора безопасности	Маловероятно	0	0,25	низкая
2.3.4. Выход из строя аппаратно-программных средств	Средства зеркалирования замены и восстановления	Технология резервного копирования	Маловероятно	0	0,25	низкая
2.3.5. Сбой системы электроснабжения	Использование источника бесперебойного электропитания	Технология резервного копирования	Маловероятно	0	0,25	низкая
2.3.6. Стихийное бедствие			Маловероятно	0	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки	Система защиты от НСД	Маловероятно	0	0,25	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Договор о не разглашении		Низкая	2	0,35	низкая

Угроза безопасности ПДн	Принятые меры по обеспечению безопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
2.5.Угрозы несанкционированного доступа по каналам связи.						
2.5.1. Перехват в пределах контролируемой зоны внутренними нарушителями.	Технологический процесс Инструкция пользова	Шифрование Физическая зашита каналов связи,	Маловероятно	0	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	теля Инструкция администратора безопасности Акт установки средств защиты	Мониторинг сетевого трафика	Маловероятно	0	0,25	низкая
2.5.3.Угрозы выявления паролей по сети			Маловероятно	0	0,25	низкая
2.5.4.Угрозы навязывание ложного маршрута сети			Маловероятно	0	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети			Маловероятно	0	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях			Маловероятно	0	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»			Маловероятно	0	0,25	низкая

Угроза безопасности ПДн	Принятые меры по обеспечению I Кеэопасности		Вероятность реализации угрозы	Y2	Коэфф. реализу-емости (Y)	Реализуемость угрозы
	Организационные	Технические				
2.5.8. Угрозы удаленного запуска приложений			Маловероятно	0	0,25	низкая
2.5.9. Угрозы внедрения по сети вредоносных программ			Маловероятно	0	0,25	низкая

10. Оценка опасности угроз

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

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

Отметим, что оценку опасности реализации угроз ПДн необходимо выполнять в увязке с классом ИСПДн, определенном в соответствии с нормативным документом «Порядок проведения классификации информационных систем персональных данных».

Действительно, поскольку оценка опасности проводится в отношении опасности одной угрозы или одного типа угроз, а ИСПДн классифицируется в отношении категории ПДн и объема обрабатываемых ПДн (количество субъектов ПДн, ПДн которых обрабатываются в одной ИСПДн).

Определение опасности угроз производится на основании опросных листов оценки опасности угроз.

Эксперты определяют опасность реализации угрозы как:

- ***низкая*** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, что соответствует реализации угроз в ИСПДн класса КЗ;
- ***средняя*** - если реализация угрозы может привести к негативным последствиям для субъектов персональ-

ных данных, что соответствует реализации угроз в ИСПДн класса К2;

- ***высокая*** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, что соответствует реализации угроз в ИСПДн класса К1.

Если нарушение заданной характеристики безопасности персональных данных не приводит к негативным последствиям для субъектов персональных данных, что соответствует реализации угроз в ИСПДн класса К4.

В случае если ранее класс системы определен как достаточно низкий, например - К3, но по оценкам экспертов опасность реализация какой- либо угрозы будет признана средней или высокой, следует пересмотреть результаты классификации ИСПДн

Структуры ИСПДн использующие платформу «1С:Предприятие» на основе типовых конфигураций, состав и объем ПДн, обрабатываемых в них позволяют, в большинстве случаев, отнести их к классу К3 или, что значительно реже, к классу К2.

11. Определение актуальности угроз

После оценки возможности реализации угрозы и определения показателей опасности реализации угрозы необходимо осуществить выбор из общего (предварительного) перечня угроз безопасности те, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами отнесения угрозы безопасности к актуальной.

Правила отнесения угрозы безопасности ПДн к актуальной приведены в нижеследующей таблице (см. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»).

Таблица № 15

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В соответствии с правилами отнесения угрозы к актуальной таблица реализуемости угроз и оценки достаточно просто преобразуется в таблицу актуальности угроз безопасности ПДн: Таблица актуальности угроз безопасности для модельной ИСПДн на платформе «1С:Предприятие»:

Таблица № 16

Тип угроз безопасности ПДн	Актуальность угрозы
1. Угрозы утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	не актуальная
1.2. Угрозы утечки видовой информации	не актуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	не актуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	не актуальная
2.1.2. Кража носителей информации	не актуальная
2.1.3. Кража ключей и атрибутов доступа	не актуальная
2.1.4. Кражи, модификации, уничтожения информации	не актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	не актуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	не актуальная
2.1.7. Несанкционированное отключение средств защиты	не актуальная

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программноматематических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекпарированные возможности системного ПО и ПО для обработки персональных данных	не актуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	не актуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т. п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	не актуальная
2.3.3. Непреднамеренное отключение средств защиты	не актуальная
2.3.4. Выход из строя аппаратно-программных средств	не актуальная
2.3.5. Сбой системы электроснабжения	не актуальная
2.3.6. Стихийное бедствие	не актуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	не актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	не актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	не актуальная
2.5.3.Угрозы выявления паролей по сети	не актуальная
2.5.4.Угрозы навязывание ложного маршрута сети	не актуальная
2.5.5.Угрозы подмены доверенного объекта в сети	не актуальная

2.5.6.Угрозы внедрения ложного объекта в ИСПДн	не актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	не актуальная
2.5.8.Угрозы удаленного запуска приложений	не актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	не актуальная

В результате по данным таблицы актуальности угроз получается **перечень актуальных угроз** (вырезка из таблицы актуальности):

- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программноаппаратных и программных средств (в том числе программно-математических воздействий) (2.2.1. Действия вредоносных программ (вирусов));
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т. п.) характера (2.3.1. Утрата ключей и атрибутов доступа).

Таким образом, с использованием данных о классе ИСПДн и составленного перечня актуальных угроз, «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного Приказом ФСТЭК России № 58 формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и/или дальнейшей эксплуатации ИСПДн.

Соблюдение требований Федерального закона № 152-ФЗ в решениях фирмы «1С»

1. Использование защищенного программного комплекса «1С:Предприятие, версия 8.2z»

Нормы законодательства о защите персональных данных предъявляют дополнительные требования и в части использования операторами ПДн программного обеспечения.

В частности, в пункте 5 Положения об обеспечении безопасности ПДн при их обработке в ИСПДн, утвержденного Постановлением Правительства России № 781 предусмотрено, что средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

Порядок сертификации средств защиты информации в отношении технических, криптографических, программных и других средств, предназначенных для защиты сведений, составляющих государственную тайну, средства в которых они реализованы, а также средства контроля эффективности защиты информации, определен Положением о сертификации средств защиты информации, утвержденным Постановлением Правительства РФ от 26.06.1995 № 608.

Вместе с тем особый порядок проведения процедуры соответствия программных средств общего назначения со встроенными средствами от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, в настоящее время не определен.

Именно пунктом 2.12 Положения, утвержденного Приказом ФСТЭК России № 58, предусмотрено, что программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия недекларированных возможностей, при этом пунктом 7 данного приказа определено, что необходимо применять программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.

Необходимость проведения контроля отсутствия недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов, определяется оператором (уполномоченным лицом).

Таким образом, в случае, если в ИСПДн содержатся данные лиц, имеющих отношение только к одной организации (сотрудники, покупатели, учредители, потенциальные клиенты и т. п.), при этом информации, касающейся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, то такой ИСПДн может быть присвоен 2 или 3 класс, для которого применение сертифицированного программного продукта с обязательной проверкой отсутствия НДВ, не обязательно.

Если ИСПДн содержит сведения о персональных данных, имеющих отношения к нескольким организациям (ведение баз в отношении нескольких организаций предусмотрено в программных продуктах фирмы «1С»), причем объем сведений значителен, то в таких случаях может быть рекомендовано в целях обеспечения защиты персональных данных использовать сертифицированные программные продукты, которые прошли сертификацию/проверку в том числе и на контроль отсутствия НДВ.

Следует обратить внимание, что рассматриваемым приказом ФСТЭК России не определено лицо, обязанное проводить сертификацию программного продукта, т. е. провести сертификацию может как разработчик ПО, так и непосредственно оператор ИСПДн. Т. е. в случаях применения программного обес

печения, в отношении которого разработчиком не проведен контроль отсутствия недекларированных возможностей, оператором ПДн может быть проведен сертификация в системе ФСТЭК России самостоятельно.

Для информации

В соответствии с определением, приведенным в Руководящем документе Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей» (введен в действие Приказом Председателя Гостехкомиссии от 04.06.1999 №114), недекларированные возможности - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Порядок классификации по уровняю контроля отсутствия недекларированных возможностей определен указанным выше руководящим документом Гостехкомисии.

С учетом требований законодательства, предусмотренных Положением, утвержденным Приказом ФСТЭК России № 58, а также в целях упрощения работы по обеспечению защиты персональных данных фирмой «1С» проведены работы по трем направлениям:

- доработка технологической платформы;
- проведение добровольной сертификации защищенного программного комплекса «1С:Предприятие, версия 8.2z»;
- доработка прикладных программных продуктов;

Проводимые работы позволят существенно упростить организацию и проведение мероприятий по защите персональных данных.

Для соответствия требованиям нормативных правовых актов в части защиты персональных данных информационным системам классов 3 и 2 необходимо фиксировать события аутентификации (входа в систему) и отказа от аутентификации, кото

рые по умолчанию включены, кроме того регистрировать события доступа и отказа в доступе к конкретным персональным данным. Иначе говоря, нужно «уметь» ответить на вопрос «кто, когда, получил доступ к зарплате Иванова», а «кто и когда его получить пытался, но не смог» (из-за ограничения прав).

В версии 8.2.10 платформы 1С:Предприятие добавлены возможности, которые решают эту задачу. А именно: регистрация событий доступа и отказа в доступе к данным и соответственно просмотр сведений о зарегистрированных событиях с точностью до полей данных.

Надо понимать, что регистрация события «Доступ» довольно ресурсоемкая, и хотя предварительные замеры производительности позволяют утверждать, что не будет заметного пользователю увеличения времени выполняемых операций, но, так как результат запроса к защищаемым данным будет фиксироваться вместе с записью о событии, размер журнала регистрации существенно увеличится, поэтому:

- с одной стороны требуется обеспечить соответствие требованиям закона - защитить все области персональных данных;
- с другой стороны минимизировать потери производительности.

Реализовано в версии 8.2.10 (выпущена 18.12.2009г.)

- **Функциональность относится к задачам DLP (Data Leak Protection)**
- **Реализуются в виде универсального механизма (развитие журнала регистрации)**
- **Регистрация аутентификации и отказа в аутентификации (реализовано в версии 8.2.9)**
- **Регистрация изменений прав пользователей позволяет определить когда какие роли назначались пользователю**
- **Регистрация фактов отказа в доступе**
  - **Регистрируются все факты отказа в доступе пользователю**
  - **Например, для поиска массовых попыток обращения к недоступным для пользователя ресурсам**
- **Регистрация доступа к защищаемым ресурсам**
  - **Разработчик включает регистрацию для доступа к определенным полям по определенным объектам метаданных**
  - **Разработчик описывает какую ключевую информацию необходимо включать в события журнала регистрации для поиска событий**
  - **Система реализует отражение всех фактов доступа к указанной информации (например, сотрудника, к данным которого выполнялось обращение)**
  - **Система предоставляет возможность отбора зарегистрированных событий по метаданным и данным. Например, поиск всех обращений к защищаемым данным по конкретному физическому лицу.**

При рассмотрении вопроса о проведении сертификации программного продукта учтено, система программ «1С:Предприятие 8» включает в себя технологическую платформу и прикладные решения, разработанные на ее основе, для автоматизации деятельности организаций и частных лиц. Сама платформа не является программным продуктом для использования конечными пользователями, которые обычно работают с одним из многих прикладных решений (конфигураций), разработанных на данной платформе.

Такой подход позволяет автоматизировать различные виды деятельности, используя единую технологическую платформу.

При принятии решения о порядке проведения сертификации программных продуктов, разработанных фирмой «1С», в системе ФСТЭК России было учтено, что изменения в технологическую платформу вносятся относительно редко, а обновления прикладных решений выходят регулярно.

Фирмой «1С» проведена сертификация защищенного программного комплекса «1С:Предприятие, версии 8.2z» (партии из 10 000 экземпляров продукции, маркированных знаками соответствия с № Г 420000 по № Г 429999) на соответствие требованиям руководящих документов по защите от несанкционированного доступа (НСД) - 5 класс. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) по 4 уровню контроля». Получен сертификат ФСТЭК России № 2137, со сроком действия до 20.07.2013, в соответствии с которым защищенный программный комплекс «1С: Предприятие, версии 8.2z» признан программным средством общего назначения со встроенными средствами защиты от несанкционирован

ного доступа к информации, не содержащей сведения, составляющие государственную тайну. Полученным сертификатом подтверждение соответствие программного продукта указанным выше требованием и разрешено использование защищенного программного комплекса «1С:Предприятие, версии 8.2z» для создания автоматизированных систем до класса 1Г включительно, а также для защиты информации в ИСПДн до класса К1 включительно. Порядок использования и настройки защищенного программного комплекса «1С:Предприятие, версии 8.2z» определены в документации к программному продукту.

Информация о ЗПК «1С:Предприятие, версия 8.2z» внесена в ГОСУДАРСТВЕННЫЙ РЕЕСТР сертифицированных средств защиты информации, размещенный на сайте ФСТЭК России под номером 2844 (http://www.fstec.ru/_razd/_serto.htm).

Важно отметить, что сертифицирована была именно платформа, а не конфигурации (например, «Бухгалтерия предприятия», «Зарплата и управление персоналом» и т. п.), так как именно в платформе реализован функционал, обеспечивающий защиту информации в части управления доступом. В связи с этим для пользователей программ системы «1С:Предприятие 8» достаточно просто перейти на новую версию платформы без необходимости дополнительной сертификации каждого прикладного решения в отдельности.

Порядок и условия продажи ЗПК «1С:Предприятие, версия 8.2z» определены в инфописьме фирмы «1С» от 29.12.2010 № 12891 (http://lc.ru/news/info.jsp?id=T2891).

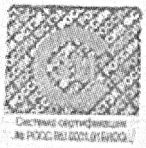
Для информации

Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Данные требования приведены Специальных требованиях и рекомендациях по технической защите конфиденциальной информации (СТР-К).

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2137

Выдан 20 июля 2010 г.
Действителен до 20 июля 2013 г.

Настоящий сертификат удостоверяет, что **защищенный программный комплекс «1С: Предприятие, версия 8.2z»** (партия из 10000 (десяти тысяч) экземпляров продукции, маркированных знаками соответствия с № Г 420000 по № Г 429999) ООО «Научно-производственный центр «1С», функционирующий на аппаратных платформах Intel x86, x64 в среде операционных систем, указанных в формуляре 46.1С.506190-82-01 30, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля, и может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно, а также для защиты информации в информационных системах персональных данных до 1 класса включительно.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники» (аттестат аккредитации от 08.04.2010 № СЗИ RU.2503.Б91.069) – техническое заключение от 06.04.2010, и экспертного заключения от 17.06.2010 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007).

Заявитель: ООО «Научно-производственный центр «1С»
Адрес: 119590, г. Москва, ул. Улофа Пальме, д. 1
Телефон: (495) 681-3763

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники».

НАЧАЛЬНИК УПРАВЛЕНИЯ ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 20 июля 2010 г.

2. Режим соответствия требованиям Федерального закона «О персональных данных» в прикладных решениях «1С:Зарплата и управление персоналом 8» и «1С:Зарплата и кадры бюджетного учреждения 8»

Согласно подзаконным актам степень защиты данных зависит от класса информационной системы, который в свою очередь определяется количеством субъектов (в данном случае физических лиц), количеством организаций и видом обрабатываемых персональных данных. Инструментарий конфигураций «1С:Зарплата и управление персоналом 8» и «1С:Зарплата и кадры бюджетного учреждения 8» способен обеспечить оптимизацию работы с персональными данными в соответствии с требованиями Федерального закона «О персональных данных» информационным системам персональных данных классов 3 и 2, в который и входят большинство систем наших пользователей.

Что сделано в «1С:Зарплата и управление персоналом 8» и «1С:Зарплата и кадры бюджетного учреждения 8»?

Перед разработчиками прикладного решения встает задача - обеспечить гибкую настройку режима соответствия требованиям Федерального закона № 152-ФЗ. В типовых решениях гибкость настройки достигается за счет:

- выделения областей персональных данных;
- управления «детальностью» регистрацией событий.

Данные, подпадающие под определение «персональные», разбиваются на 4 области:

- личные сведения;
- сведения об образовании и компетенциях;
- сведения об имуществе;
- сведения о доходах.

Пользователю (администратору информационной системы) предлагается установить области данных, для которых будет выполняться регистрация событий доступа и отказа в доступе (см. рис. 7).

Вместе с тем это вовсе не означает, что частично «включив» регистрацию событий, мы «частично» выполняем требования закона. В требованиях действующих нормативных правовых актов таких требований не предусмотрено. Просто, наиболее вероятным кажется сценарий, при котором доступ к таким областям данных, как сведения о доходах, например, находится в руках у очень ограниченного круга лиц и детально регистрировать каждое отдельное событие нет необходимости. В этом случае область данных можно «отключить» и снизить нагрузку на систему.

Регистрация списка лиц при доступе к данным определяет «детальность» сведений о событии. От этой настройки зависит, будет ли в журнале расшифровано, «чья именно зарплата была прочитана», или будет указано: «была прочитана зарплата» без расшифровки по записям.

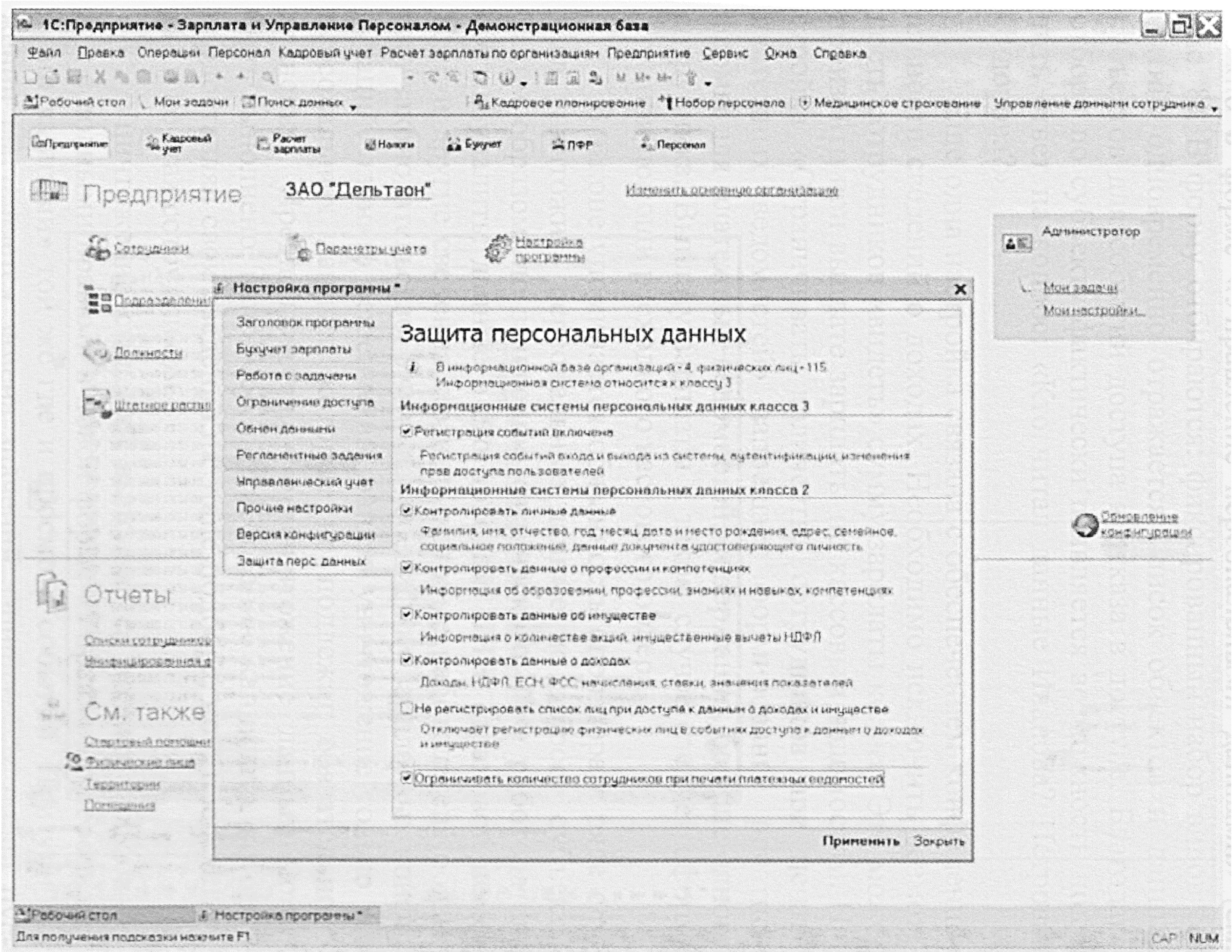


Рис. 7 Настройка режима защиты персональных данных

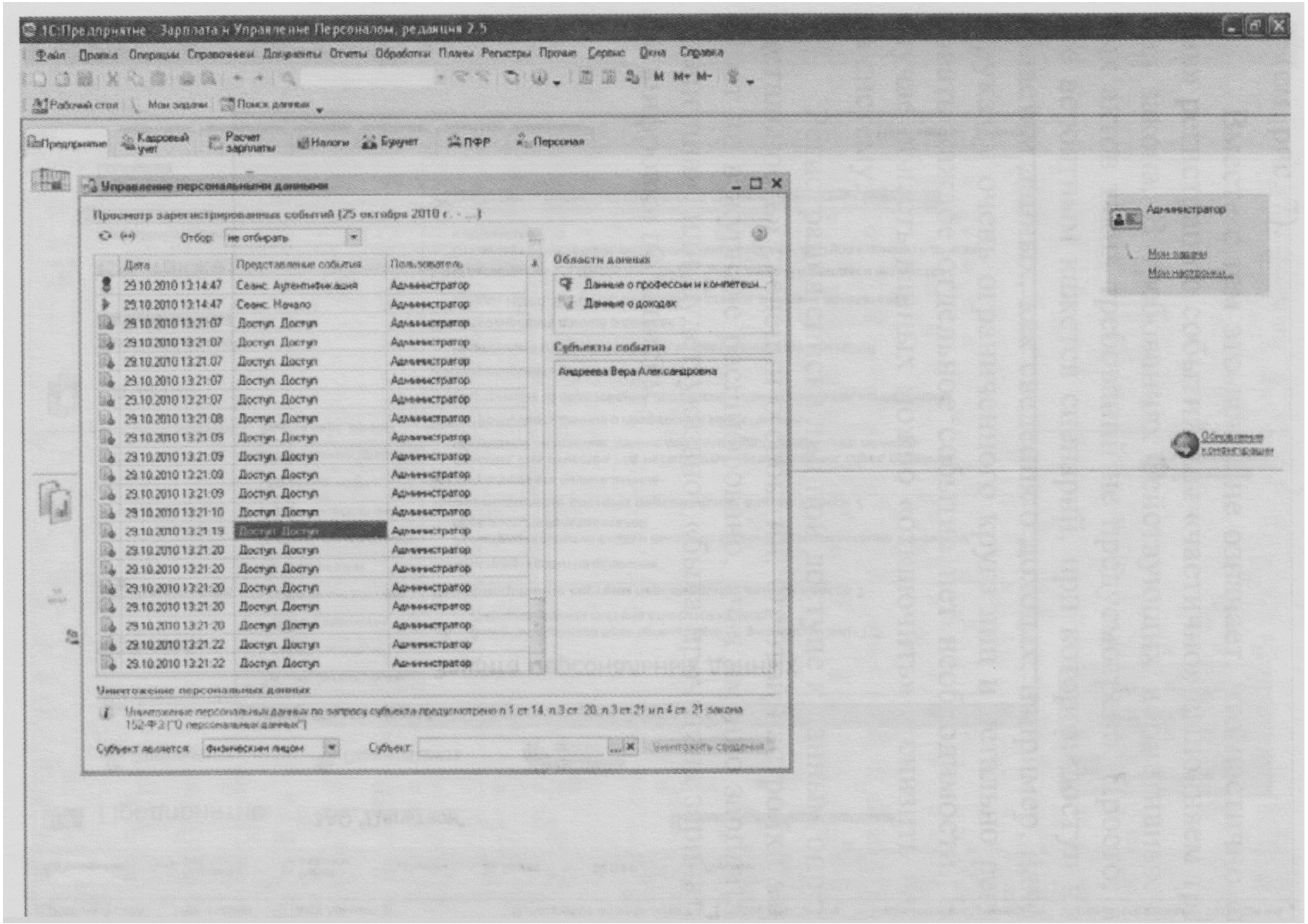


Рис. 8 Форма «Управление персональными данными»

Все события фиксируются в журнале регистрации, но просмотреть новые события в удобной форме «ответов на вопросы» можно в форме «Управление персональными данными» (см. рис. 8). В форму отбираются: фиксированный набор видов событий, одновременно отражается список объектов и данных субъектов для событий доступа и отказа в доступе. Благодаря отбору по субъекту фактически появляется возможность получить ответ на вопрос: «Кто читал данные Иванова? Петрова? Сидорова?»

Еще одна настройка связана с обеспечением конфиденциальности сведений о доходах. Необходимо исключить возможность сотрудников «видеть» сумму зарплаты коллег. Это может произойти при выплате зарплаты по кассовым ведомостям. Настройка «Ограничивать количество сотрудников при печати платежных ведомостей» запрещает формирование печатной формы для платежных ведомостей, содержащих больше одного сотрудника. Выплату зарплаты в таком случае следует оформлять при помощи расходного кассового ордера.

В законе упоминается обязанность оператора в ряде случаев уничтожить персональные данные по запросу субъекта. Таким образом, по заявлению физического лица работодатель обязан удалить: данные о его доходах, ИНН, страховой номер ПФР и другие сведения, хранить которые работодателя обязывает законодательство. Учитывая специфику зарплатных конфигураций, принято решение выполнять уничтожение только тех персональных данных, которые не подлежат обязательному хранению. Предполагается, что уничтожение данных может быть выполнено, например, по требованию кандидата, который предоставлял свои сведения на этапе подбора, но в последствие так и не стал сотрудником.

Уничтожение сведений выполняется только пользователем с полными правами в новой форме «Управление персональными данными» той же где и просмотр событий. При уничтожении выполняется замена значений защищаемых полей пустыми значениями, иначе говоря, происходит очистка полей, а ссылочная целостность базы данных сохраняется.

Кроме того, перед обработкой персональных данных необходимо получить согласие субъекта, который может в общем случае согласиться разрешить обработку только в течение определенного срока. В конфигурациях «1С» предусмотрены соответствующие возможности. В типовую анкету, которая используется в системе как анкета резюме кандидата, может быть дополнительно введено два вопроса:

- «Разрешить обработку персональных данных»
- «Срок предоставления персональных данных, мес.»

Программа позволяет осуществить настройку «обязательности ответа» на данные вопросы. С целью контроля соблюдения законодательства о защите персональных данных рекомендуется указывать «всегда обязателен к заполнению» (рис. 9).

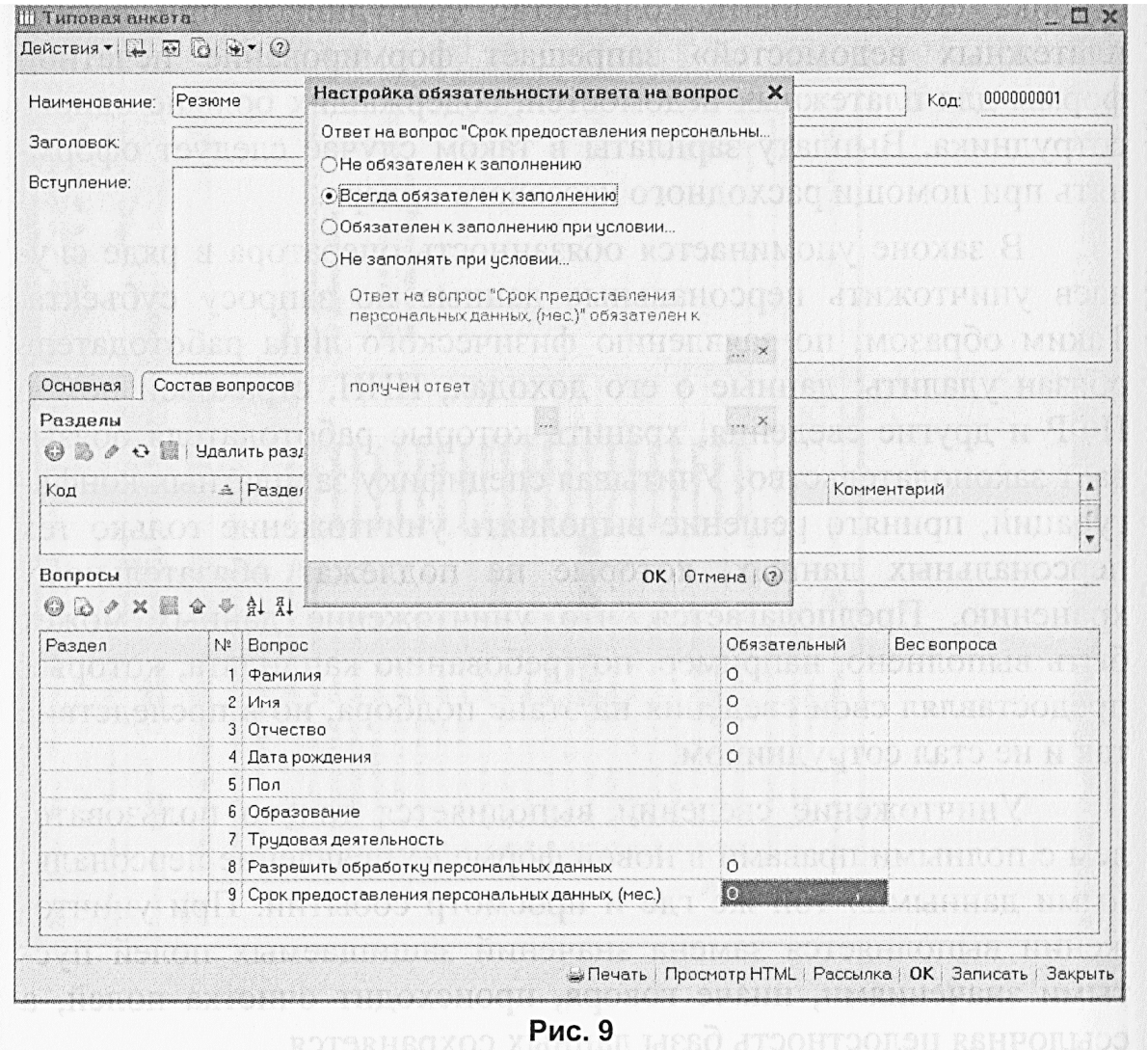


Рис. 9

При заполнении опроса кандидат, или лицо заполняющее опрос кандидата, должен в явном виде «поставить галочку» в поле «Разрешит персональных данных», иначе, документ не будет записан, и сведения не п формационную базу (рис. 10).

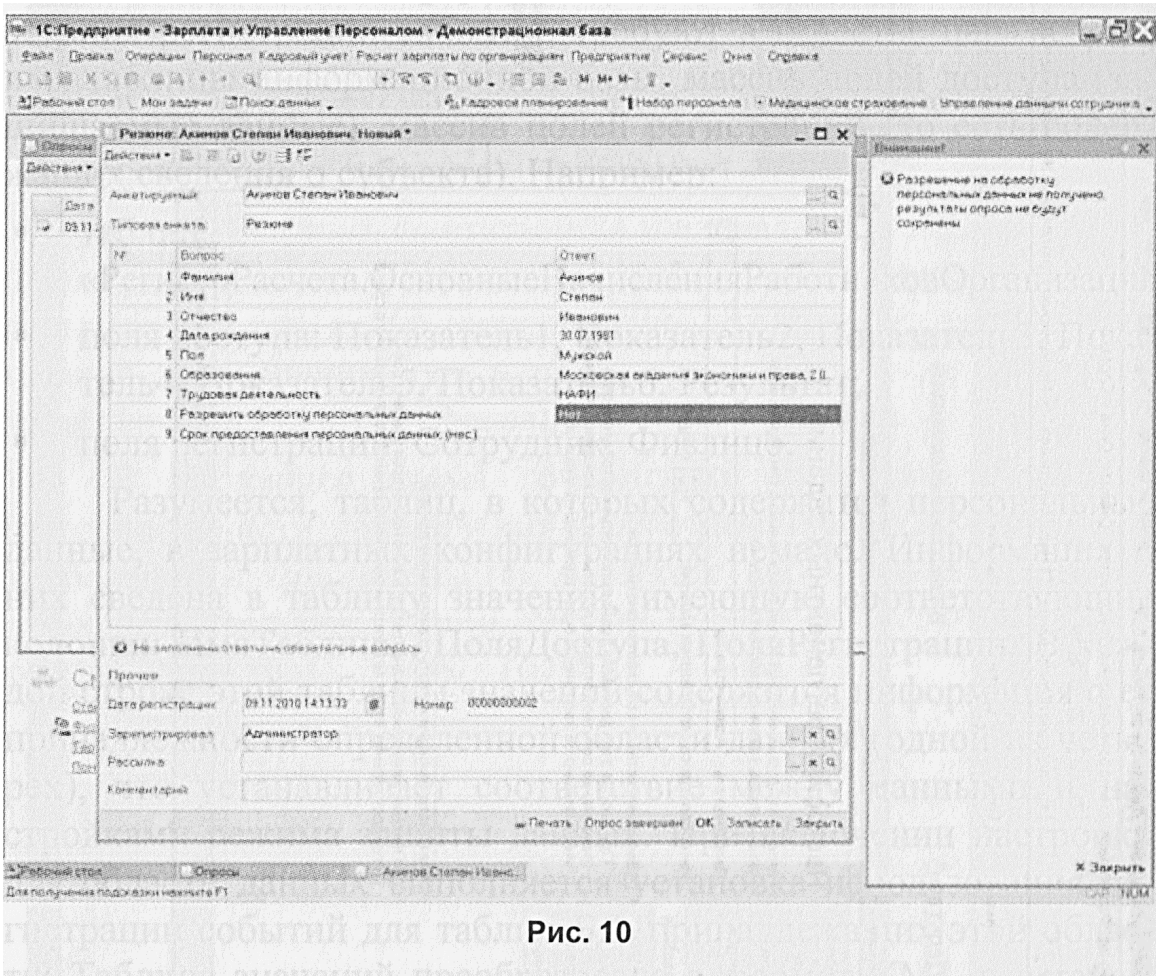


Рис. 10

Кроме того, если включить в настройках регламентных заданий автоматическое уничтожение персональных данных, то данные кандидатов будут уничтожаться автоматически по истечении срока, указанного в опросе (рис. 11).

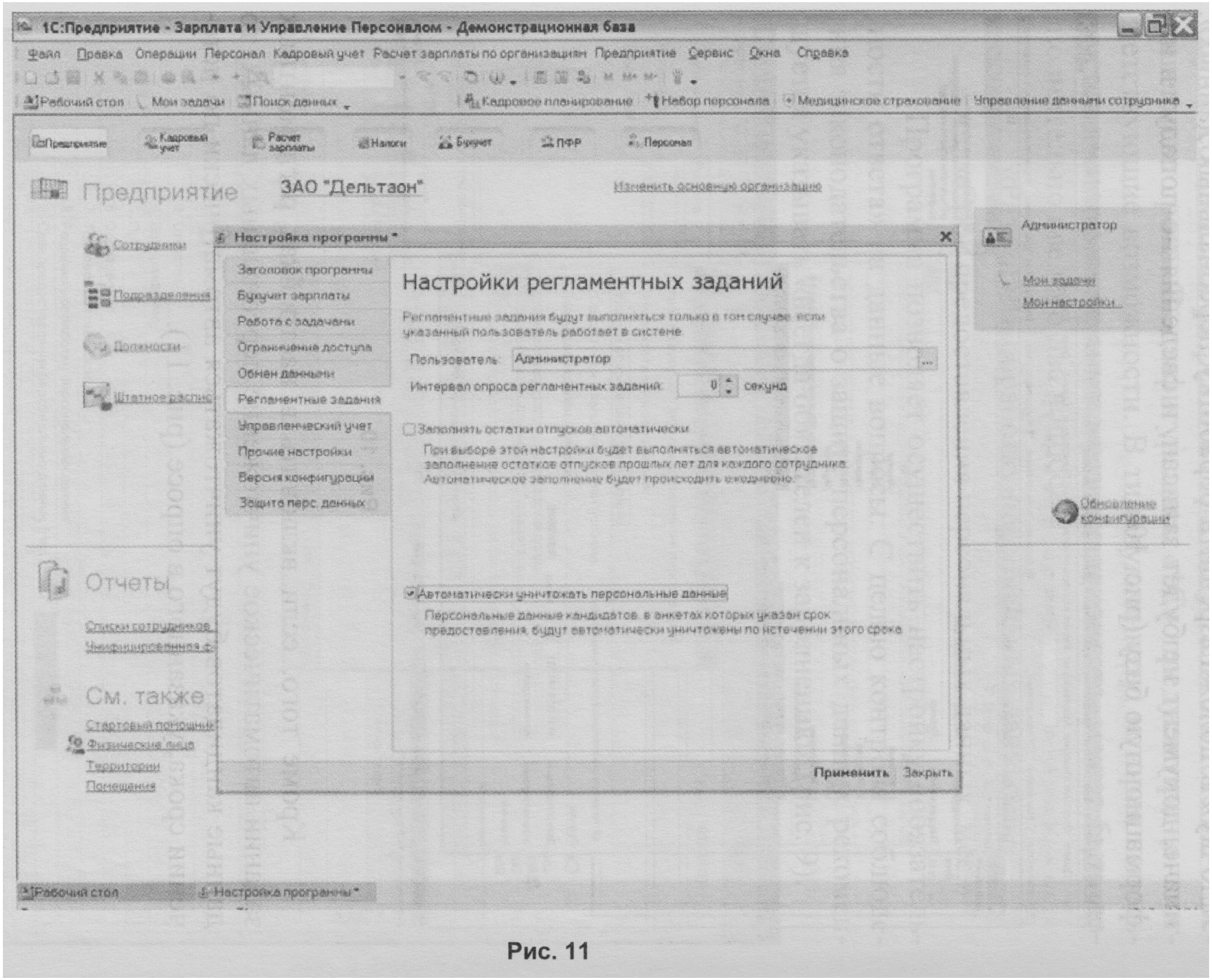

1С:Предприятие - Зарплата и Управление Персоналом - Демонстрационная база
Файл Правка Операции Персонал Кадровый учет Расчет зарплаты по организациям Предприятие Сервис Окна Справка
Рабочий стол Мои задачи Поиск данных
Кадровое планирование Набор персонала Медицинское страхование Управление данными сотрудника
Предприятие
Кадровый учет
Расчет зарплаты
Налоги
Бюджет
ПФР
Персонал
Предприятие
ЗАО "Дельтаон"
Изменить основную организацию
Настройка программы *
Заголовок программы
Бухучет зарплаты
Работа с задачами
Ограничение доступа
Обмен данными
Регламентные задания
Управленческий учет
Прочие настройки
Версия конфигурации
Защита перс. данных
Настройки регламентных заданий
Регламентные задания будут выполняться только в том случае, если указанный пользователь работает в системе.
Пользователь: Администратор
Интервал опроса регламентных заданий: 0 секунд
Заполнять остатки отпусков автоматически
При выборе этой настройки будет выполняться автоматическое заполнение остатков отпусков прошлых лет для каждого сотрудника. Автоматическое заполнение будет происходить ежедневно.
Автоматически уничтожать персональные данные
Персональные данные кандидатов, в анкетах которых указан срок предоставления, будут автоматически уничтожены по истечении этого срока.
Применить
Закрыть
Администратор
Мои задачи
Мои настройки...
Обновление конфигурации
Сотрудники
Подразделения
Должности
Штатное расписание
Отчеты
Списки сотрудников
Унифицированная ф...
См. также
Стартовый помощник
Физические лица
Территории
Помещения
Рабочий стол
Настройка программы *

Рис. 11

Как это работает?

Теперь несколько слов о том, как обеспечивается настройка регистрации новых событий «Доступ» и «Отказ в доступе». Методы объектов платформы, выполняющие установку использования регистрации событий, требуют в качестве параметров: имя таблицы информационной базы, массив полей доступа (защищаемые данные), массив полей регистрации (то есть содержащих сведения о субъекте). Например:

- таблица «РегистрРасчета.ОсновныеНачисленияРаботниковОрганизаций»,
- поля доступа: Показатель 1, Показатель2, ПоказательЗ, Показатель^ Показатель5, Показательб, Результат;
- поля регистрации: Сотрудник, Физлицо.

Разумеется, таблиц, в которых содержатся персональные данные, в зарплатных конфигурациях немало. Информация о них сведена в таблицу значений, имеющую соответствующие колонки: ИмяТаблицы, ПоляДоступа, ПоляРегистрации. В каждой строке этой таблицы значений содержится информация о ее принадлежности определенной области данных (одной из четырех), что устанавливает соответствие между данными и настройками режима защиты данных. При включении настройки для области данных выполняется установка использования регистрации событий для таблиц БД, принадлежащих этой области. Таблица значений преобразована в формат XML и в таком виде поставляется в составе конфигурации в макете двоичных данных «СведенияОПерсональныхДанных».

Важно отметить, что с помощью появившейся в платформе возможности можно решать далеко не только эту, но и другие задачи контроля доступа к данным.

Примечание

Механизм доступен в конфигурациях ЗУП и ЗБУ, начиная с версий 2.5.19 и 1.0.8 соответственно, при использовании платформы 1С:Предприятие версии 8.2.10.

Ответственность за несоблюдение требований законодательства о персональных данных

В соответствии со статьей 24 Федерального закона № 152- ФЗ лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

В настоящее время говорить о правоприменительной практики в части привлечения к ответственности за нарушение требований законодательства о защите персональных данных, несколько

1. Административная ответственность

Статья КоАП	Вид нарушения	Субъект правонарушения	Ответственность
ст. 5. 27	Нарушение законодательства о труде и об охране труда	на должностных *лиц*[25]	штраф в размере от пятисот до пяти тысяч рублей
		на лиц, осуществляющих предпринимательскую деятельность без образования юри- дического лица	штраф в размере от пятисот до пяти тысяч рублей или административное приостановление деятельности на срок до девяноста *суток*
		на юридических лиц	штраф в размере от трех до пяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток
ст. 5.39	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,	на должностных лиц	штраф в размере от одной до трех тысяч рублей.

[25] В соответствии с пунктом 2 статьи 5.27 Ко АП 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 КоАП	Вид нарушения	Субъект правонарушения	Ответственность
	либо предоставление гражданину неполной или заведомо недостоверной информации		
ст. 13.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	на граждан	предупреждение или наложение штрафа в размере от трехсот до пятисот рублей
		на должностных лиц	штраф в размере пятисот до одной тысячи рублей
		на юридических лиц	штраф в размере от пяти до десяти тысяч рублей
ч. 1 ст. 13.12	Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну),	на граждан	штраф в размере от трехсот до пятисот рублей
		на должностных лиц	штраф в размере от пятисот до одной тысячи рублей
		на юридических лиц	штраф в размере от пяти до десяти рублей
ч. 2 ст. 13.12	Использование несертифицированных информационных систем, баз и банков данных, а также несертифициро- ванных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)	на граждан	штраф в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой
		на должностных лиц	штраф в размере от одной до двух тысяч рублей
		на юридических лиц	штраф в размере от десяти до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой

Статья КоАП	Вид нарушения	Субъект правона рушения	Ответственность
ч.3 ст. 13.12	Нарушение условий, предусмотренных лицензией на проведение работ, связанных с ис-пользованием 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	на должностных лиц	штраф в размере от двух до трех тысяч рублей
		на юриди-ческих лиц	штраф в размере от пятнадцати до двадцати тысяч рублей
ч. 4 ст. 13.12	Использование несер-тифицированных средств, предназначенных для защиты информации, составляющей государственную тайну	на должностных лиц	Штраф в размере от трех до четырех тысяч рублей
		на юриди-ческих лиц	штраф в размере от двадцати до тридцати тысяч рублей с конфискацией несер-тифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой
ч. 5 ст. 13.12	Грубое нарушение[26] условий, предусмотренных лицензией на осуществление дея-тельности в области защиты информации (за исключением информации, составляющей государственную тайну)	на лиц, осуществ-ляющих предпринима-тельскую деятельность без образова-ния юр. лица	штраф в размере от тысячи до тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток

[26] Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

Статья КоАП	Вид нарушения	Субъект правона рушения	Ответственность
		на должностных лиц	штраф в размере от тысячи до тысячи пятисот рублей
		на юридических лиц	штраф в размере от десяти до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток
ч. 1 ст. 13.13	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)	на граждан	штраф в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой
		на должностных лиц	штраф в размере от двух до трех тысяч рублей с конфискацией средств защиты информации или без таковой
		на юридических лиц	штраф в размере от десяти до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой
ч. 2 ст. 13.13	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	на должностных лиц	штраф в размере от четырех до пяти тысяч рублей
		на юридических лиц	штраф в размере от тридцати до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой

Статья КоАП	Вид нарушения	Субъект правонарушения	Ответственность
ст. 13.14	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	на граждан	штрафа в размере от пятисот до одной тысячи рублей
		на должностных лиц	штраф в размере от четырех до пяти тысяч рублей
ч. 1 ст. 19.4	Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль), а равно воспрепятствование осуществлению этим должностным лицом служебных обязанностей	на граждан	штраф в размере от пятисот до одной тысячи рублей
		на должностных лиц	штраф в размере от двух до четырех тысяч рублей
ч. 1 ст. 19.5	Невыполнение в установленный срок законного предписания(постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства	на граждан	штраф в размере от трехсот до пятисот рублей
		на должностных лиц	штраф в размере от одной тысячи до двух тысяч рублей или дисквалификацию на срок до трех лет
		на юридических лиц	штраф в размере от десяти тысяч до двадцати тысяч рублей
ч. 2 ст. 19.5	Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа	на должностных лиц	штраф в размере от пяти тысяч до десяти тысяч рублей или дисквалификация на срок до трех лет
		на юридических лиц	штраф в размере от двухсот тысяч до пятисот тысяч рублей.

Статья КоАП	Вид нарушения	Субъект правонарушения	Ответственность
ст. 19.6	Непринятие по постановлению (представлению) органа (должностного лица), рассмотревшего дело об административном правонарушении, мер по устранению причин и условий, способствовавших совершению административного правонарушения	на должностных лиц	штраф в размере от трехсот до пятисот рублей
ст. 19.7	Непредставление или несвоевременное представление в государственный орган (должностному 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, 19.8, 19.19 КоАП	на граждан	штраф в размере от ста до трехсот рублей
		на должностных лиц	штраф в размере от трехсот до пятисот рублей
		на юридических лиц	штраф в размере от трех до пяти тысяч рублей
ч. 1 ст. 19.20	Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна)	на граждан	штраф в размере от пятисот до тысячи рублей
		на должностных лиц	штраф в размере от тысячи до двух тысяч рублей
		на юридических лиц	штраф в размере от десяти до двадцати тысяч рублей

Статья УК РФ	Вид нарушения	Ответственность
	либо осуществление предпринимательской деятельности без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением лицензионных требований и условий, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере	
ч. 2 ст. 171	Осуществление предпринимательской деятельности без регистрации или с нарушением правил регистрации, а равно представление в орган, осуществляющий государственную регистрацию юридических лиц и индивидуальных предпринимателей, документов, содержащих заведомо ложные сведения, либо осуществление предпринимательской деятельности без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением лицензионных требований и условий, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере, а) совершенное организованной группой; б) сопряженное с извлечением дохода в особо крупном размере	штраф 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 лишение свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового

Статья УК РФ	Вид нарушения	Ответственность
ст. 140	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	штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет
ч. 1 ст. 272 УК РФ	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	штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительные работы на срок от шести месяцев до одного года, либо лишение свободы на срок до двух лет

3. Ответственность за нарушения трудового законодател ьства

В соответствии с ТК РФ разглашение персональных данных, а также нарушение норм, регулирующих получение, обработку и защиту персональных данных работников, может грозить работнику организации увольнением (ст. 81, 90 ТК). И частности пункт «в» статьи 81 ТК РФ предусматривает, что трудовой договор может быть расторгнут в случае разглашении охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

Согласно статье 90 ТК РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Баймакова Ирина Александровна,
Новиков Александр Викторович,
Рогачев Алексей Иванович,
Хыдыров Агиль Хыдыр оглы

Обеспечение защиты персональных данных Методическое пособие 3-е издание

Подписано в печать 11.02.2011. Формат 60x90 '/,6.
Бумага офсетная. Гарнитура Arial, Times New Roman. Печать офсетная.
Тираж 2 ООО экз. Заказ 3-471

Издательство ООО «1С-Паблишинг»
127473, Москва, ул. Достоевского, 1/21, строение 1

По вопросам розничного приобретения книг, выпускаемых издательством фирмы «1С» (ООО «1С-Паблишинг») обращайтесь в книжные и интернет-магазины, к партнерам-1С:Франчайзи и в отдел продаж фирмы «1С».

Фирма «1С»
123056, Москва, а/я 64,
Отдел продаж: Селезневская ул., 21 (м. «Достоевская», «Новослободская»)
Тел.: (495) 737-9257, факс: (495) 681-4407 e-mail: lc@lc.ru,
www.lc.ru

По вопросам оптовых закупок учебных и методических пособий по программным продуктам фирмы «1С» обращайтесь в **ООО «1С-Паблишинг»:**
127473, Москва, ул. Достоевского, 1/21, строение 1 Тел.: (495) 681-02-21, факс: (495) 681-44-07 e-mail: publishing@lc.ru
books.lc.ru

_____ Отпечатано с оригиналов фирмы "1С-Паблишинг" _____
Казанский производственный комбинат программных средств 420 044 Казань, ул. Ямашева, 36