Министерство науки и высшего образования Российской Федерации

Уральский государственный экономический университет

Д. М. Назаров, К. М. Саматов

Основы обеспечения безопасности персональных данных в организации

Рекомендовано
Советом по учебно-методическим вопросам и качеству образования
Уральского государственного экономического университета
в качестве учебного пособия

Екатеринбург
Издательство Уральского государственного
экономического университета
2019

УДК 32.973.26я73
ББК 004.056(075.8)
Н19

Рецензенты:

Региональный учебно-научный центр «Интеллектуальные системы и информационная безопасность» Института естественных наук и математики Уральского федерального университета имени первого Президента России Б. Н. Ельцина (протокол № 6 от 30 ноября 2018 г.);

А. В. Савоськин, кандидат юридических наук, доцент, советник судьи Уставного Суда Свердловской области

Назаров, Д. М.

Н19 Основы обеспечения безопасности персональных данных в организации [Текст] : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. — 118 с.

В учебном пособии рассмотрены основные положения обработки и защиты персональных данных в организации, а также вопросы, связанные с защитой персональных данных в рамках международного права и при трансграничной передаче. Уделено внимание проблемам прохождения контрольно-надзорных мероприятий операторами персональных данных.

Предлагаемое учебное пособие предназначено для студентов высших учебных заведений, обучающихся по направлениям 10.03.01 «Информационная безопасность», 09.03.03 «Прикладная информатика в экономике» и 09.03.04 «Информатика и вычислительная техника», а также для специалистов по защите информации.

УДК 32.973.26я73
ББК 004.056(075.8)

Оглавление

Введение

С момента выхода в свет первой редакции Федерального закона «О персональных данных» (2006 г.) прошло 12 лет, и подавляющее большинство физических и юридических лиц уже имеют опыт применения его норм на практике. Однако до сих пор, в попытке улучшить регуляторное воздействие, в законодательные акты по вопросам обработки и защиты персональных данных вносятся поправки. Например, в июле 2017 г. вступили в силу поправки к Кодексу об административных правонарушениях РФ, увеличивающие размеры штрафов за нарушение законодательства в этой сфере.

В настоящее время вопрос обработки персональных данных находится в секторе внимания специалистов по безопасности абсолютно любой организации. Трудно найти организацию, которая не обрабатывала бы персональные данные своих сотрудников или контрагентов. В свою очередь, любой гражданин вступает во взаимоотношения с различными физическими и юридическими лицами, в результате которых образуются массивы (базы данных) персональных данных. В то же время у сотрудников служб информационной безопасности возникают трудности в применении действующих правовых норм, регулирующих данную сферу общественных отношений.

Представляется целесообразным осуществлять обучение по организации обработки и защиты персональных данных в рамках дисциплин «Основы информационной безопасности» и «Основы управления информационной безопасностью» по направлениям подготовки «Информационная безопасность», «Прикладная информатика в экономике» и «Информатика и вычислительная техника».

1. Персональные данные как правовой институт

1.1. Понятие персональных данных: исторический и юридический аспект

Защита частной жизни имеет давнюю историю. Еще в дореволюционный период этот вопрос привлекал внимание ученых-юристов. Правовые нормы, являющиеся составной частью неприкосновенности частной жизни, относящиеся к неприкосновенности корреспонденции, уже имели место в Почтовом уставе 1857 г. и в Уставе о телеграфах 1876 г.

В советский период в Конституцию Союза ССР 1936 г. были включены нормы о неприкосновенности личности, жилища, переписки. Конституция СССР 1977 г. также содержала нормы о защите личной жизни граждан, о тайне переписки, телефонных переговоров и телеграфных сообщений. Однако правовые гарантии конституционного права граждан на неприкосновенность личной жизни были явно недостаточны, в порядке вещей было ограничение рассматриваемых прав.

Новый этап формирования института неприкосновенности частной жизни начался с принятой 22 ноября 1991 г. Декларации прав и свобод человека и гражданина (ст. 9), которая провозгласила право каждого на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, телеграфных и иных сообщений. Принципиальным моментом было установление судебного порядка ограничения указанных прав.

Обозначенная линия неприкосновенности частной жизни прослеживается и в Конституции Российской Федерации

1993 г. (ст. 23, 24). Статья 23 Конституции гарантирует каждому «…право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья 24 установила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия».

Термин «персональные данные», тесно связанный с частной жизнью человека, появился в российском законодательстве в середине 1990-х гг., тогда же были определены основные черты правового режима персональных данных. Федеральным законом от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (ныне утратил силу) персональные данные были отнесены к категории конфиденциальной информации, установлен запрет на сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица, без его согласия, кроме как на основании судебного решения.

При этом содержание понятия «персональные данные» в указанном Федеральном законе не было раскрыто. Позже был издан Указ Президента РФ от 6 марта 1997 г. № 188 (действующий на сегодняшний день), утвердивший Перечень сведений конфиденциального характера, согласно которому персональные данные «включают в себя сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность».

Основы правового режима персональных данных, установленные в Федеральном законе «Об информации, информатизации и о защите информации», содержали ряд черт, характерных для европейской модели защиты персональных данных. Принципиальным различием, сохранившимся до настоящего времени, с европейской моделью правового регулирования является акцент на защиту информации персонального характера в отрыве от защиты прав субъектов персональных данных и их интересов. Указанный подход был реализован и в Федеральном законе от 27 июля 2006 г. № 152-ФЗ

«О персональных данных» (далее — Федеральный закон «О персональных данных») и принятых в его исполнение подзаконных актах.

В декабре 2005 г. Российская Федерация ратифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, взяв на себя тем самым обязательства привести национальное законодательство в соответствие с этой Конвенцией. В рамках данных обязательств были приняты упомянутый Федеральный закон «О персональных данных», который закрепляет общие принципы их охраны, а также ряд подзаконных актов. И хотя нормы названного Закона существенно не отличаются от норм Конвенции, подзаконными актами устанавливаются требования, которые не характерны для законодательства и практики других стран, подписавших Конвенцию.

Кроме того, следует учитывать, что европейское законодательство после принятия Конвенции активно развивалось и страны Европейского союза при формировании механизмов защиты прав личности при обработке персональных данных руководствуются положениями Директив 95/46/ЕС и 97/66/ЕС Европейского парламента и Совета Европы, согласно которым юридические и технические требования, устанавливаемые в целях обеспечения защиты персональных данных, прав частных лиц и законных интересов юридических лиц, должны быть четко сбалансированы, чтобы не создавать помех для развития рынка. Сбалансированность, в свою очередь, означает соразмерность, обоснованность и выполнимость этих требований.

Именно этого недостает в ряде случаев российскому законодательству.

Понятие персональных данных содержалось ранее и в Трудовом кодексе РФ. Так, согласно ст. 85 ТК РФ персональные данные работника — это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Данное определение конкретизировало общее понятие персональных данных применительно к сфере трудовых отношений и не противоречило ему.

В то же время с принятием Федерального закона от 7 мая 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием

Федерального закона „О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных“» и Федерального закона «О персональных данных» ст. 85 ТК РФ утратила силу.

В действующей редакции Федерального закона «О персональных данных» (ст. 3) под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Такое определение появилось благодаря изменениям, внесенным в названный Закон 25 июля 2011 г. Первоначально под персональными данными понималась 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.

Таким образом, из определения исчезло лишь перечисление той информации, которая относится к персональным данным. Поскольку конструкция данной нормы представляла собой открытый перечень, то исключение этого перечня не повлекло особых изменений в существе понятия «персональные данные». Основной критерий остался прежним: относимость информации к конкретному лицу и возможность его идентификации.

По мнению ряда авторов (Р. В. Амелин, Н. В. Богатырева, Ю. В. Волков, Ю. А. Марченко, А. С. Федосин), конкретно указанные в законе атрибуты позволяли правоприменителям приходить к выводу, что простое сообщение фамилии, имени и отчества лица вне зависимости от контекста является распространением персональных данных. Новое же определение более точно соответствует положению ст. 2 Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108, заключена в г. Страсбурге 28 января 1981 г.), согласно которому персональной информацией признана любая информация, касающаяся конкретного или могущего быть идентифицированным лица (субъекта данных).

Вместе с тем, по мнению Л. К. Терещенко, наличие такого перечня в первоначальной редакции Закона сыграло важную

роль, поскольку давало представление о характере информации, относимой законодателем к персональным данным. Несмотря на то что Федеральный закон «О персональных данных» содержит максимально широкую их характеристику, в практической деятельности нередко возникают проблемы с определением того, какая информация относится к персональным данным. Отсутствие перечня в отдельных случаях, в том числе и в судебной практике, позволяет по-разному толковать отнесение тех или иных категорий данных к персональным. Интересным моментом является и то, что вступивший в силу Европейский регламент по защите персональных данных (General Data Protection Regulation) также содержит в себе некоторую конкретизацию персональных данных (см. главу 4).

Широкое толкование и отсутствие перечня информации, относящейся к персональным данным, порождает следующие негативные моменты: во-первых, непонимание операторов (организаций, обрабатывающих персональные данные), что именно необходимо относить к персональным данным, и, во-вторых, широкие возможности контролирующих органов по привлечению операторов к ответственности за непредоставление сведений об обработке персональных данных.

В частности, в судебной практике имеются решения судов по спору между территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и операторами персональных данных, в которых последним вменялось отсутствие в уведомлениях об обработке указания определенных категорий персональных данных. Например, решение Арбитражного суда Свердловской области по делу № А60-41475/2011. Представляется, что наличие умысла организаций при совершении указанных действий маловероятно.

1.2. Система законодательства о персональных данных

В теории права система законодательства определяется как совокупность нормативно-правовых актов, находящихся в иерархическом и субординационном соотношениях друг

с другом. Место каждого нормативного акта в данной системе зависит от его юридической силы, которая, в свою очередь, зависит от уровня органа, принявшего данный акт, и порядка его принятия.

В сфере обработки персональных данных существует следующая система нормативных правовых актов, регулирующих эти правоотношения.

I. *Конституция Российской Федерации и нормы международного права.*

Конституция РФ принята на всенародном голосовании 12 декабря 1993 г. и является Основным законом Российской Федерации. Конституция имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции. Применительно к институту персональных данных Конституция РФ выступает основным гарантом реализации правовых норм, его составляющих, и соблюдения прав граждан в процессе их реализации.

Международные договоры Российской Федерации согласно ст. 5 Федерального закона от 15 июля 1995 г. № 101-ФЗ «О международных договорах Российской Федерации» наряду с общепризнанными принципами и нормами международного права являются составной частью правовой системы Российской Федерации.

Положения официально опубликованных международных договоров Российской Федерации, не требующие издания внутригосударственных актов для применения, действуют в РФ непосредственно. Для осуществления иных положений международных договоров Российской Федерации принимаются соответствующие правовые акты.

Часть 4 ст. 4 Федерального закона «О персональных данных» устанавливает приоритет международных договоров Российской Федерации в области регулирования отношений по обработке персональных данных, а именно: если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены российским законодательством, применяются правила международного договора. Указанная норма дублирует ч. 2 ст. 5 Федерального закона от 15 июля 1995 г. № 101-ФЗ.

Основными международными актами в области защиты персональных данных являются следующие:

• Всеобщая декларация прав человека, принятая на третьей сессии Генеральной Ассамблеи ООН Резолюцией 217A(III) от 10 декабря 1948 г., которая провозглашает, что никто не может подвергаться произвольному вмешательству в личную и семейную жизнь, каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств (ст. 12);

• Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.);

• Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108, Страсбург, 28 января 1981 г.).

В Конвенции определяется порядок сбора и обработки данных о личности, принципы хранения и доступа к этим данным, способы физической защиты данных. Конвенция гарантирует соблюдение прав человека при сборе и обработке персональных данных, а также запрещает обработку данных о расе, политических взглядах, здоровье, религии без соответствующих юридических оснований. Данная Конвенция была ратифицирована Федеральным законом от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» с отдельными заявлениями, в частности, Российская Федерация заявила, что не будет применять Конвенцию к персональным данным:

а) обрабатываемым физическими лицами исключительно для личных и семейных нужд;

б) отнесенным к государственной тайне в порядке, установленном законодательством РФ о государственной тайне;

в) которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации.

Российская Федерация оставила за собой также право устанавливать ограничения прав субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Кроме того, важным на текущий момент является регламент Европейского союза General Data Protection Regulation

принятый в 2016 г. и вступивший в силу в мае 2018 г. (подробному рассмотрению данного регламента посвящена глава 4).

II. *Собственно законодательство Российской Федерации в области обработки персональных данных*. Включает в себя следующие нормативные правовые акты в порядке приоритета:

1) Федеральный закон «О персональных данных», осуществляющий непосредственное прямое регулирование правоотношений в области обработки персональных данных;

2) иные федеральные законы, определяющие случаи и особенности обработки персональных данных, а именно:

• Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

• Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»;

• Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»;

• Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»;

• Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

• Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

• Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

• Федеральный закон от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»;

• Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

• иные федеральные законы.

Часть норм, определяющих отдельные случаи регулирования обработки персональных данных, содержится в кодексах, которые также являются федеральными законами. Так, Семейный кодекс РФ содержит перечень персональных данных, подлежащих установлению в отношении лиц, желающих усыновить ребенка, оформить в отношении него опеку (попечительство) либо взять ребенка в приемную семью (ст. 123 СК РФ). Глава 14 Трудового кодекса РФ (ТК РФ) регулирует защиту персональных данных работника. Гражданский ко-

декс РФ (ГК РФ) содержит нормы, регулирующие право на имя гражданина, в том числе и в международном частном праве (ст. 1198), а также нормы касательно охраны изображения гражданина (ст. 152.1).

Ряд норм, содержащихся в Кодексе об административных правонарушениях РФ (КоАП РФ), Уголовном кодексе РФ (УК РФ), устанавливает ответственность за нарушение законодательства в области обработки персональных данных (подробнее см. параграф 3.5).

III. *На основании и во исполнение федеральных законов* государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты по отдельным вопросам, касающимся обработки персональных данных. Указанные нормативные правовые акты по своей юридической силе являются подзаконными. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию. В категории нормативных правовых актов, регулирующих отношения по обработке персональных данных, можно выделить:

1) указы и распоряжения Президента РФ:

• указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

• указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

• указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

• распоряжение Президента РФ от 10 июля 2001 г. № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;

2) акты Правительства РФ:

• постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

• постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

• постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

• постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

• постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом „О персональных данных“»;

• распоряжение Правительства РФ от 15 августа 2007 г. № 1055-р «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона „О персональных данных“»;

3) нормативные правовые акты федеральных органов исполнительной власти:

• приказ Министерства связи и массовых коммуникаций РФ от 21 декабря 2011 г. № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги „Ведение реестра операторов, осуществляющих обработку персональных данных“»;

• приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 20 июня 2012 г. № 621 «О Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных»;

• приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 3 декабря 2012 г. № 1255 «Об утверждении Положения об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

• приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

• приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

• приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

• приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

• приказ ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;

4) акты органов местного самоуправления в пределах их полномочий (различные политики в области обработки персональных данных).

IV. *Локальные нормативные акты*, регламентирующие порядок обработки персональных данных и их защиты в конкретной организации.

Таким образом, можно говорить о том, что институт персональных данных регламентирован целым набором нормативных актов. При этом действующий на сегодняшний день Фе-

деральный закон «О персональных данных» включает в себя достаточно большое количество положений, закрепленных в нормах международного права.

1.3. Место института персональных данных в системе права РФ

Система права — совокупность правовых форм, внутренне упорядоченная по отношениям, обеспечивающим относительную самостоятельность и единство этой совокупности, которое выражается в ее интегральных, обеспечительных и координационных свойствах и функциях. Это определение, сформулированное А. Б. Ипатовым, охватывает существенные признаки как системы права, так и ее подсистем: отраслей, подотраслей, институтов[1].

Структурными элементами системы права (подсистемами) являются: отрасль, подотрасль, институт, субинститут и норма права.

Вопрос о том, какое место в системе права занимает институт персональных данных, является на сегодняшний день наименее изученным. Несмотря на важность данного института с практической точки зрения, сегодняшняя юридическая наука почти не имеет работ, посвященных его изучению.

Одна из возможных причин — то, что, во-первых, защита персональных данных многими понимается, скорее, как чисто техническая задача — защита от утечки, защита от несанкционированного доступа, от хищения и т.д. При таком понимании происходит смещение акцентов в техническую область. Между тем защита персональных данных — это защита субъекта данных, т.е. того лица, которое предоставляет свои персональные данные государственному органу либо частной организации, защита его прав.

Другой возможной причиной является то, что нормы, регулирующие обработку персональных данных, принято считать частью института неприкосновенности частной жизни.

---

[1] *Ипатов А. Б.* К вопросу о месте страхового права в системе права // Юрист. 2005. № 7.

Одна из основных идей, которая имеет место во многих исследовательских работах, такова: права субъекта персональных данных — это юридическая конструкция, производная от прав человека, сконцентрированная в источниках международного права.

Необходимо различать два понятия — персональные данные и тайну частной жизни. Тайна частной жизни (личная и семейная тайна) — достаточно широкое понятие, не получившее точного нормативного закрепления и в ряде случаев охватывающее персональные данные. Тем не менее отдельно взятые факты о лице, такие как фамилия, имя, отчество, место работы, адрес и т.п., а также сведения о большинстве повседневных событий, связанных с этим лицом, не всегда могут считаться тайной, поскольку по своему характеру эти сведения являются общедоступными и могут быть непроизвольно получены любым случайным лицом.

В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер[1]. В противовес этому, персональные данные, как правило, являются своего рода идентификатором субъекта в человеческом обществе.

Институт тайны частной жизни защищает от умышленного вмешательства в личную жизнь, которое, как правило, выражается в нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, о чем прямо указано в Конституции РФ (ст. 23). Термин «персональные данные», в свою очередь, тесно связан с понятием «обработка». Обработка персональных данных начинается тогда, когда гражданин «свободно, своей волей и в своем интересе» (на что прямо указано в ч. 1 ст. 9 Федерального закона «О персональных данных») передает свои данные оператору для выполнения каких-либо функций (например, заключения трудового договора) или делает их общедоступными (например, регистрируясь в социальных сетях).

В ст. 5 Федерального закона «О персональных данных» указано, что целью данного закона является обеспечение за-

[1] *Определение* Конституционного Суда РФ от 9 июня 2005 г. № 248-О.

щиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Исходя из формулировки следует, что институт частной жизни является составной частью института персональных данных, причем тоже в некоторой его части.

Таким образом, необходимо отграничивать институт персональных данных от института неприкосновенности частной жизни.

В теории права не сложилось однозначного подхода к определению критериев выделения структурных элементов системы права. В данном вопросе можно согласиться с теми авторами, которые допускают выделение наряду с главными основаниями деления (предмет и метод регулирования) еще и дополнительные (отраслевые принципы, функции регулирования и др.). Этот подход учитывает объективность влияния на систему права общественных отношений, от которых право, как средство социального регулирования, не может не зависеть.

К признакам института права С. С. Алексеев относит самостоятельность регулятивного воздействия на определенные общественные отношения; юридическую однородность норм, выраженную в специфической группе понятий, общих положений, терминов; своеобразие юридической конструкции, которое выражается в следующем: наличие комплекса «равноправных» нормативных предписаний, юридическая разнородность предписаний, наличие устойчивых закономерных связей, создающих из отдельных предписаний специфическую юридическую конструкцию.

Е. А. Киримова называет следующие признаки правового института как структурного элемента системы права: относительная самостоятельность; специфичность способа правового регулирования; наличие или принципиальная возможность формирования общих понятий в рамках видовых явлений.

Опираясь на теорию права, можно провести анализ института персональных данных.

Так, предметом указанного института являются общественные отношения, связанные с обработкой персональных данных, осуществляемой государственными и муниципальными органами, юридическими и физическими лицами с использованием

средств автоматизации (средств вычислительной техники), в том числе в информационно-телекоммуникационных сетях, или без использования средств автоматизации, а также с их защитой от неправомерного доступа, уничтожения или блокирования (конфиденциальность, целостность и доступность информации).

Указанный институт содержит разветвленный понятийный аппарат. В частности, ст. 3 Федерального закона «О персональных данных» содержит такие дефиниции, как: «персональные данные», «оператор», «обработка персональных данных», «автоматизированная обработка персональных данных», «обезличивание персональных данных», «информационная система персональных данных», «трансграничная передача персональных данных» и т.п.

Кроме того, указанная сфера жизнедеятельности на сегодняшний день является относительно обособленной и имеет целый арсенал источников, содержащих в себе как нормы материального права (федеральные законы), так и нормы процессуального права (подзаконные нормативные акты), предписывающие процедуры, которые обязан провести оператор персональных данных для защиты обрабатываемой им информации.

Статья 5 Федерального закона «О персональных данных» содержит принципы и условия обработки персональных данных. Анализ указанных принципов и иных норм, содержащихся в указанном Федеральном законе и изданных в соответствии с ним подзаконных нормативных актах, позволяет сделать вывод, что для данного института характерен преимущественно императивный метод правового регулирования.

Таким образом, очевидно, что рассмотренная выше совокупность правовых норм, регулирующих общественные отношения, связанные с обработкой персональных данных и их защитой, имеет все присущие самостоятельному правовому институту отличительные черты.

Для определения места данного института в системе права Российской Федерации обратимся к классификации. Как известно, существует деление права на частное и публичное, материальное и процессуальное.

Проведенный выше анализ показывает, что институт персональных данных относится к публичной отрасли права. В то

же время нормы данного института находят свое отражение и в такой традиционно относимой к частному праву отрасли, как трудовое (гл. 14 ТК РФ), гражданское право (ст. 152.1 ГК РФ) и даже международное частное право (ст. 1198 ГК РФ).

Таким образом, указанный правовой институт регулирует общественные отношения, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому данный институт следует рассматривать как межотраслевой.

С практической точки зрения важность института персональных данных заключается в том, что:

во-первых, любое физическое лицо является носителем (субъектом) персональных данных, интересы которого связаны с тем, что «принадлежащие» ему персональные данные не должны распространяться произвольным образом и должна обеспечиваться их защита;

во-вторых, любое юридическое лицо с момента вступления в трудовые отношения хотя бы с одним работником или заказчиком становится оператором персональных данных, на которого возлагается обязанность по обеспечению конфиденциальности, целостности и доступности указанных данных, а также ответственность за нарушения законодательства о персональных данных.

Контрольные вопросы

1. В каких документах появилось первоначальное упоминание о тайне частной жизни?
2. Каким образом осуществлялась защита персональных данных в Советской России?
3. Когда и в каком нормативно-правовом акте впервые появился термин «персональные данные»?
4. В чем заключается основное различие между российским подходом к защите персональных данных и зарубежным?
5. В чем основной недостаток сформулированного в российском законодательстве понятия «персональные данные»?
6. Что представляет собой система законодательства о персональных данных? Из каких элементов она состоит? Какие элементы являются основными?

7. В чем различия между персональными данными и тайной частной жизни?

8. Какой метод регулирования является преобладающим по отношению к персональным данным?

Кейсы

Кейс 1. *Новый руководитель службы информационной безопасности*

Представьте, что вас только что наняли на работу руководителем службы информационной безопасности в организации: банк, образовательное учреждение, металлургический комбинат, торговая сеть, ресторан. Опираясь на сформулированное определение «персональные данные» и составляющие его элементы определите, какие категории персональных данных обрабатываются в каждой из указанных организаций.

Кейс 2. *Законодательство о персональных данных*

Банк обрабатывает персональные данные следующих категорий субъектов:

1) работник организации (включая сведения о судимости и портретные фотографии);

2) близкие родственники работника;

3) соискатели на замещение вакантных должностей;

4) участник (акционер) или работник юридического лица, являющийся аффилированным лицом по отношению к банку;

5) клиент (потребитель услуги), представитель клиента, выгодоприобретатель, бенефициарный владелец клиента — граждане РФ и иностранные граждане;

6) контрагент, представитель контрагента, бенефициарный владелец контрагента;

7) физическое лицо, входящее в органы управления банка.

Руководителем банка перед службой информационной безопасности поставлена задача подготовить служебную записку в формате one page only (не более одной страницы) с перечислением нормативно-правовых актов, которыми должен руководствоваться банк при обработке персональных данных.

2. Нормативно-правовое обеспечение защиты персональных данных

2.1. Общие условия обработки персональных данных

В соответствии со ст. 3 Федерального закона «О персональных данных» обработка персональных данных — это любое действие (операция) или совокупность действий (операций), совершаемых с использованием или без использования средств автоматизации, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Согласно ст. 5 Федерального закона «О персональных данных» при обработке персональных данных должны соблюдаться следующие принципы:

1) обработка должна осуществляться на законной и справедливой основе;

2) обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка, несовместимая с целями сбора персональных данных;

3) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4) обработке подлежат только те персональные данные, которые отвечают целям обработки;

5) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Не допускается обработка избыточных данных по отношению к заявленным целям обработки;

6) при обработке должны быть обеспечены точность и достаточность персональных данных, а в необходимых случаях — актуальность по отношению к целям обработки. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

7) форма хранения персональных данных должна позволять определять субъекта этих данных. Хранение не должно длиться дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

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

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться действующим законодательством;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения

персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством к специальным категориям персональных данных, за исключением случаев, предусмотренных федеральными законами;

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

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

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств;

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

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

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

Таким образом, общим правилом обработки персональных данных является наличие согласия субъекта персональных данных на их обработку, которое может быть дано самим субъектом или его представителем в любой позволяющей подтвердить факт его получения форме.

Поскольку в случае возникновения спора доказать получение согласия субъекта на обработку его персональных данных должен оператор (ч. 3 ст. 9 Федерального закона «О персональных данных»), целесообразно оформить такое согласие письменно. В некоторых случаях письменная форма согласия

прямо предусмотрена законом (ч. 4 ст. 9 Федерального закона «О персональных данных»). Например, письменное согласие работника на обработку его персональных данных требуется:

а) при получении персональных данных работника у третьей стороны (п. 3 ст. 86 ТК РФ);

б) при передаче персональных данных работника третьим лицам, кроме тех случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в иных предусмотренных федеральными законами случаях (абз. 2 ст. 88 ТК РФ);

в) для обработки специальных категорий персональных данных (п. 1 ч. 2 ст. 10 Федерального закона «О персональных данных»). К этим данным относятся сведения о расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни);

г) для обработки биометрических персональных данных (ч. 1 ст. 11 Федерального закона «О персональных данных»). К биометрическим относятся персональные данные, на основании которых можно установить личность субъекта и которые используются оператором для установления его личности.

При недееспособности субъекта письменное согласие на обработку его данных дает его законный представитель (родитель, опекун, попечитель и т.п.) (ч. 6 ст. 9 Федерального закона «О персональных данных»). А в случае смерти субъекта такое согласие оформляют его наследники, если только оно не было получено от него самого при жизни (ч. 7 ст. 9 Федерального закона «О персональных данных»).

Оператор, с согласия субъекта вправе поручить обработку его персональных данных другому лицу (ч. 3 ст. 6 Федерального закона «О персональных данных»). При этом ответственность перед субъектом за действия указанного лица несет оператор (ч. 5 ст. 6 Федерального закона «О персональных данных»). Например, в практической деятельности часто встречается ситуация, когда в группе компаний ведение кадрового учета осуществляется одним юридическим лицом для нескольких.

Письменное согласие субъекта на обработку персональных данных должно включать (ч. 4 ст. 9 Федерального закона «О персональных данных»):

1) фамилию, имя, отчество, адрес субъекта, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе;

2) при получении согласия от представителя субъекта — его фамилию, имя, отчество, адрес, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия представителя;

3) наименование или фамилию, имя, отчество и адрес оператора;

4) цель обработки персональных данных;

5) перечень персональных данных, которые подлежат обработке;

6) фамилию, имя, отчество и адрес лица или наименование организации, осуществляющих обработку персональных данных по поручению оператора, если она поручена такому лицу или организации;

7) перечень действий с персональными данными, на совершение которых дано согласие, общее описание способов их обработки;

8) срок, в течение которого действует согласие на обработку персональных данных, и способ отзыва согласия;

9) подпись субъекта.

Отсутствие хотя бы одного из указанных пунктов будет означать нарушение установленных законодательством требований к составу сведений, включаемых в согласие в письменной форме, и может повлечь административную ответственность (см. параграф 3.5).

Кроме того, действующее законодательство предусматривают 10 случаев, когда согласие на обработку персональных данных не требуется:

1) обработка необходима в целях исполнения заключенного с субъектом договора или возложенных на оператора обязанностей, функций и полномочий (ч. 1 ст. 6 Федерального закона «О персональных данных»);

2) обработка предусмотрена коллективным договором, соглашением, а также локальными актами работодателя, принятыми в установленном ст. 372 ТК РФ порядке (абз. 2 Разъяснений Роскомнадзора);

3) обязанность по обработке предусмотрена законодательством, в том числе для опубликования и размещения персональных данных работников (служащих) в Интернете (абз. 1 п. 1 Разъяснений Роскомнадзора). Например, медицинская организация обязана информировать граждан в доступной форме, в том числе с использованием Интернета, о своих медицинских работниках, уровне их образования, квалификации (п. 7 ч. 1 ст. 79 Федерального закона от 21 ноября 2011 г. № 323-ФЗ);

4) обработка специальных категорий персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством (п. 2.3 ч. 2 ст. 10 Федерального закона «О персональных данных»). Такая обработка допускается, например, в отношении сведений о состоянии здоровья педагогических работников (абз. 6 ч. 2 ст. 331 ТК РФ);

5) обработка персональных данных специальных категорий проводится органами прокуратуры при условии, что такие данные были получены в установленных законодательством РФ случаях (п. 7.1 ч. 2 ст. 10 Федерального закона «О персональных данных»);

6) обработка персональных данных близких родственников работника проводится в объеме, предусмотренном личной карточкой (форма № Т-2, утв. постановлением Госкомстата России от 5 января 2004 г. № 1), а также при получении алиментов, оформлении социальных выплат, допуска к государственной тайне и др. (абз. 1 п. 2 Разъяснений Роскомнадзора);

7) обработка персональных данных связана с выполнением работником своих трудовых обязанностей (п. 3 Разъяснений Роскомнадзора);

8) обработка персональных данных проводится в целях организации работодателем пропускного режима на территорию его служебных зданий и помещений (абз. 1 п. 5 Разъяснений Роскомнадзора);

9) персональные данные работника передаются третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных федеральными законами (абз. 2 ст. 88 ТК РФ);

10) обработка персональных данных осуществляется в отношении уволенных работников, например, в рамках бухгалтерского и налогового учета (подп. 5 п. 3 ст. 24 НК РФ, ст. 29 Федерального закона от 6 декабря 2011 г. № 402-ФЗ, абз. 6–10 п. 5 Разъяснений Роскомнадзора).

Кроме того, данное субъектом персональных данных согласие на их обработку не является необратимым. Оно может быть отозвано. При этом не нужно объяснять причины такого решения или выполнять какие-либо условия, необходимо только уведомить оператора персональных данных о принятом решении.

В подобной ситуации продолжение обработки персональных данных работника без его согласия возможно при наличии оснований, перечисленных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11 Федерального закона «О персональных данных».

К таким основаниям Федеральным законом «О персональных данных» относятся следующие:

• обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

• обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

• обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на Едином портале государственных и муниципальных услуг;

• обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому

субъект персональных данных будет являться выгодоприобретателем или поручителем;

• 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 осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

• обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

• обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

• обработка персональных данных, сделанных общедоступными субъектом персональных данных;

• обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка персональных данных может быть продолжена после отзыва согласия субъекта персональных данных, даже если речь идет о специальных категориях персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, в случаях, предусмотренных ч. 2 ст. 10 Федерального закона «О персональных данных».

К таким случаям законодатель относит следующие:

• персональные данные сделаны общедоступными субъектом персональных данных;

• обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

• обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»;

• обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

• обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

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

• обработка персональных данных 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 персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

• обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно в связи с осуществлением правосудия;

• обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном произ-

водстве, уголовно-исполнительным законодательством Российской Федерации;

• обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

• обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

2.2. Обязанности организации (оператора) в связи с обработкой персональных данных

В соответствии с ч. 1 ст. 22 Федерального закона «О персональных данных» оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор[1]) о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных в ч. 2 ст. 22 указанного Федерального закона.

В соответствии с ч. 2 ст. 22 Федерального закона «О персональных данных» оператор вправе осуществлять без уведомления Роскомнадзора обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

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

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых со-

[1] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

ответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

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

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

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

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

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

В указанных выше девяти случаях уведомлять уполномоченный орган об обработке персональных данных является правом, а не обязанностью оператора.

При этом следует отметить, что на практике часть юристов толкует данную норму следующим образом: обрабатываемые в указанных случаях персональные данные можно не включать в направляемое в Роскомнадзор уведомление об обработке персональных данных.

Проведенный анализ судебной практики свидетельствует о том, что данное толкование норм не является верным. Судебная практика показывает, что в случае, когда организация подает уведомление об обработке персональных данных в уполномоченный орган, она должна предоставлять полную информацию о себе как об операторе персональных данных.

Так, Арбитражный суд Новгородской области в решении по делу № А44-1867/2011 по спору между ЗАО «ИТС+» и Управлением Роскомнадзора по Новгородской области указал, что ЗАО «ИТС+» добровольно подавало в уполномоченный орган уведомление о намерении осуществить обработку персональных данных, а Управление Роскомнадзора обязано было проверить соответствие его содержания и правомерно отметило как нарушение отсутствие в уведомлении сведений о том, что организация обрабатывает персональные данные своих сотрудников и их близких родственников.

Арбитражный суд Астраханской области в решении по делу № А061975/2011 по спору между ИФНС по Ленинскому району г. Астрахани и Управлением Роскомнадзора по Астраханской области указал на то, что ИФНС, определив себя оператором персональных данных, при направлении уведомления об обработке персональных данных должна была заполнить уведомление в соответствии с утвержденными рекомендациями по его заполнению.

К аналогичным выводам пришел и Арбитражный суд Свердловской области в решении по делу № А60-41475/2011, разрешая спор между Территориальным фондом обязательного медицинского страхования Свердловской области и Управлением Роскомнадзора по Свердловской области.

Таким образом, арбитражные суды однозначно высказываются за то, что при направлении уведомления в Роскомнадзор оператор обязан указывать абсолютно все категории обрабатываемых им персональных данных.

Обработка персональных данных на практике осуществляется в трех формах: без использования средств автоматизации; с использованием средств автоматизации; смешанная, включающая в себя обе вышеназванные.

Согласно п. 3 ст. 4 Федерального закона «О персональных данных» порядок обработки персональных данных, осуществляемой без использования средств автоматизации, может

устанавливаться федеральными законами и иными нормативными правовыми актами РФ.

В настоящее время действует Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства РФ от 15 сентября 2008 г. № 687 (далее — Положение). Согласно данному Положению обработкой персональных данных без применения средств автоматизации считаются использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека (п. 1 Положения).

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

Пункт 7 Положения содержит условия, которые необходимо соблюдать при использовании типовых форм документов, предполагающих или допускающих включение в них персональных данных. Например, унифицированных форм первичной учетной документации по учету труда и его оплаты, утвержденных постановлением Госкомстата России от 5 января 2004 г. № 1.

Согласно подп. «а» п. 7 Положения, типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать: сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; фамилию, имя, отчество и адрес оператора; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения данных; сроки их обработки; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки персональных данных.

Типовая форма должна содержать поле, в котором субъект персональных данных может проставить отметку о согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, — при необходимости получения такого согласия (подп. «б» п. 7 Положения).

При этом форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими данными, не нарушая прав и законных интересов иных субъектов персональных данных (подп. «в» п. 7 Положения). Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы (подп. «г» п. 7 Положения).

Как правило, большая часть неавтоматизированной обработки персональных данных связана с ведением личных дел работников организации. При этом следует отметить, что согласно п. 7 ст. 86 ТК РФ защиту персональных данных работника от неправомерного их использования или утраты работодатель должен обеспечивать за счет своих средств. В соответствии со ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем. Из указанных норм следует, что работодатель должен издать соответствующий локальный нормативный акт, регулирующий вопросы хранения и использования персональных данных, а также обеспечивающий защиту последних от неправомерного их использования или утраты. С соответствующим актом, а также со своими правами в сфере защиты персональных данных работники должны быть ознакомлены под подпись.

Для защиты персональных данных от неправомерного использования работодатель обязан (ч. 1 ст. 88 ТК РФ):

а) осуществлять их передачу только в пределах одной организации;

б) регламентировать процедуру передачи персональных данных локальными нормативными актами (положение о персональных данных работников; утвержденный приказом список лиц, имеющих доступ к персональным данным; обязательство о неразглашении персональных данных);

в) ознакомить работников, которым открыт доступ к персональным данным других работников организации, с указанными локальными нормативными актами под подпись;

г) передавать персональные данные работников по мотивированному запросу только специально уполномоченным лицам, а также представителям работников, в том объеме, который необходим им для выполнения конкретных функций.

Исходя из требований п. 7 ст. 86 и ст. 87 ТК РФ на работодателя возложена обязанность по защите персональных данных работников.

Защита персональных данных включает в себя установление особого режима доступа в те помещения, где хранятся такие данные, направленного на защиту последних от несанкционированных доступа, изменений или распространения.

Действующим законодательством не предусмотрены конкретные требования к оборудованию помещения, где должны храниться персональные данные. Однако исходя из требований ТК РФ, во избежание несанкционированного доступа к персональным данным работников, следует оборудовать помещение, где хранятся такие данные, запирающимися шкафами для хранения информации на бумажных носителях. Работодатель должен установить в локальном нормативном акте требования к помещению, где хранятся персональные данные работников, и условия их хранения. Следует также учитывать, что персональные данные работника хранятся в документированной форме, характер которой определяется работодателем.

Согласно ст. 3 Федерального закона «О персональных данных» под автоматизированной обработкой понимается обработка данных с помощью средств вычислительной техники. Необходимо учитывать, что обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти данные содержались в информационной системе персональных данных либо были извлечены из нее (п. 2 Положения).

Обязанности оператора при автоматизированной обработке содержатся в гл. 4 Федерального закона «О персональных данных» и принятых во исполнение указанного федерального закона подзаконных актах (постановление Правительства РФ № 1119, приказы ФСТЭК России № 17 и 21).

В соответствии с требованиями данной главы оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных действую-

щим законодательством. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных действующему законодательству, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения действующего законодательства, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых мерах по защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информа-

ционно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых мерах по защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (разработка моделей угроз и нарушителей);

2) принятием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн), необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных (см. параграф 2.4);

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (см. параграф 2.5);

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию соответствующей информационной системы;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистра-

ции и учета всех действий, совершаемых с персональными данными в соответствующей информационной системе;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в ИСПДн.

Всего предусмотрено четыре уровня защищенности: наименьшее количество требований необходимо обеспечить для 4-го уровня; наибольшее количество — для 1-го уровня.

При смешанной обработке персональных данных оператор должен соблюдать все требования, предусмотренные как для неавтоматизированной, так и для автоматизированной обработки.

2.3. Особенности обработки в базах данных, находящихся на территории Российской Федерации, и трансграничной передачи персональных данных

Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» внесены изменения в ч. 4 ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии с которыми оператор информационной системы в случаях,

установленных законодательством РФ, обязан обеспечить нахождение на территории РФ баз данных информации, с использованием которых осуществляется сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ.

Действующим законодательством (ч. 5 ст. 18 Федерального закона «О персональных данных») установлена обязанность оператора персональных данных при их сборе, в том числе посредством информационно-телекоммуникационной сети Интернет, обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных ст. 6 названного Федерального закона, а именно:

• обработка персональных данных необходима для достижения целей, предусмотренных международным договором или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

• обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

• обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов РФ, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

• обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельно-

сти при условии, что при этом не нарушаются права и законные интересы субъекта.

В перечисленных выше случаях, исходя из буквального толкования норм действующего законодательства, обязанность по использованию баз данных, находящихся исключительно на территории Российской Федерации, на оператора не возлагается.

Таким образом, можно сделать вывод, что для исполнения возложенной на оператора ч. 5 ст. 18 Федерального закона «О персональных данных» обязанности необходимо обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ, исключительно в процессе сбора, т.е. при получении оператором персональных данных для их последующей обработки в соответствии с заявленными целями сбора.

Кроме того, Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» внесены изменения в ч. 3 ст. 22 Федерального закона «О персональных данных», возлагающие на оператора обязанность указать в уведомлении об обработке персональных данных сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации, в случае, когда предоставление уведомления является обязательным.

Непредоставление указанных сведений в уведомлении, равно как и непредоставление самого уведомления влечет административную ответственность по ст. 19.7 КоАП РФ в виде административного штрафа, максимальный размер которого составляет 5 000 р.

Трансграничная передача персональных данных должна осуществляться преимущественно в иностранные государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов.

Трансграничная передача персональных данных на территории иностранных государств, не присоединившихся

к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (не обеспечивающих адекватной защиты прав субъектов), может осуществляться в исключительных случаях, с обязательным соблюдением одного из следующих условий (ч. 4 ст. 12 Федерального закона «О персональных данных»):

• наличие письменного согласия субъекта персональных данных на трансграничную передачу;

• исполнение договора, стороной которого является субъект персональных данных;

• защита жизни, здоровья, иных жизненно важных интересов субъекта или других лиц при невозможности получения согласия в письменной форме.

В целях исполнения возложенных на оператора ч. 3 ст. 12 Федерального закона «О персональных данных» обязанностей рекомендуется предусмотреть в локальных нормативных актах оператора следующий порядок: перед началом трансграничной передачи персональных данных работник оператора, ответственный за организацию обработки персональных данных, проверяет, входит ли иностранное государство в Перечень стран, присоединившихся к Конвенции о защите физических лиц в отношении автоматизированной обработки данных личного характера CETS № 108 (ссылка публикуется на официальном сайте Роскомнадзора) или утвержденный перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных (утверждается приказом Роскомнадзора).

Указанный порядок рекомендуется применять также в случаях заключения договоров на оказание услуг по предоставлению находящихся на территории иностранных государств вычислительных мощностей в целях обработки и хранения информации потребителя услуг с использованием технических средств, взаимодействующих через информационно-телекоммуникационную сеть (так называемых облачных сервисов).

2.4. Построение системы защиты персональных данных в организации

Защита персональных данных представляет собой регламентированный бизнес-процесс[1], предупреждающий нарушение установленного порядка доступности, целостности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании.

Для обеспечения внешней (физической) защиты персональных данных оператор обязан принять следующие меры:

- установить пропускной режим и особый порядок приема, учета и контроля деятельности посетителей;
- установить особый порядок выдачи пропусков и удостоверений работников;
- использовать технические средства охраны;
- использовать программно-технический комплекс защиты информации на электронных носителях и т.п.

Для обеспечения внутренней (организационной) защиты персональных данных оператор обязан предпринять следующее:

- ограничить и регламентировать состав работников, функциональные обязанности которых требуют доступа к персональным данным;
- избирательно и обоснованно распределить документы и информацию, содержащую персональные данные, между лицами, уполномоченными на работу с такими данными;
- рационально размещать рабочие места для исключения бесконтрольного использования защищаемой информации;
- регулярно проверять знание работниками, имеющими отношение к работе с персональными данными, требований нормативно-методических документов по защите таких данных;
- создавать необходимые условия для работы с документами и базами данных, содержащими персональные данные;

[1] Совокупная последовательность действий по преобразованию ресурсов, полученных на входе, в конечный продукт, имеющий ценность для потребителя (в том числе и внутреннего), на выходе.

• определять состав работников, имеющих право доступа (входа) в помещения, в которых хранятся персональные данные;

• организовать порядок уничтожения информации;

• своевременно выявлять и устранять нарушения установленных требований по защите персональных данных;

• проводить профилактическую работу с должностными лицами, имеющими доступ к персональным данным работников, по предупреждению разглашения таких сведений.

В настоящее время преимущественное большинство организаций использует электронные системы хранения и обработки персональных данных.

При обработке таких данных работодатель должен обеспечить их защиту в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119 (далее — Требования) (п. 3 Требований, п. 2 ст. 3 Федерального закона «О персональных данных»). Для этого первоначально необходимо провести оценку уровня защищенности принадлежащих ему информационных систем персональных данных:

1) определить тип ИСПДн в зависимости от категории обрабатываемых персональных данных (табл. 1);

2) определить, обрабатываются в ИСПДн персональные данные только сотрудников оператора или же в ней обрабатываются персональные данные лиц, не работающих в организации;

3) определить количество субъектов, данные которых обрабатываются в ИСПДн (более или менее 100 000);

4) определить тип актуальных угроз безопасности персональных данных.

Существует три типа угроз, которые создают актуальную опасность несанкционированного доступа к персональным данным при их обработке в ИСПДн (табл. 2).

Согласно п. 7 Требований, оператор определяет актуальность угроз безопасности персональных данных самостоятельно, на основании разработанной модели угроз.

Для ИСПДн устанавливаются четыре уровня защищенности персональных данных. Оператор определяет уровень защищенности и документально фиксирует его.

Таблица 1

Типы ИСПДн в зависимости от категории обрабатываемых персональных данных

Тип ИСПДн	Категория персональных данных	Описание
ИСПДн-С	В ИСПДн обрабатываются специальные категории персональных данных	Данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни
ИСПДн-Б	В ИСПДн обрабатываются биометрические персональные данные и не обрабатываются специальные категории персональных данных	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта
ИСПДн-О	В ИСПДн обрабатываются общедоступные персональные данные	Персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со ст. 8 Федерального закона «О персональных данных»
ИСПДн-И	В ИСПДн обрабатываются иные категории персональных данных	Персональные данные, не относящиеся к специальным категориям персональных данных, не являющиеся биометрическими или общедоступными

Таблица 2

Типы актуальных угроз для ИСПДн

Тип угроз	Описание
1	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИСПДн
2	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн
3	Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн

После определения уровня защищенности необходимо реализовать комплекс правовых, организационных и технических мер, предусмотренных для данного целевого уровня (табл. 3).

Таблица 3

Меры для обеспечения уровня защищенности

Принимаемые меры	Уровень защищенности персональных данных			
	4	3	2	1
Организация режима обеспечения безопасности помещений	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Утверждение перечня лиц, имеющих доступ к обрабатываемым персональным данным	+	+	+	+
Использование сертифицированных средств защиты информации	+	+	+	+
Назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИСПДн		+	+	+
Обеспечение доступа к электронным журналам только для работников оператора			+	+
Регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным				+
Создание либо возложение на одно из структурных подразделений функций по обеспечению безопасности персональных данных				+

Кроме того, необходимо определить состав и содержание организационных и технических мер по обеспечению безопасности персональных данных для выполнения требований согласно приказу ФСТЭК России № 21. Если обработка производится в государственных или муниципальных информационных системах, провести уточнение перечня мер согласно приказу ФСТЭК России № 17. Если для обеспечения безопасности персональных данных используются средства криптографической защиты информации, уточнить состав и содержание организационных и технических мер согласно приказу ФСБ России от 10 июля 2014 г. № 378.

Как правило, большинство информационных систем персональных данных, принадлежащих организации, имеют четвертый уровень защищенности. Для его обеспечения необходимо:

• обезопасить от неконтролируемого проникновения помещения, в которых размещена информационная система;

• обеспечить сохранность носителей персональных данных;

• издать приказ (распоряжение) в произвольной форме с перечнем работников, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе;

• защитить информацию с помощью средств, прошедших процедуру оценки соответствия (средства защиты должны иметь сертификаты ФСТЭК России, либо ФСБ России, если используются криптографические средства защиты информации).

2.5. Особенности применения средств защиты информации в информационных системах персональных данных

В соответствии с подп. «г» п. 13 постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн всех уровней защищенности обязательным является требование по использованию средств защиты информации, прошедших оценку соответствия требованиям законодательства РФ в области обеспечения безопасности, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Иными словами, если для информационной системы персональных данных существует актуальная угроза (например, воздействие вредоносного программного обеспечения), то для ее нейтрализации необходимо применение средства защиты информации (в указанном примере — антивирусного программного средства), прошедшего процедуру оценки соответствия требованиям законодательства РФ.

В соответствии с ч. 1 и 4 ст. 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» в отношении продукции, используемой в целях защиты охраняемой в соответствии с законодательством РФ информации ограниченного доступа, особенности оценки соответствия устанавливаются Правительством РФ или органом исполнительной власти, уполномоченным в области противодействия тех-

ническим разведкам и технической защиты информации (ФСТЭК России).

Постановлением Правительства РФ от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения» предусмотрено, что оценка соответствия средств, предназначенных для защиты информации конфиденциального характера, средств, в которых они реализованы, а также средств контроля эффективности защиты информации, используемых в целях защиты государственного информационного ресурса и (или) персональных данных, осуществляется в форме обязательной сертификации.

Таким образом, средства защиты персональных данных подлежат оценке соответствия в форме обязательной сертификации.

Изложенной позиции придерживается ФСТЭК России в своих разъяснительных документах:

1) информационное сообщение ФСТЭК России от 4 мая 2012 г. № 240/24/1701 «О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа»;

2) информационное сообщение ФСТЭК России от 24 марта 2017 г. № 240/24/1382 «По вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации».

Во избежание возможных штрафов и санкций со стороны регуляторов (ФСТЭК России, ФСБ России, Роскомнадзор) оператору персональных данных рекомендуется использовать средства защиты персональных данных, в том числе антивирусные программные средства, межсетевые экраны, а также средства анализа защищенности, сертифицированные на соот-

ветствие обязательным требованиям по безопасности информации.

Нарушение установленных законодательством РФ требований по защите информации влечет ответственность. Формы возможной ответственности за нарушение требований законодательства РФ в области защиты персональных данных рассмотрены в главе 3.

Контрольные вопросы

1. Что представляет собой «обработка персональных данных»?
2. Перечислите и охарактеризуйте принципы обработки персональных данных.
3. Какие дополнительные обязанности по обработке персональных данных накладывает Трудовой кодекс РФ?
4. Перечислите случаи, в которых письменное согласие субъекта персональных данных является обязательным.
5. Перечислите обязательные элементы письменного согласия субъекта персональных данных.
6. Перечислите случаи, когда не требуется получать письменное согласие субъекта персональных данных.
7. Перечислите случаи, в которых возможна обработка персональных данных после отзыва согласия субъекта (включая специальные категории и биометрические категории).
8. В каких случаях оператор может осуществлять обработку персональных данных без уведомления об этом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)?
9. Перечислите и охарактеризуйте формы обработки персональных данных.
10. Какие требования предъявляются к типовым формам или связанным с ними документам (инструкция по заполнению, карточки, реестры и журналы), содержащим персональные данные?
11. Перечислите основные меры обеспечения безопасности персональных данных при автоматизированной обработке.

12. Какие требования предъявляются к политике оператора в области персональных данных?

13. В каких случаях персональные данные должны обрабатываться только в базах данных, находящихся на территории Российской Федерации?

14. Какие требования предъявляются для трансграничной передачи персональных данных?

15. Перечислите меры физической безопасности, которые должен обеспечить оператор персональных данных.

16. Перечислите организационные меры обеспечения безопасности персональных данных.

17. Перечислите типы информационных систем персональных данных. Какие критерии влияют на уровень защищенности информационной системы персональных данных?

18. Перечислите и охарактеризуйте основные требования, которые необходимо выполнить для обеспечения четвертого уровня защищенности.

19. Соблюдение каких обязательных требований необходимо в случае применения средств защиты информации в информационных системах персональных данных?

Кейсы

Кейс 1. *Подготовка уведомления в Роскомнадзор*

Банк обрабатывает персональные данные следующих категорий субъектов:

1) работники организации (включая сведения о судимости и портретные фотографии);

2) близкие родственники работника;

3) соискатели на замещение вакантных должностей;

4) участник (акционер) или работник юридического лица, являющийся аффилированным лицом по отношению к банку;

5) клиент (потребитель услуги), представитель клиента, выгодоприобретатель, бенефициарный владелец клиента — граждане РФ и иностранные граждане;

6) контрагент, представитель контрагента, бенефициарный владелец контрагента;

7) физическое лицо, входящее в органы управления банка.

Перед вами как специалистом по защите информации стоит задача подготовить уведомление в Роскомнадзор о намерении осуществлять обработку персональных данных. К подготовленному вами проекту уведомления юристом компании было вынесено замечание — исключить из него основания обработки и категории персональных данных, связанные с работниками организации. Каковы будут ваши действия?

Кейс 2. *Кадровый учет в компании*

Численный состав работников ООО «У» насчитывает около 50 чел. Поскольку штат небольшой, персональные данные работников обрабатываются исключительно на бумажных носителях информации и не заносятся ни в какую информационную систему.

При этом отличительным свойством кадровой политики организации является текучесть персонала, которая не является исключением и для отдела кадров.

Исходя из текущей ситуации подготовьте перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ в соответствии с требованиями п. 13 постановления Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Кейс 3. *Внедрение Microsoft Office 365*

Руководством международной компании, имеющей представительство в Российской Федерации, было принято решение о внедрении облачного сервиса Microsoft Office 365.

Технические средства сервиса Microsoft Office 365 находятся за рубежом (за пределами территории РФ), при этом компания планирует при помощи Microsoft Office 365 осуществлять обработку персональных данных работников — граждан Российской Федерации.

Предложите решение по организации обработки персональных данных работников в облачном сервисе Microsoft Office 365, соответствующее нормам действующего законодательства РФ.

Кейс 4. *Уровень защищенности информационной системы персональных данных*

Опираясь на изложенный в главе материал, определите уровень защищенности информационной системы персональных данных для следующих организаций:

1) банк;

2) медицинская организация;

3) торговая сеть.

Для определения категорий персональных данных, обрабатываемых в организации, воспользуйтесь реестром операторов, осуществляющих обработку персональных данных (https://pd.rkn.gov.ru/operators-registry/operators-list).

По итогам работы подготовьте проект акта определения уровня защищенности.

3. Контроль и надзор за обработкой персональных данных. Ответственность за нарушения действующего законодательства

3.1. Органы, осуществляющие контроль и надзор за операторами персональных данных

Вопросам контроля и надзора за обработкой персональных данных и ответственности за нарушение действующего законодательства в указанной сфере посвящена гл. 5 Федерального закона «О персональных данных».

В соответствии со ст. 23 указанного Федерального закона уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, т.е. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Российской Федерации.

Уполномоченный орган по защите прав субъектов персональных данных в рамках контрольно-надзорной деятельности имеет право:

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

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

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

• ограничивать доступ к информации, обрабатываемой с нарушением законодательства РФ в области персональных данных, в порядке, установленном законодательством РФ;

• принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

• обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

• направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (ФСБ России), и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), применительно к сфере их деятельности, сведения о принимаемых оператором мерах по защите информации и о наличии у него шифровальных (криптографических) средств;

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

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

• привлекать к административной ответственности лиц, виновных в нарушении Федерального закона «О персональных данных».

Таким образом, основным органом, осуществляющим проверку операторов персональных данных, является Роскомнадзор в лице его территориальных органов (например, Управление Роскомнадзора по Свердловской области). Однако следует отметить, что в соответствии с ч. 8 ст. 19 Федерального закона «О персональных данных» контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в государственных ИСПДн осуществляются ФСБ России и ФСТЭК России в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

Иными словами, функции по контролю за соблюдением оператором государственных информационных систем организационных и технических мер по защите персональных данных возложены также на ФСТЭК России и ФСБ России (функции последней ограничены порядком использования средств криптографической защиты информации).

В соответствии с п. 1 ч. 1 ст. 13 и ч. 1 ст. 14 Федерального закона «Об информации, информационных технологиях и о защите информации» государственные информационные системы — это федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ, на основании правовых актов государственных органов. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Указанные нормы на практике толкуются следующим образом: если в государственной организации (учреждении, органе) имеется информационная система, о введении в эксплуатацию которой принят локальный нормативный акт (приказ, распоряжение), либо информационная система создана в соответствии с каким-либо законом или подзаконным нормативно-правовым актом, то она считается государственной информа-

ционной системой и оператор становится поднадзорным регуляторам в лице ФСТЭК России и ФСБ России.

Например, если в Министерстве образования РФ есть «1С:Зарплата и кадры», где ведется обработка персональных данных сотрудников данного министерства, то указанная информационная система является государственной. Соответственно, проводить контрольные мероприятия могут ФСТЭК России и ФСБ России (если для защиты персональных данных используются криптографические средства).

Сложившееся в практике толкование норм ст. 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» является неверным, так как в них содержится два обязательных условия, только одновременное выполнение которых позволяет считать информационную систему государственной:

1) информационная система должна быть создана на основании федерального закона (в законе должно быть прямо указано на это), либо закона субъекта РФ, либо на основании правового акта государственного органа (речь идет о правовом акте, прошедшем регистрацию в Министерстве юстиции РФ);

2) информационная система должна быть создана в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами либо в иных установленных федеральными законами целях. Это означает, что информационная система должна быть предназначена для выполнения каких-либо публично-правовых функций.

Еще одним регулятором наряду с Роскомнадзором, ФСТЭК России и ФСБ России является Прокуратура РФ, которая в силу возложенных на нее Законом РФ от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» полномочий вправе проводить проверку соблюдения государственными органами, учреждениями и (или) юридическими лицами требований действующего законодательства РФ (в том числе законодательства о персональных данных).

В части персональных данных работников организации в качестве регулятора выступает также Государственная инспекция труда. Это следует из ст. 353 ТК РФ.

Таким образом, предмет контроля и надзора за организацией в части соблюдения ею требований законодательства о персональных данных со стороны Роскомнадзора и Государ-

ственной инспекции труда совпадает. Последняя свою контрольно-надзорную функцию реализует также посредством проверок, обследований и подготовки материалов о привлечении виновных лиц к ответственности. В соответствии с подп. 16 ч. 2 ст. 28.3 КоАП РФ ревизоры Роструда вправе в пределах своих полномочий составлять протоколы об административных правонарушениях, в том числе предусмотренных ч. 2 ст. 5.27 КоАП РФ, поэтому на практике нередко Роскомнадзором и Государственной инспекцией труда проводятся совместные проверки.

3.2. Особенности проведения контрольно-надзорных мероприятий

Порядок организации и проведения проверок юридических лиц, индивидуальных предпринимателей органами, уполномоченными на осуществление государственного контроля (надзора), муниципального контроля, порядок взаимодействия этих органов, их права и обязанности, а также права и обязанности юридических лиц, индивидуальных предпринимателей при осуществлении государственного контроля (надзора), меры по защите их прав и законных интересов регламентируются Федеральным законом от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее — Федеральный закон «О защите прав юридических лиц»).

Указанный Федеральный закон предусматривает следующие две группы проверок: плановая и внеплановая; документарная и выездная.

В соответствии со ст. 9 Федерального закона «О защите прав юридических лиц» предметом плановой проверки является соблюдение юридическим лицом, индивидуальным предпринимателем в процессе осуществления деятельности совокупности предъявляемых обязательных требований и требований, установленных муниципальными правовыми актами, а также соответствие сведений, содержащихся в уведомлении о начале осуществления отдельных видов предпринимательской деятель-

ности (например, уведомление об обработке персональных данных), обязательным требованиям. Плановые проверки проводятся не чаще чем один раз в три года. Плановые проверки проводятся на основании разрабатываемых органами государственного контроля (надзора), органами муниципального контроля в соответствии с их полномочиями ежегодных планов (например, план проверок Управления Роскомнадзора по Свердловской области на 2018 г.). Утвержденный руководителем органа государственного контроля (надзора) или органа муниципального контроля ежегодный план проведения плановых проверок доводится до сведения заинтересованных лиц посредством его размещения на официальном сайте соответствующего органа в сети Интернет либо иным доступным способом.

В соответствии со ст. 10 Федерального закона «О защите прав юридических лиц» предметом внеплановой проверки является соблюдение юридическим лицом, индивидуальным предпринимателем в процессе осуществления деятельности обязательных требований и требований, установленных муниципальными правовыми актами, выполнение предписаний органов государственного контроля (надзора), органов муниципального контроля, проведение мероприятий по предотвращению причинения вреда жизни, здоровью граждан, вреда животным, растениям, окружающей среде, по обеспечению безопасности государства, по предупреждению возникновения чрезвычайных ситуаций природного и техногенного характера, по ликвидации последствий причинения такого вреда.

Основаниями для проведения внеплановой проверки являются:

1) истечение срока исполнения юридическим лицом, индивидуальным предпринимателем ранее выданного предписания об устранении выявленного нарушения обязательных требований и (или) требований, установленных муниципальными правовыми актами;

2) поступление в органы государственного контроля (надзора), органы муниципального контроля обращений и заявлений граждан, в том числе индивидуальных предпринимателей, юридических лиц, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

а) возникновение угрозы причинения вреда жизни, здоровью граждан, вреда животным, растениям, окружающей среде, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации, безопасности государства, а также угрозы чрезвычайных ситуаций природного и техногенного характера;

б) причинение вреда жизни, здоровью граждан, вреда животным, растениям, окружающей среде, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации, безопасности государства, а также возникновение чрезвычайных ситуаций природного и техногенного характера;

в) нарушение прав потребителей (в случае обращения граждан, права которых нарушены);

3) приказ (распоряжение) руководителя органа государственного контроля (надзора), изданный в соответствии с поручениями Президента РФ, Правительства РФ и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

В соответствии со ст. 11 и 12 Федерального закона «О защите прав юридических лиц» плановая и внеплановая проверки проводятся в форме документарной и (или) выездной проверки.

В соответствии с ч. 4 ст. 1 Федерального закона «О защите прав юридических лиц» особенности организации и проведения проверок в части, касающейся вида, предмета, оснований проведения проверок, сроков и периодичности их проведения, уведомлений о проведении внеплановых выездных проверок и согласования проведения внеплановых выездных проверок с органами прокуратуры, могут устанавливаться другими федеральными законами при осуществлении следующих видов государственного контроля (надзора): федеральный государственный надзор в области связи; федеральный государственный надзор за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права.

В соответствии со ст. 11 Федерального закона «О защите прав юридических лиц» предметом документарной проверки являются сведения, содержащиеся в документах юридического

лица, индивидуального предпринимателя, устанавливающих их организационно-правовую форму, права и обязанности, документы, используемые при осуществлении их деятельности и связанные с исполнением ими обязательных требований и требований, установленных муниципальными правовыми актами, с исполнением предписаний и постановлений органов государственного контроля (надзора), органов муниципального контроля.

В процессе проведения документарной проверки должностными лицами органа государственного контроля (надзора) в первую очередь рассматриваются документы юридического лица, индивидуального предпринимателя, имеющиеся в распоряжении органа государственного контроля (надзора), в том числе уведомления о начале осуществления отдельных видов предпринимательской деятельности, акты предыдущих проверок, материалы рассмотрения дел об административных правонарушениях и иные документы о результатах осуществленных в отношении этого юридического лица, индивидуального предпринимателя государственного контроля (надзора), муниципального контроля.

В том случае, если в ходе документарной проверки выявлены ошибки и (или) противоречия в представленных юридическим лицом, индивидуальным предпринимателем документах либо несоответствие сведений, содержащихся в этих документах, сведениям, содержащимся в документах, имеющихся у органа государственного контроля (надзора), и (или) полученным в ходе осуществления государственного контроля (надзора), информация об этом направляется юридическому лицу, индивидуальному предпринимателю с требованием представить в течение 10 рабочих дней необходимые пояснения в письменной форме.

Юридическое лицо, индивидуальный предприниматель, представляющие в орган государственного контроля (надзора), орган муниципального контроля пояснения относительно выявленных ошибок и (или) противоречий в представленных документах либо относительно несоответствия указанных сведений, вправе представить дополнительно в орган государственного контроля (надзора), орган муниципального контроля документы, подтверждающие достоверность ранее представленных документов.

При проведении документарной проверки орган государственного контроля (надзора), орган муниципального контроля не вправе требовать у юридического лица, индивидуального предпринимателя сведения и документы, не относящиеся к предмету документарной проверки, а также сведения и документы, которые могут быть получены этим органом от иных органов государственного контроля (надзора), органов муниципального контроля.

В соответствии со ст. 12 Федерального закона «О защите прав юридических лиц» предметом выездной проверки являются содержащиеся в документах юридического лица, индивидуального предпринимателя сведения, а также соответствие их работников, состояние используемых указанными лицами при осуществлении деятельности территорий, зданий, строений, сооружений, помещений, оборудования, подобных объектов, транспортных средств, производимые и реализуемые юридическим лицом, индивидуальным предпринимателем товары (выполняемая работа, предоставляемые услуги) и принимаемые ими меры по исполнению обязательных требований и требований, установленных муниципальными правовыми актами.

Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения юридического лица, месту осуществления деятельности индивидуального предпринимателя и (или) по месту фактического осуществления их деятельности.

Выездная проверка проводится в случае, если при документарной проверке не представляется возможным:

1) удостовериться в полноте и достоверности сведений, содержащихся в уведомлении о начале осуществления отдельных видов предпринимательской деятельности и иных имеющихся в распоряжении органа государственного контроля (надзора) документах юридического лица, индивидуального предпринимателя;

2) оценить соответствие деятельности юридического лица, индивидуального предпринимателя обязательным требованиям или требованиям, установленным муниципальными правовыми актами, без проведения соответствующего мероприятия по контролю.

Руководитель, иное должностное лицо или уполномоченный представитель юридического лица обязаны предоставить должностным лицам органа государственного контроля (надзора), органа муниципального контроля, проводящим выездную проверку, возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ проводящих выездную проверку должностных лиц и участвующих в выездной проверке экспертов, представителей экспертных организаций на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения, к используемым оборудованию, подобным объектам, транспортным средствам и перевозимым ими грузам.

Органы государственного контроля (надзора) могут привлекать к проведению выездной проверки экспертов, экспертные организации, не состоящие в гражданско-правовых и трудовых отношениях с юридическим лицом, индивидуальным предпринимателем, в отношении которых проводится проверка, и не являющиеся аффилированными лицами проверяемых лиц.

Срок проведения каждой из проверок не может превышать 20 рабочих дней.

В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц органа государственного контроля (надзора), органа муниципального контроля, проводящих выездную плановую проверку, срок проведения выездной плановой проверки может быть продлен, но не более чем на 20 рабочих дней.

По результатам проверки должностными лицами органа государственного контроля (надзора), органа муниципального контроля, проводящими проверку, составляется акт по установленной форме в двух экземплярах.

К акту проверки прилагаются протоколы объяснения работников, на которых возлагается ответственность за нарушение обязательных требований или требований, установленных муниципальными правовыми актами, предписания об устра-

нении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

Акт проверки оформляется непосредственно после ее завершения в двух экземплярах, один из которых с копиями приложений вручается руководителю, иному должностному лицу или уполномоченному представителю юридического лица, индивидуальному предпринимателю, его уполномоченному представителю под расписку об ознакомлении либо об отказе в ознакомлении с актом проверки.

Юридическое лицо, индивидуальный предприниматель, проверка которых проводилась, в случае несогласия с фактами, выводами, предложениями, изложенными в акте проверки, либо с выданным предписанием об устранении выявленных нарушений в течение 15 дней с даты получения акта проверки вправе представить в соответствующие орган государственного контроля (надзора), орган муниципального контроля в письменной форме возражения в отношении акта проверки и (или) выданного предписания об устранении выявленных нарушений в целом или его отдельных положений. При этом юридическое лицо, индивидуальный предприниматель вправе приложить к таким возражениям документы, подтверждающие обоснованность возражений, или их заверенные копии либо в согласованный срок передать их в орган государственного контроля (надзора).

В случае выявления при проведении проверки нарушений обязательных требований или требований, установленных муниципальными правовыми актами, должностные лица органа государственного контроля (надзора), органа муниципального контроля, проводившие проверку, в пределах полномочий, предусмотренных законодательством РФ, обязаны:

1) выдать предписание об устранении выявленных нарушений с указанием сроков их устранения;

2) принять меры по контролю за устранением выявленных нарушений, их предупреждению, а также меры по привлечению лиц, допустивших выявленные нарушения, к ответственности.

Следует отметить, что Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-

телекоммуникационных сетях» внесены изменения в ч. 3.1 ст. 1 Федерального закона «О защите прав юридических лиц», в соответствии с которыми положения данного Федерального закона, устанавливающие порядок организации и проведения проверок, не применяются при осуществлении контроля и надзора за обработкой персональных данных. Данные изменения вступили в силу с 1 сентября 2015 г.

Внесение указанной нормы означает существенное расширение возможности регуляторов в рамках проверок деятельности операторов на предмет ее соответствия требованиям законодательства о персональных данных. Такие проверки выведены из-под действия Федерального закона «О защите прав юридических лиц». Это, в частности, означает отсутствие ограничений на проведение внеплановых проверок.

При выявлении в ходе государственного контроля нарушений действующего законодательства оператор может быть подвергнут административному штрафу.

3.3. Подготовка оператора к плановой проверке

Планы проверок практически всех организаций публикуются на официальном сайте Генеральной прокуратуры РФ в начале года. На нем любая организация-оператор по ИНН или ОГРН может узнать о предстоящих в текущем году проверках, их длительности и периоде проведения. Кроме того, регуляторы обязаны осуществлять размещение планов своих контрольно-надзорных мероприятий на официальных сайтах.

Непосредственно процесс подготовки оператора к плановой проверке может включать в себя следующие этапы.

Этап 1. Сбор информации (бенчмаркинг). Анализ опыта организаций, проходивших проверку в прошедшем году (либо в текущем, если проверка планируется во второй половине года). Посещение обучающих семинаров (конференций) с участием представителей регуляторов.

Этап 2. Проведение внутреннего аудита:

• анализ уведомления в Роскомнадзор (если проверяющий орган Роскомнадзор) — уведомление желательно обновить за 1–2 месяца до проверки (если, конечно, позволяют сроки);

• анализ политики в области обработки персональных данных — при необходимости внести в нее корректировки и сделать скриншот с сайта, где она размещена;

• ревизия сертификатов соответствия на средства защиты информации — необходимо проверить, чтобы они были надлежащим образом заверены и не были просрочены;

• подготовка перечня имеющихся локальных нормативных актов по защите информации (инструкции, регламенты, приказы, распоряжения).

Этап 3. Непосредственно подготовка к проверке. Для всех регуляторов подготавливаются следующие документы:

• учредительные документы юридического лица: выписка из ЕГРЮЛ, Устав (Положение), приказ о назначении руководителя. Копия документа, удостоверяющего полномочия физического лица, которое будет представлять интересы юридического лица при проведении проверки. Организационно-штатная структура юридического лица (штатное расписание, положение);

• журнал учета проверок юридического лица;

• документы, в которых зафиксировано, какие категории персональных данных обрабатывает оператор. Например, Политика в области обеспечения безопасности персональных данных, Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных;

• перечень информационных систем персональных данных. Как правило, их несколько, так как законодательство не допускает объединение информационных систем персональных данных, созданных в различных целях (например, ИСПДн, обрабатывающие данные о клиентах и данные о сотрудниках, необходимо разграничивать);

• модели угроз, акты определения уровня защищенности, формуляры и сертификаты на средства защиты информации;

• документы о назначении ответственного или структурного подразделения, ответственного за обеспечение обработки персональных данных;

• перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей;

• документы, регламентирующие режимные мероприятия (Инструкция по режиму безопасности). Журнал (реестр, кни-

га), содержащий персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию или в иных аналогичных целях;

• документ, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение таких последствий (инструкция по реагированию на инциденты информационной безопасности, инструкции по внутреннему контролю (аудиту), акты внутренних проверок);

• документы, подтверждающие ознакомление сотрудников с внутренними регламентами по обеспечению безопасности персональных данных (листы ознакомления). Также рекомендуется оформить листы ознакомления с Федеральным законом «О персональных данных», постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (для проверки ФСБ).

Представленный выше обобщенный перечень документов, необходимых для предоставления регуляторам, конкретизируется перед самой проверкой.

Этап 4. Непосредственно участие в проверке. Если проверка документарная, в адрес организации направляется приказ, в котором указывается перечень документов, необходимых для предоставления регулятору, и срок, отводимый на их предоставление. В указанный срок оператору необходимо предоставить регулятору запрашиваемые документы любым доступным способом: направить по почте либо нарочным с отметкой о получении. Регулятор примет эти документы, проведет их анализ и по его результатам составит и направит (также почтой либо нарочным) акт и, возможно, предписание.

Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения юридического лица, месту

осуществления деятельности индивидуального предпринимателя и (или) по месту фактического осуществления их деятельности. Обычно за 10 дней или месяц до начала проверки направляется по факсу или приносится сотрудником приказ о проведении проверки. Затем за 1–2 дня обговаривается время, когда комиссия приходит в организацию.

Проверка начинается с ознакомления руководителя организации с документами, удостоверяющими личности и принадлежность к государственному органу членов комиссии, затем вручается приказ о проведении проверки с перечнем вопросов и необходимых для предоставления документов, обговаривается срок их предоставления.

Руководитель, иное должностное лицо или уполномоченный представитель юридического лица обязаны предоставить должностным лицам органа государственного контроля (надзора), органа муниципального контроля, проводящим выездную проверку, возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, в случае, если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ проводящих выездную проверку должностных лиц и участвующих в выездной проверке экспертов, представителей экспертных организаций на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения, к используемому оборудованию.

По предоставлении документов комиссия производит их анализ. Работа с документами в случае выездной проверки может проходить как на территории организации, так и на территории самого регулятора (члены комиссии могут забрать их с собой). По итогам проверки подготавливается и вручается под подпись руководителю организации акт. К акту может быть приложено предписание об устранении выявленных нарушений. На практике, если нарушения незначительные, регуляторы часто дают возможность устранить их на месте и предписание не выносится. Нарушения, отдельные отступления вносятся в акт с указанием на то, что все устранено в ходе проверки.

Кроме того, в ходе проведения планового контроля могут проводиться мероприятия по обходу рабочих мест. Роскомнадзор и Государственная инспекция труда могут сделать акцент на проверке личных дел сотрудников в отделе кадров

(случайной выборкой). Комиссия просматривает личные дела сотрудников (в отделе кадров) на соответствие категорий персональных данных, содержащихся в документах кадрового делопроизводства, категориям, представленным в уведомлении об обработке персональных данных; проверяет порядок хранение личных дел сотрудников. ФСБ России производит обход с целью проверки режима, наличия опечатывающих устройств (на кабинетах, рабочих станциях, сейфах); мест хранения криптосредств (должны храниться в сейфах с опечатывающими устройствами на замочных скважинах); серверного помещения на наличие сигнализации, охраны, видеонаблюдения. ФСТЭК России может посмотреть техническую часть, сверить установленные средства защиты информации с эталонными при помощи программных средств анализа защищенности.

3.4. Подготовка оператора к внеплановой проверке

Как уже отмечалось, внеплановая проверка может проводиться в документарной и (или) выездной форме.

О проведении внеплановой выездной проверки юридическое лицо, индивидуальный предприниматель уведомляются органом государственного контроля (надзора) не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом. На практике при проведении проверки, касающейся обработки персональных данных, срок уведомления больше (от 10 дней до 1 месяца).

К уведомлению, как правило, прикрепляется приказ о проведении проверки, перечень документов, необходимых для предоставления регулятору, устанавливается срок. Во всем остальном порядок проведения проверки и ее форма (документарная либо выездная) схожи с плановой.

Иными словами, отличие заключается только в сроке и порядке уведомления о контрольно-надзорном мероприятии, а соответственно, основной проблемой будет подготовка недостающих документов и отсутствие времени на консультацию с операторами, имеющими опыт прохождения подобных проверок.

3.5. Ответственность за нарушение норм, регулирующих защиту персональных данных

1. Ответственность оператора персональных данных. В КоАП Ф с февраля 2017 г. введена специальная статья, предусматривающая ответственность за нарушение законодательства в области персональных данных. Данная статья включает семь разных случаев нарушения законодательства о персональных данных, за которые предусмотрена административная ответственность:

1) обработка персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, если эти действия не содержат уголовно наказуемого деяния, — влечет предупреждение или наложение административного штрафа на граждан в размере от 1 000 до 3 000 р.; на должностных лиц — от 5 000 до 10 000 р.; на юридических лиц — от 30 000 до 50 000 р.;

2) обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, — влечет наложение административного штрафа на граждан в размере от 3 000 до 5 000 р.; на должностных лиц — от 10 000 до 20 000 р.; на юридических лиц — от 15 000 до 75 000 р.;

3) невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных — влечет предупреждение или наложение административного штрафа на граждан в размере от 700 до 1 500 р.; на должност-

ных лиц — от 3 000 до 6 000 р.; на индивидуальных предпринимателей — от 5 000 до 10 000 р.; на юридических лиц — от 15 000 до 30 000 р.;

4) невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, — влечет предупреждение или наложение административного штрафа на граждан в размере от 1 000 до 2 000 р.; на должностных лиц — от 4 000 до 6 000 р.; на индивидуальных предпринимателей — от 10 000 до 15 000 р.; на юридических лиц — от 20 000 до 40 000 р.;

5) невыполнение оператором в сроки, установленные законодательством РФ в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, — влечет предупреждение или наложение административного штрафа на граждан в размере от 1 000 до 2 000 р.; на должностных лиц — от 4 000 до 10 000 р.; на индивидуальных предпринимателей — от 10 000 до 20 000 р.; на юридических лиц — от 25 000 до 45 000 р.;

6) невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния — влечет наложение административного штрафа на граждан в размере от 700 до 2 000 р.; на должностных лиц — от 4 000 до 10 000 р.; на индивидуальных

предпринимателей — от 10 000 до 20 000 р.; на юридических лиц — от 25 000 до 50 000 р.;

7) невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных — влечет предупреждение или наложение административного штрафа на должностных лиц в размере от 3 000 до 6 000 р.

Из текста данной нормы можно сделать вывод, что оператор как юридическое лицо может быть привлечен к административной ответственности за нарушение порядка сбора, хранения, использования или распространения персональных данных.

Помимо организации, ответственность за нарушение несет ее руководитель как должностное лицо. Это вытекает из смысла ст. 2.4 КоАП РФ, где указано, что под должностным лицом понимается лицо, выполняющее организационно-распорядительные или административно-хозяйственные функции.

Объектом правонарушения являются общественные отношения, складывающиеся в области защиты информации. Предметом правонарушения является порядок сбора, хранения, использования или распространения информации о гражданах (персональных данных). Данный порядок определяет Федеральный закон «О персональных данных».

Объективная сторона правонарушений состоит в несоблюдении норм федерального законодательства, регулирующих вопросы работы с информацией о гражданах (персональными данными). Выражена в форме конкретных действий субъекта, перечисленных выше.

Субъектами правонарушений могут быть граждане, должностные, юридические лица. Субъективная сторона правонарушения характеризуется умыслом или неосторожностью.

Протоколы об административных правонарушениях, предусмотренных комментируемой статьей, уполномочены составлять должностные лица органа, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), — это следует из п. 58 ч. 2 ст. 28.3 КоАП РФ.

Законодательство РФ устанавливает обязанности представителей определенных профессий (врачей, адвокатов, нотариусов и др.) по сохранению в тайне полученной информации и указывает на уголовную, гражданскую и административную ответственность за разглашение этих сведений. Такая ответственность предусмотрена ст. 137, 138, 155 УК РФ и ст. 152 ГК РФ.

Помимо данной статьи, КоАП РФ предусматривает также ответственность граждан и должностных лиц за нарушение правил защиты информации (ст. 13.12 КоАП РФ), за разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ), а также ответственность должностных лиц за отказ в предоставлении информации (ст. 5.39 КоАП РФ).

Статья 13.12. Нарушение правил защиты информации. Объектом административных правонарушений являются общественные отношения по защите информации. Порядок защиты информации регламентирован Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», ГК РФ и др.

Объективная сторона правонарушения выражается:

• в использовании несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации;

• в нарушении требований по защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ.

Субъектами правонарушения являются граждане, должностные и юридические лица. Субъективная сторона правонарушения характеризуется умыслом или неосторожностью.

Дела об указанных административных правонарушениях рассматривают должностные лица органов, осуществляющих государственный контроль в области обращения и защиты информации (ст. 23.46 КоАП РФ), т.е. должностные лица органов ФСБ России, ФСТЭК России и Роскомнадзора.

Статья 13.14. Разглашение информации с ограниченным доступом. Объектом правонарушения являются охраняемые законом интересы личности, общественные и государственные интересы, для реализации которых необходимо ограничение в доступе к определенным категориям сведений.

Статья распространяется на категории информации конфиденциального характера и не касается информации, составляющей государственную тайну. Это прежде всего сведения, касающиеся тайны следствия и судопроизводства; служебная тайна (сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами); профессиональная тайна — сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телефонных и иных сообщений и т.д.); коммерческая тайна (сведения, связанные с коммерческой деятельностью); сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Имеется в виду также банковская тайна (ст. 857 ГК РФ, ст. 26 Закона РФ от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» и ряд других источников). Порядок получения и использования информации ограниченного доступа устанавливается законом, подзаконными актами, договором.

Объективная сторона правонарушения связана с разглашением 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.

Субъект правонарушения специальный — гражданин или должностное лицо, получившие доступ к защищаемым категориям информации в связи с исполнением служебных или профессиональных обязанностей.

Субъективная сторона правонарушения характеризуется умыслом или неосторожностью.

Постановление о возбуждении дела выносится прокурором (ст. 28.4 КоАП РФ) либо протокол о правонарушении составля-

ется должностным лицом органов внутренних дел (полиции) (п. 1 ч. 2 ст. 28.3 КоАП РФ).

Дела о правонарушениях рассматриваются мировым судьей или судьей суда общей юрисдикции (ч. 1 ст. 23.1 КоАП РФ).

Статья 5.39. Отказ в предоставлении информации. Объектом правонарушений являются общественные отношения, складывающиеся по поводу получения и предоставления информации в любой сфере общественной жизни. Предметом правонарушения является информация, т.е. сведения о лицах, фактах, событиях, явлениях, процессах и т.п. Порядок предоставления информации регламентирован Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», законами РФ от 19 апреля 1991 г. № 1032-1 «О занятости населения в Российской Федерации», от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей», постановлением Правительства РФ от 24 ноября 2009 г. № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» и др.

Объективная сторона правонарушений составляет действия (бездействия), выражающиеся:

- в неправомерном отказе в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами;
- в несвоевременном ее предоставлении;
- в предоставлении заведомо недостоверной информации.

Субъектами правонарушений являются должностные лица.

Субъективная сторона правонарушения выражается умыслом.

Возбуждение дела по данной статье осуществляет прокурор (ст. 28.4 КоАП РФ). Дела об административных правонарушениях рассматривают судьи (ст. 23.1 КоАП РФ).

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

троль), муниципальный контроль. Объектом правонарушения является установленный порядок управления.

Объективная сторона правонарушения заключается в невыполнении виновным лицом в установленный срок законного предписания (постановления, решения, представления) об устранении нарушений законодательства, выявленных самостоятельно должностным лицом, вынесшим такое предписание, либо ставших ему известными в силу каких-либо обстоятельств.

В качестве субъекта административной ответственности выступают граждане, индивидуальные предприниматели, юридические лица и должностные лица.

Субъективная сторона правонарушения характеризуются умыслом либо неосторожной формой вины.

Однако возможна ситуация, в которой постановление о назначении административного наказания было признано недействительным только ввиду того, что должностное лицо контролирующего органа допустило грубые нарушения в ходе проверки. В соответствии с ч. 1 ст. 20 Федерального закона от 26 декабря 2008 г. № 294-ФЗ результаты проверки, проведенной с грубым нарушением установленных требований, не могут являться доказательствами совершения организациями административных правонарушений и подлежат отмене вышестоящим органом государственного контроля или арбитражным судом. Вместе с тем указанные обстоятельства не влекут незаконности предписания, поскольку невыполнение требований, изложенных в предписании, образует отдельный состав административного правонарушения. Проверяемое лицо через некоторое время может быть привлечено к административной ответственности ввиду того, что контролирующие органы захотят проверить исполнение им предписания.

2. Ответственность работника, имеющего доступ к персональным данным других работников. Исходя из смысла ст. 90 ТК РФ работник, по вине которого было допущено нарушение норм, регулирующих обработку и защиту персональных данных других работников, может быть привлечен к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности.

2.1. Административная ответственность работника, имеющего доступ к персональным данным других работников. На основании ст. 2, 3, 5, 6 Федерального закона «О персональных

данных» персональные данные относятся к информации, доступ к которой ограничен. В соответствии со ст. 13.14 КоАП РФ разглашение подобной информации (за исключением случаев, если такое разглашение влечет уголовную ответственность) лицом, получившим доступ к ней в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа:

- на граждан — от 500 до 1 000 р.;
- на должностных лиц — от 4 000 до 5 000 р.

Следовательно, если будет установлено, что разглашение персональных данных произошло по вине работника, ответственного за хранение, обработку и использование персональных данных других работников, то его могут привлечь к административной ответственности в виде штрафа.

2.2. Дисциплинарная ответственность работника, имеющего доступ к персональным данным других работников. Персональные данные относятся к сведениям, которые охраняются федеральным законом. Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТК РФ). Согласно подп. «в» п. 6 ч. 1 ст. 81 ТК РФ трудовой договор с работником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе по причине разглашения персональных данных другого работника. Поскольку такое увольнение относится к увольнениям за нарушение трудовой дисциплины, то работника, разгласившего персональные данные, необходимо уволить с соблюдением процедуры, предусмотренной ст. 193 ТК РФ.

2.3. Уголовная ответственность работника, имеющего доступ к персональным данным других работников. В соответствии со ст. 137 УК РФ незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются штрафом до 200 000 р. или в размере заработной платы либо иного дохода осужденного за период до 18 месяцев,

либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

Часть 2 указанной статьи предусматривает, что те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом от 100 000 до 300 000 р. или в размере заработной платы либо иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Следовательно, если работник, ответственный за хранение, обработку и использование персональных данных других работников, злоупотреблял своими служебными полномочиями, распространял сведения о частной жизни других работников без их согласия, то он может быть привлечен к уголовной ответственности.

2.4. Материальная ответственность работника, имеющего доступ к персональным данным других работников. Статьей 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих обработку и защиту персональных данных работников. Так, в результате незаконного распространения информации о персональных данных работника последнему может быть причинен моральный вред, подлежащий возмещению работодателем. В соответствии со ст. 238 ТК РФ работник обязан возместить работодателю причиненный последнему прямой действительный ущерб. Согласно ч. 2 указанной статьи под прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред работнику был допущен по вине лица, которое было ответственно за неразглашение персональных данных, то работодатель может привлечь последнее к материальной ответственности за ущерб, который был нанесен работнику такими действиями. В соответствии с п. 7 ч. 1 ст. 243 ТК РФ материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

2.5. Гражданско-правовая ответственность работника, имеющего доступ к персональным данным других работников.

В соответствии со ст. 151 ГК РФ, если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Согласно ч. 2 ст. 1099 ГК РФ моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом. На основании ст. 152 ГК РФ гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Следовательно, если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работника, допущенного лицом, ответственным за осуществление вышеперечисленных действий с персональными данными, работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии со статьями ГК РФ.

Таким образом, можно сделать следующие выводы.

Основными контрольными органами, осуществляющими надзор за соблюдением действующего законодательства о персональных данных, являются три федеральные службы: Роскомнадзор РФ, ФСТЭК России, ФСБ России. При этом каждая служба обладает своим видением относительно применения тех или иных правовых норм, что может приводить к необоснованному выявлению нарушений и привлечению операторов к ответственности.

Действующее законодательство содержит широкий перечень норм, предусматривающих ответственность различных категорий субъектов за его нарушение. Однако существующие санкции на сегодняшний день нельзя признать эффективными. Так, размер штрафов в десятки-сотни раз меньше издержек, которые необходимо понести организации для реализации комплекса мероприятий по защите информации. Указанное обстоятельство приводит к тому, что на практике операторы отказываются от выделения необходимых средств и сознательно идут на нарушение законодательства.

Контрольные вопросы

1. Перечислите и охарактеризуйте основных регуляторов в сфере персональных данных.

2. Что считается государственной информационной системой? Приведите примеры государственных информационных систем.

3. Какие функции применительно к сфере персональных данных выполняют Прокуратура РФ и Государственная инспекция труда?

4. Перечислите основания для проведения внеплановой проверки на предмет соблюдения законодательства о персональных данных.

5. Опишите алгоритм проведения плановой проверки на предмет соблюдения законодательства о персональных данных.

6. Опишите алгоритм проведения внеплановой проверки на предмет соблюдения законодательства о персональных данных.

7. Опишите алгоритм подготовки оператора к плановой проверке.

8. Опишите алгоритм подготовки оператора к внеплановой проверке.

9. Перечислите виды ответственности за нарушение законодательства в сфере обработки персональных данных.

10. Дайте характеристику составу административного правонарушения, предусмотренному ст. 5.39 КоАП РФ.

11. Дайте характеристику составу административного правонарушения, предусмотренному ст. 13.12 КоАП РФ.

12. Дайте характеристику составу административного правонарушения, предусмотренному ст. 13.14 КоАП РФ.

13. Дайте характеристику составу административного правонарушения, предусмотренному ст. 19.5 КоАП РФ.

14. В каких случаях работник организации, допущенный к работе с персональными данными, может быть подвергнут дисциплинарной и уголовной ответственности? Чем это регламентируется? Какие санкции предусмотрены?

Кейсы

Кейс 1. *Подготовка к проверке регуляторов*

Исходя из материалов главы подготовьте схему бизнес-процессов:

1) бизнес-процесс «подготовка к плановой проверке»;

2) бизнес-процесс «подготовка к внеплановой проверке».

Сделайте чек-лист с описанием мероприятий по подготовке к указанным видам проверок.

Кейс 2. *Внеплановая проверка Роскомнадзора*

Проанализируйте решение Арбитражного суда Свердловской области по делу № А60-41475/2011 (http://kad.arbitr.ru/Card/7b61a697-825d-4f7e-b232-5a5ef01a3a5f).

Опишите, в чем, по вашему мнению, заключались ошибки оператора персональных данных. Какие рекомендации вы бы дали оператору в части подготовки к контрольно-надзорным мероприятиям Роскомнадзора.

Кейс 3. *Разглашение персональных данных работником*

Службой информационной безопасности компании средствами системы мониторинга действий пользователей была выявлена сотрудница, которая передала неизвестному лицу файл, содержащий персональные данные.

Каковы дальнейшие действия службы информационной безопасности (опишите алгоритм)?

К какому виду ответственности следует привлечь данную сотрудницу?

4. Общий регламент по защите данных (General Data Protection Regulation) Европейского союза

Директива 95/46/EC Европейского парламента и Совета Европейского союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных» 25 мая 2018 г. была отменена. В настоящее время действует Общий регламент по защите данных (General Data Protection Regulation, сокращенно GDPR), принятый 27 апреля 2016 г. GDPR вносит свои изменения в защиту физических лиц в отношении обработки их персональных данных.

4.1. Территориальная сфера применения

GDPR имеет экстерриториальную сферу применения. Действие регламента распространяется на:

1) компании, зарегистрированные на территории Европейского союза (далее по тексту — ЕС), независимо от места проведения самой обработки;

2) компании, не зарегистрированные на территории ЕС, если:

• производится предложение товаров/услуг гражданам или резидентам ЕС;

• производится мониторинг действий граждан или резидентов ЕС;

3) компании, зарегистрированные в странах, следующих законодательству ЕС на основании международных договоров.

Для того чтобы понять, предлагает ли компания свои товары или услуги лицам, находящимся на территории ЕС, следует установить очевидность намерения, т.е. волеизъявление компании считать себя заключившей договор с любым лицом, находящимся на территории ЕС, акцептовавшим ее оферту. По GDPR одними из признаков намерений является использование веб-сайтом функционала на языке государства — члена ЕС и производство расчета цен в валюте государства — члена ЕС с возможностью заказа либо упоминание потребителей или пользователей, находящихся на территории ЕС.

Под мониторингом понимается отслеживание лиц в сети Интернет с дальнейшим применением или потенциальной возможностью применения различных технологий по обработке персональных данных для анализа либо прогнозирования предпочтений, личностных характеристик, особенностей поведения.

Компании, не зарегистрированные в ЕС, обязаны в форме письменного документа назначить представителя ЕС, когда выполняется хотя бы одно из условий:

• обработка происходит постоянно;

• обрабатываются специальные категории персональных данных в больших количествах;

• обрабатываются персональные данные, связанные с судимостями или преступлениями;

• существует высокий риск нарушения прав и свобод человека.

Представителем может стать физическое или юридическое лицо, расположенное в стране ЕС, в которой находятся субъекты данных. Его задача от имени компании взаимодействовать с властями ЕС и гражданами, выполнять указания компании. Он точно так же привлекается к ответственности за нарушения.

4.2. Лица, осуществляющие обработку персональных данных

GDPR вводит новые понятия: контролер и процессор.

Контролер (англ. controller) — физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. В случае, когда цели и средства обработки определяются правом Евросоюза или государства-члена, контролер или критерии для его назначения могут быть установлены правом Евросоюза или государства-члена.

Процессор (обработчик, англ. processor) — физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени и по поручению контролера.

В том случае, если два или более контролеров совместно определяют цели и средства обработки, они являются совместными контролерами. Они должны прозрачным способом определить свои соответствующие функциональные обязанности на предмет соблюдения обязательств.

Договоренность должна надлежащим образом отражать соответствующие роли и взаимоотношения контролеров, действующих совместно по отношению к субъектам данных. Существенные условия договоренности должны быть доступны для субъектов данных. Независимо от условий договоренности, субъект данных может осуществлять свои права в отношении каждого контролера.

Между процессором и контролером должен существовать договор либо иной правовой акт, содержащий:

- предмет и период, в течение которого осуществляется обработка;
- характер и цель обработки;
- тип персональных данных и категории субъектов данных;
- обязанности и права контролера;
- обязательства соблюдать конфиденциальность.

Контролер должен удостовериться, что процессор применяет технические и организационные меры, отвечающие требованиям и обеспечивающие защиту прав субъекта данных.

Процессор не должен привлекать другого процессора без предварительного письменного оформления специального или общего разрешения контролера. Процессор должен проинформировать контролера о любых предполагаемых изменениях. Контролер имеет возможность высказать возражения против любых изменений.

Если процессор нарушает требования GDPR в отношении определения целей и средств обработки, то этот процессор должен рассматриваться в качестве контролера применительно к такой обработке, в том числе в случае наложения штрафа.

4.3. Обработка и хранение персональных данных

Принципы обработки персональных данных обновлены, но в целом аналогичны Директиве 95/46/ЕС:

- правомерность, справедливость и прозрачность (транспарентность);
- целевое ограничение;
- минимизация данных;
- точность;
- ограниченность хранения;
- целостность и конфиденциальность.

Добавляется понятие о прозрачности обработки и обязанность компании быть готовой подтвердить выполнение требований законодательства по защите персональных данных.

4.4. Правомерность обработки и согласие субъекта персональных данных

Основания для обработки остались такими же, как и в Директиве 95/46/ЕС:

- согласие субъекта данных;
- заключение договора;

• выполнение юридических обязательств;

• защита жизненных интересов субъекта данных;

• выполнение общественных интересов или осуществление официальных полномочий;

• обеспечение законных интересов компании.

В GDPR появилась статья, в которой говорится об обработке, не требующей идентификации. Если при использовании обрабатываемых персональных данных идентифицировать (определить) субъекта данных невозможно, то обработку таких данных можно производить. При этом права субъекта к таким данным не применяются, за исключением случая, когда субъект предоставил дополнительную информацию, которая теперь позволяет его определить. Компания должна быть способна подтвердить, что возможности идентифицировать субъекта нет.

Установлены конкретные требования к согласию субъекта персональных данных. Согласие на обработку должно быть представлено отдельно от других условий и согласий. Оно должно быть изложено в конкретной и понятной форме, легкодоступным языком. Согласие должно быть дано на основании активных действий, а не «по умолчанию» или путем бездействия. Субъект данных должен иметь возможность отозвать свое согласие так же легко, как и дать его.

Отдельным пунктом вынесено согласие ребенка. За детей, не достигших 16 лет, согласие должно давать лицо, осуществляющее родительские функции или функции опеки. Государства могут законодательно предусмотреть меньший возраст при условии, что он не будет ниже 13 лет.

4.5. Информация, передаваемая субъекту персональных данных

GDPR расширяет перечень обязательных данных, которые компания должна предоставить субъекту данных в момент получения персональных данных для поддержания справедливости и транспарентности обработки.

Информация обязательная к предоставлению включает:

• сведения о компании, производящей обработку;

• данные о лице, ответственном за защиту персональных данных, там, где это применимо;

• цели и правомерность основания обработки;

• сведения об иных получателях информации, если таковые имеются;

• сведения о трансграничной передаче;

• срок хранения персональных данных, если возможно;

• информацию о праве доступа, исправления, удаления, возражения, ограничения обработки и праве на переносимость субъекта персональных данных;

• информацию о праве отзыва согласия субъектом персональных данных;

• информацию о праве подачи жалобы в надзорный орган;

• обязательность/необязательность предоставления персональных данных субъектом;

• наличие автоматизированного принятия решения.

4.6. Право субъекта на доступ к данным

При обращении субъекта данных компания обязана предоставить ему сведения следующего характера:

• цели обработки;

• категории обрабатываемых данных;

• информация об иных получателях персональных данных;

• срок хранения персональных данных, если возможно, либо критерии определения этого срока;

• информация о праве доступа, исправления, удаления, возражения, ограничения обработки и праве на переносимость субъекта персональных данных;

• информация о праве подачи жалобы в надзорный орган;

• данные об источнике информации, связанной с персональными данными, если она получена не от субъекта данных;

• информация о применении автоматизированного принятия решения.

При запросе субъекта компания также обязана предоставить ему копию обрабатываемых персональных данных субъекта, в том числе в электронной форме.

4.7. Право субъекта на изменение, удаление персональных данных

GDPR делает акцент на правах субъекта данных, давая к ним обширные разъяснения.

Компания обязана при обращении субъекта исправить или дополнить неточные данные. Должна быть реализована возможность удаления персональных данных в случаях, когда:

- персональные данные больше не нужны для заявленных целей;
- субъект данных отозвал согласие;
- не имеется правовой аргументации, мешающей запросу субъекта на удаление;
- персональные данные обработаны неправомерно;
- имеются правовые обязательства по удалению в законодательстве страны компании;
- согласие было дано в детском возрасте.

4.8. Право на переносимость данных

Нововведением GDPR является понятие о переносимости данных.

При осуществлении автоматизированной обработки на основании согласия субъекта персональных данных или договора по требованию субъекта компания обязана предоставить ему касающиеся его данные в структурированном виде, в том числе в машиночитаемом формате. Компания обязана беспрепятственно передать персональные данные субъекта по его запросу другим организациям, если это технически осуществимо.

4.9. Защита персональных данных и уведомление об утечке информации

GDPR вносит понятия защиты «by design» и «by default».

Понятие «by design» означает защиту еще на этапе проектирования (разработки) для осуществления принципов обра-

ботки данных, например псевдонимизацию. Псевдонимизацией является такая обработка данных, когда персональные данные не могут быть соотнесены с субъектом данных без использования дополнительной информации. Дополнительная информация должна храниться отдельно от самих данных с применением мер, обеспечивающих их защиту. По сути, псевдонимизация аналогична предусмотренному российским законодательством процессу обезличивания.

Понятие «by default» означает защиту по умолчанию, компания должна обеспечить обработку персональных данных с максимальной защитой конфиденциальности (например, данные должны обрабатываться короткий период хранения с ограниченной доступностью). Иными словами, по умолчанию личные данные не становятся доступными для неопределенного количества людей.

Должны применяться технические и организационные меры, обеспечивающие надлежащий уровень безопасности, на основании рисков (например, риск случайного или преднамеренного удаления, потери, изменения данных и т.д.).

В случаях утечки персональных данных, компания обязана сообщить о происшествии надзорному органу, за исключением случаев, когда эта утечка едва ли обернется рисками для прав и свобод лиц. Рекомендуемый срок — в течение 72 часов после обнаружения. В уведомление необходимо включить:

- сведения о характере утечки, а также сведения о категории и количестве персональных данных, если возможно;
- данные лица, ответственного за защиту, или контактные данные пункта, где может быть получена подробная информация;
- возможные последствия утечки;
- меры, принятые или предполагаемые к принятию, по устранению утечки и смягчению последствий.

По GDPR надзорный орган назначается в каждой стране соответствующими нормативно-правовыми актами.

Взаимодействовать с надзорным органом государства — члена ЕС должен представитель компании, назначенный в этом государстве. Уведомление об утечке персональных данных рекомендуется направлять в надзорный орган государства, в котором расположен представитель ЕС. По GDPR в случаях, когда компания учреждена в нескольких государ-

ствах — членах ЕС, или значительное число субъектов данных находится более чем в одном государстве, в действиях по проверке соответствия требованиям участвуют надзорные органы каждого государства. При этом дается четкое указание, что по мере возможности надзорные органы должны действовать совместно.

По GDPR процесс действий российских компаний без представительства в ЕС не раскрыт. Логично предположить, что надзорный орган государства, чьи субъекты персональных данных пострадали от утечки, должен действовать совместно с Роскомнадзором. Но этот момент остается спорным.

Компания должна документировать любые утечки персональных данных, их последствия, а также принятые меры по устранению последствий.

Компания должна сообщить об утечке персональных данных субъекту персональных данных в разумный срок, за исключением случаев, когда:

- проблема не приведет к высоким рискам для прав и свобод субъекта;
- данные были зашифрованы;
- принятые меры исключают возможные риски правам и свободам субъекта;
- для сообщения требуются несоразмерные усилия (в этом случае уведомление возможно через средства массовой информации).

4.10. Учетные записи обработки данных

Компания обязана вести учетные записи процессов обработки данных в письменной, в том числе электронной, форме. Учетные записи должны содержать:

- наименование, реквизиты компании и, когда применимо, представителя компании в ЕС, лица, ответственного за защиту данных;
- цели обработки;
- описание субъектов данных и категорий обрабатываемых персональных данных;

• сведения об иных получателях, которым были или будут раскрыты персональные данные;

• сведения о трансграничной передаче;

• предусмотренные сроки удаления персональных данных, когда это возможно;

• сведения о применяемых технических и организационных мерах безопасности, когда это возможно.

Компания не обязана вести учетные записи, если в ней менее 250 сотрудников и она выполняет следующие условия:

• осуществляемая обработка не может привести к возникновению рисков для прав и свобод субъекта данных;

• обработка носит случайный характер;

• не обрабатываются специальные категории персональных данных;

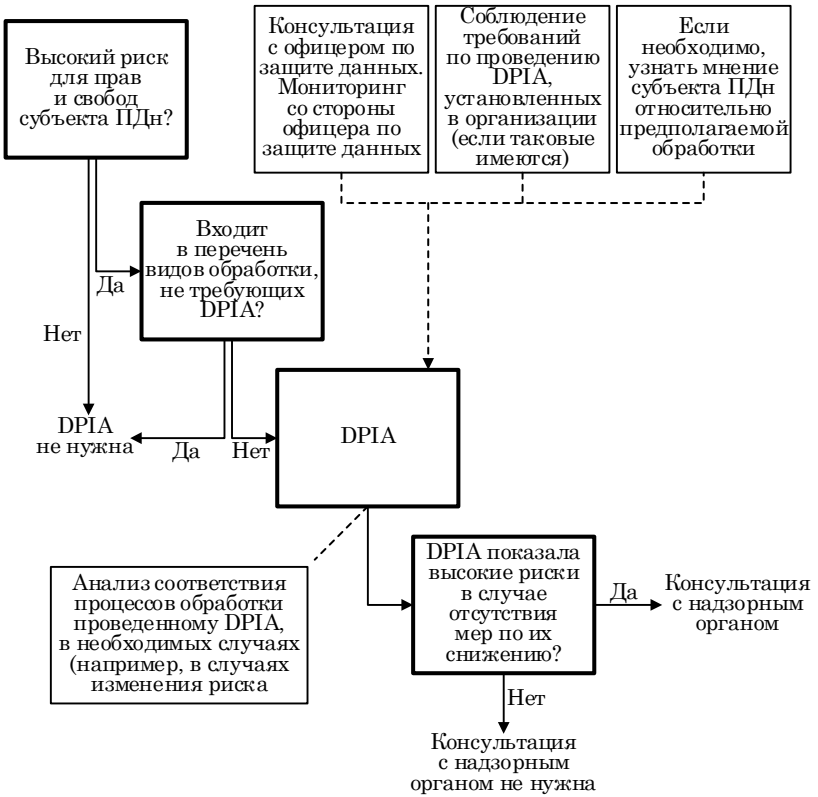
• не обрабатываются персональные данные, связанные с судимостями или правонарушениями.

4.11. Оценка воздействий на защиту персональных данных

В GDPR выделена отдельная статья, посвященная «оценке воздействия на защиту данных» (англ. data protection impact assessment, DPIA). Для выполнения предусмотренных в ней требований нужно определить степень важности каждого конкретного бизнес-процесса, связанного с обработкой персональных данных, посредством оценки ущерба, нанесенного в период сбоя в работе.

На рисунке показан алгоритм DPIA по GDPR.

Если обработка может повлечь за собой высокий риск для прав и свобод субъектов персональных данных, компания, до начала обработки, обязана провести оценку воздействия на защиту персональных данных предполагаемых бизнес процессов, связанных с обработкой. Если компания производит постоянный мониторинг субъектов или обрабатывает в большом количестве специальные категории данных, а также персональные данные, касающиеся осужденных и правонарушителей, то она обязана провести DPIA.



Алгоритм оценки воздействия
на защиту персональных данных

В оценку воздействия как минимум нужно включить:

• описание предусмотренных операций по обработке персональных данных;

• оценку необходимости и соразмерности операций обработки по отношению к заявленным целям обработки;

• оценку рисков для прав и свобод субъектов персональных данных;

• меры по обеспечению защиты персональных данных.

GDPR не указывает, как конкретно должен проходить процесс DPIA. Главное, чтобы структура оценки воздействия включала указанный минимум. В опубликованных разъясне-

ниях по DPIA Рабочей группы по вопросам защиты физических лиц при обработке персональных данных (WP29), в состав которой входят представители органов по защите данных государств — членов ЕС, есть некоторые рекомендации по проведению DPIA. С 25 мая 2018 г. WP29 была заменена на Европейский совет по защите данных (European Data Protection Board, EDPB).

Орган по защите данных в Великобритании (Information Commissioner's Office, ICO) также дает свои рекомендации по проведению DPIA на сайте[1], где, например, можно найти образец шаблона DPIA.

Оценка воздействия должна обеспечивать подтверждение соблюдения требований GDPR.

4.12. Ответственный за защиту данных

В GDPR есть самостоятельный раздел об офицере по защите данных (англ. data protection officer). Если организация является органом власти или учреждением, или производит постоянный мониторинг субъектов, или обрабатывает в большом объеме специальные категории данных, а также персональные данные, касающиеся осужденных и правонарушителей, то она обязана назначить офицера по защите данных. В других случаях назначение делается на усмотрение компании или на основании законов ее государства. Компания должна опубликовать реквизиты офицера по защите данных.

4.13. Условия наложения штрафов

Для усиления обязательности соблюдения норм GDPR вводит штрафы за любые нарушения.

На принятие решения о наложении и размере штрафа влияют следующие обстоятельства:

[1] URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias.

• характер, тяжесть и продолжительность нарушения; количество пострадавших субъектов данных и размер понесенного ущерба;

• по неосторожности или преднамеренно совершено нарушение;

• меры, принятые для смягчения ущерба;

• использованные меры по защите данных;

• прошлые нарушения;

• степень сотрудничества с надзорным органом;

• категории затронутых нарушением персональных данных;

• как стало известно о нарушении, например, было ли уведомление об утечке;

• иные отягчающие или смягчающие факторы.

Если было нарушено несколько положений, то общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

1. Административные штрафы в размере до 10 млн евро или в размере до 2 % от годового оборота компании за весь предыдущий финансовый год (в зависимости от того, какая сумма больше) накладываются за нарушение требований в следующих сферах:

• обработка персональных данных ребенка;

• обработка, не требующая идентификации;

• защита при проектировании и по умолчанию;

• совместная обработка с другими компаниями;

• назначенные представители компании;

• отчетные записи;

• обеспечение безопасности обработки персональных данных;

• уведомления об утечках;

• оценка воздействий процессов обработки на защиту данных;

• требования к офицеру по защите данных.

2. Административные штрафы в размере до 20 млн евро или в размере до 4 % от годового оборота компании за весь предыдущий финансовый год (в зависимости от того, какая сумма больше) накладываются за нарушение требований в следующих сферах:

• принципы обработки;

- правомерность обработки;
- согласие субъекта на обработку персональных данных;
- специальные категории;
- права субъекта;
- трансграничная передача.

4.14. Ключевые отличия требований GDPR от российского закона «О персональных данных»

Сравнительный анализ, представленный в табл. 4, показал, что GDPR и Федеральный закон «О персональных данных» схожи. Основные отличия GDPR заключаются в:

- уточненном перечне персональных данных;
- назначении представителя в ЕС;
- списке информации, передаваемой субъекту, касательно процесса обработки;
- процессе оценки воздействия на защиту данных (DPIA);
- защите «by design» и «by default»;
- праве субъекта персональных данных на переносимость данных в машиночитаемом формате;
- требованиях к согласию субъекта персональных данных на обработку данных в части использования легкодоступного языка, конкретных обязательств в части детей, отделения от других обязательств;
- требованиях к обработке персональных данных детей;
- конкретизированном списке информации необходимой для ведения учетных записей по обработке персональных данных;
- уведомлении об утечке персональных данных надзорного органа и субъекта;
- жестких наказаниях (крупные штрафы) за невыполнение требований.

Таблица 4

Сравнительный анализ GDPR и Федерального закона «О персональных данных»

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
1. Сведения, отнесенные к ПДн	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу	Любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу; идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно. К персональным данным относятся: имя, идентификационный номер, данные о местоположении, идентификатор в Интернете (онлайн-идентификатор) или один или несколько показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности физического лица	Уточненный перечень данных, относящихся к персональным
2. Лицо, выполняющее обработку	Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Лицо, осуществляющее обработку персональных данных по поручению оператора	Контролер (англ. controller) — физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. Процессор (англ. processor) — физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени и по поручению контролера	Оператор аналогичен контролеру. Лицо, осуществляющее обработку персональных данных по поручению оператора, аналогично процессору

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
3. Совместная обработка данных	Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта данных на основании заключаемого с этим лицом договора или иного правового акта. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных. В поручении оператора должны быть определены перечень действий с персональными данными, которые будут совершаться лицом, осуществляющим обработку, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных. Лицо, осуществляющее обработку по поручению оператора, не обязано получать согласие субъекта на обработку данных. Если оператор поручает обработку другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором	В том случае, если два или более контролеров совместно определяют цели и средства обработки, они являются совместными контролерами. Между процессором и контролером должен существовать договор либо иной правовой акт. Контролер должен удостовериться, что процессор применяет технические и организационные меры, отвечающим требованиям и обеспечивающие защиту прав субъекта данных. Если процессор нарушает требования GDPR в отношении определения целей и средств обработки, то этот процессор должен рассматриваться в качестве контролера применительно к такой обработке, в том числе в случае наложения штрафа	GDPR вносит понятие совместных контролеров, т.е. компаний, совместно занимающихся обработкой, и обязательство открытого для субъекта данных соглашения, включающего роли и обязанности каждой компании-контролера. Лицо, осуществляющее обработку персональных данных по поручению, в обоих документах должно действовать на основании правовых актов и соблюдать все обязанности и требования по защите данных. За исключением факта, что по GDPR в некоторых случаях ответственным за нарушение требований к обработке будет являться процессор, т.е. лицо, осуществляющее обработку по поручению оператора

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
4. Принципы обработки персональных данных	1. Законная и справедливая основа. 2. Ограничение достижением конкретных, заранее определенных и законных целей. 3. Не допускается объединение баз данных персональных данных, обработанных в целях, несовместимых между собой. 4. Персональные данные должны отвечать целям их обработки. 5. Персональные данные должны соответствовать заявленным целям и не должны быть избыточными. 6. Точность, достаточность, актуальность персональных данных. Возможность удаления или уточнения неполных или неточных данных. 7. Хранение не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей	a) Правомерность, справедливость и прозрачность (транспарентность); b) целевое ограничение; c) минимизация данных; d) точность; e) ограниченность хранения; f) целостность и конфиденциальность	Пункт 1 Федерального закона «О персональных данных» аналогичен п. «a» GDPR, за исключением понятия прозрачности обработки данных. Принцип прозрачности (транспарентости) требует, чтобы любые сведения и сообщения, относящиеся к обработке персональных данных, были легко доступны субъекту персональных данных и ясны для понимания, а также чтобы использовался четкий и простой язык. Пункты 2 и 4 аналогичны п. «b»; 5 — «c»; 6 — «d»; 7 — «e». Федеральный закон «О персональных данных» в п. 3 делает уточнение для баз данных. Пункт «f» GDPR закреплен в российском законодательстве в отдельных статьях и является также обязательным. GDPR обязывает организации быть готовыми предоставить обоснование соответствия требованиям

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
5. Условия обработки персональных данных	1. Согласие субъекта персональных данных. 2. На основании международных договоров РФ или законов РФ, возложенных законодательством РФ функций, полномочий и обязанностей. 3. Участие лица в судопроизводстве или в целях исполнения судебного акта. 4. Исполнение полномочий федеральных органов. 5. Исполнение договора. 6. Защита жизненно важных интересов субъекта персональных данных. 7. Осуществление прав и законных интересов организации либо достижение общественно значимых целей. 8. Деятельность средств массовой информации либо иная творческая деятельность. 9. Статистические или иные исследовательские цели. 10. Персональные данные сделаны общедоступными субъектом данных. 11. Персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с действующим законодательством	a) Согласие субъекта данных; b) исполнение договора; c) выполнение юридических обязательств; d) защита жизненных интересов субъекта данных; e) выполнение общественных интересов или осуществление официальных полномочий; f) обеспечение законных интересов организации	Условия для обработки сопоставимы. GDPR позволяет государствам закреплять более конкретные положения для применения норм

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
6. Требования к согласию субъекта персональных данных на обработку персональных данных	Субъект дает согласие на обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку может быть дано в любой позволяющей подтвердить факт его получения форме. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Обязанность предоставить доказательство получения согласия возлагается на оператора. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает его законный представитель	Контролер должен быть способен подтвердить, что субъект данных согласен на обработку персональных данных. Если согласие субъекта данных дается в виде письменного заявления, которое также касается других вопросов, запрос о согласии должен быть представлен способом, который четко отличен от других вопросов, в понятной и легкодоступной форме, с использованием ясного и простого языка. Субъект данных должен иметь право в любое время отозвать согласие. Прежде чем давать согласие, субъект данных должен быть проинформирован об этом. Процедура отзыва согласия должна быть такой же простой, как и процедура предоставления согласия. Согласие должно быть предоставлено по доброй воле. Обработка персональных данных ребенка является правомерной, если ребенку исполнилось как минимум 16 лет. Если ребенок еще не достиг возраста 16 лет, такая обработка является правомерной на основании согласия лица, осуществляющего родительские функции или функции опеки	GDPR дает уточнения по согласию: • использовать в согласии легкодоступный язык; • отделить согласие от других соглашений и обязательств; • избавиться от настроек дачи согласия «по умолчанию»; • молчание не является согласием, нужны активные действия по даче согласия; • процесс отзыва должен быть прост, как и его дача (поставить галочку — убрать галочку); • должна быть представлена информация о возможности отзыва согласия. В GDPR дается конкретное требование к согласию для детей младше 16 лет

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
7. Специальные категории данных	Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством РФ, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами	Персональные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские воззрения либо членство в профсоюзе, а также генетические данные, биометрические данные для однозначной идентификации физического лица, данные, касающиеся здоровья, половой жизни или сексуальной ориентации физического лица. Обработка персональных данных, связанных с уголовными приговорами и правонарушениями или связанных с мерами безопасности, осуществляется только под контролем официального органа либо когда обработка разрешена правом государства	Определение специальных категорий аналогично, за исключением рассмотрения персональных данных, относящихся к уголовным делам и правонарушениям, в отдельной статье
8. Права субъекта данных	Право субъекта персональных данных на доступ к его персональным данным. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных. Право на обжалование действий или бездействия оператора	Получение информации субъектом данных при сборе персональных данных. Право субъекта данных на доступ к данным. Право на исправление данных. Право на удаление данных. Право на ограничение обработки. Право на переносимость данных. Право на возражение	GDPR требует прозрачности обработки от операторов, поэтому при передаче персональных данных на обработку субъект данных должен получить всю информацию. По GDPR компания обязана предоставить субъекту персональных данных по запросу копию его ПДн, в том числе в электронном виде, а также право на переносимость. В остальном права субъектов персональных данных в обоих документах аналогичны

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
9. Обязанности оператора при сборе персональных данных	При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию об обработке	В том случае, если персональные данные собираются от субъекта данных, контролер должен в момент получения персональных данных предоставить субъекту информацию об обработке	В № 152-ФЗ предоставление информации перед обработкой происходит по запросу субъекта данных. GDPR обязывает передать информацию до начала обработки в любом случае
10. Принятие решений на основании исключительно автоматизированной обработки	Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных. Оператор обязан разъяснить субъекту персональных данных 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.	Субъект данных должен иметь право не подчиняться решению, основанному исключительно на автоматизированной обработке, включая составление профиля, которое порождает правовые последствия, касающиеся его. За исключением случаев, когда принятие решения: a) является необходимым для заключения или исполнения договора; b) дозволено правом законодательства; c) основывается на прямом согласии субъекта данных. В случаях, связанных с согласием и договором, контролер данных должен применять надлежащие меры для защиты прав и свобод субъекта данных и его законных интересов, как минимум, конкретное информирование субъекта данных, предоставление права запросить вмешательство контролера, права выражать точку зрения, а также оспаривать решение.	В GDPR добавляется, что принятие решения на основании автоматизированной обработки возможно при заключении договора, а не только по согласию субъекта данных или по разрешению законодательства. По GDPR и по Федеральному закону «О персональных данных» субъект данных может выразить свою точку зрения и заявить свое возражение в отношении принятого решения

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
	Оператор обязан рассмотреть возражение в течение 30 дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения	Решения не должны основываться на особых категориях персональных данных, за некоторым исключением	
11. Меры по обеспечению безопасности персональных данных	Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. Обеспечение безопасности ПДн достигается: 1) определением угроз безопасности;	Учитывая современный уровень развития техники, затраты, связанные с внедрением, а также характер, объем, контекст и цели обработки, вероятностное возникновение рисков и опасности для прав и свобод физических лиц, организация должна принимать соответствующие технические и организационные меры, обеспечивающие надлежащий уровень безопасности соразмерный рискам. Каждый контролер должен вести учетные записи обработки данных, находящейся под его ответственностью. При определении надлежащего уровня безопасности в расчет должны приниматься в том числе риски, которые представляет собой сама обработка, в особенности риски от случайного или неправомерного уничтожения, потери, изменения, несанкционированного раскрытия или доступа к ПДн, переданным, сохраненным либо или иным образом обработанным.	Оба документа требуют обеспечения безопасности персональных данных, приводя минимальные наборы технических и организационных мер. GDPR делает уточнения к обязательному ведению учетных записей по процессу обработки, за исключением некоторых случаев. Обязательна оценка воздействия предполагаемых процессов обработки на безопасность данных. По GDPR при построении систем безопасности должна быть произведена оценка рисков, что аналогично разработке модели угроз. GDPR вносит требования к защите при проектировании и по умолчанию (англ. by design, by default). По GDPR организация обязана в случаях утечки данных сообщать о ней в надзорный орган и субъекту данных

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
	2) применением организационных и технических мер по обеспечению безопасности персональных данных; 3) применением сертифицированных средств защиты информации; 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн; 5) учетом машинных носителей персональных данных; 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер; 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа; 8) установлением правил доступа к персональным данным, обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн; 9) контролем за реализацией принимаемых мер по обеспечению безопасности данных и уровня защищенности ИСПДн	Меры, обеспечивающие надлежащий уровень безопасности соразмерный рискам, включают среди прочего следующее: a) псевдонимизация и криптографическая защита персональных данных; b) средства для обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки и услуг; c) средства своевременного восстановления доступности и доступа к персональным данным в случае природного или технического инцидента; d) процедура регулярной проверки и оценки эффективности технических и организационных мер, обеспечивающая безопасность обработки. В тех случаях, когда тип обработки данных (в частности, при использовании новых технологий, а также принимая во внимание характер, объем, контекст и цели обработки) вероятнее всего приведет к высокому риску для прав и свобод физических лиц, контролер должен до этой обработки осуществить оценку воздействия предусмотренных операций обработки на защиту персональных данных. Защита данных для определенных целей/случаев и по умолчанию	

Продолжение табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
12. Лица, ответственные за организацию обработки персональных данных	Оператор назначает лицо, ответственное за организацию обработки персональных данных. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано: 1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных; 2) доводить до сведения работников оператора положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; 3) организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов	В определенных случаях организация должна назначить офицера по защите персональных данных. В иных случаях организации могут или, если этого требует право государства, должны назначить офицера по защите персональных данных. Офицер по защите персональных данных должен назначаться на основании профессиональных качеств, включая экспертные знания в сфере права защиты данных и практики, а также способность осуществлять поставленные перед ним задачи. Офицер по защите персональных данных может являться сотрудником контролера или процессора либо осуществлять задачи на основании договора об оказании услуг. Субъекты данных могут обращаться к офицеру по защите персональных данных по всем вопросам, связанным с обработкой их персональных данных, а также осуществлением их прав. Офицер по защите персональных данных должен выполнять как минимум следующие задачи: а) информировать и давать советы организации, а также сотрудникам, которые осуществляют обработку, относительно их обязанностей по Регламенту и иным положениям о защите данных;	Лицо, ответственное за организацию обработки персональных данных, в целом аналогично офицеру по защите персональных данных. За исключением факта, что в GDPR офицер обязан выбираться на основании его профессиональных знаний и возможности выполнения поставленных перед ним задач, в Федеральном законе «О персональных данных» таких уточнений нет. По GDPR в некоторых случаях офицер может не назначаться; по Федеральному закону «О персональных данных» лицо, ответственное за организацию обработки персональных данных, назначается обязательно

Окончание табл. 4

Требования	ФЗ «О персональных данных»	GDPR	Общее и различия
		b) осуществлять мониторинг соблюдения Регламента, иных положений о защите данных и политик организации в отношении защиты персональных данных, в том числе распределения обязанностей, повышения осведомленности и обучения персонала, занятого в обработке данных, а также относительно аудита; c) давать рекомендации, когда они запрашиваются, относительно оценки воздействия на защиту данных, а также осуществлять мониторинг их выполнения; d) сотрудничать с надзорным органом; e) действовать в качестве контактного центра для надзорного органа по вопросам, относящимся к обработке	
13. Ответственность за нарушение требований	Лица, виновные в нарушении требований, несут предусмотренную законодательством РФ ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков	За любое нарушение требований GDPR накладывается штраф	GDPR содержит конкретный перечень нарушений и соответствующих штрафов, достигающих 20 млн евро

Контрольные вопросы

1. На смену какому документу ЕС пришел GDPR?
2. Перечислите, на кого и в каких случаях будет распространяться действие GDPR.
3. В каких случаях компании должны назначать представителя в ЕС?
4. Кто может быть назначен представителем компании в ЕС?
5. Кто такой контролер по GDPR?
6. Кто такой процессор по GDPR?
7. Какие элементы должен содержать договор (иной правовой акт) между контролером и процессором?
8. Перечислите основные принципы обработки персональных данных по GDPR. В чем отличие от российского закона «О персональных данных»?
9. Что такое обработка персональных данных, не требующая идентификации?
10. Какие требования к согласию субъекта персональных данных предъявляет GDPR? В чем отличие от российского законодательства?
11. В чем различие между GDPR и Федеральным законом «О персональных данных» в части предоставления информации субъекту персональных данных?
12. Что понимается по «правом субъекта на доступ к данным»?
13. Что понимается под «правом субъекта на изменение, удаление персональных данных»? В чем заключается отличие от российского законодательства?
14. Что понимается под «правом на переносимость данных»? Есть ли аналог в российском праве?
15. Что понимается под защитой «by design» и «by default»?
16. Что такое псевдонимизация, какими свойствами она обладает?
17. В каких случаях и в какие сроки необходимо уведомлять об утечке персональных данных? Что необходимо включить в уведомление? Есть ли аналогичное требование в российском законодательстве?

18. Какие требования предъявляются к учетным записям обработки персональных данных?

19. Что такое DPIA? Опишите алгоритм ее проведения.

20. Каков размер штрафов по GDPR и каковы условия их наложения? В какой пропорции соотносятся размеры штрафа по GDPR со штрафами по КоАП РФ?

Кейсы

Кейс 1. *Уведомление регулятора об утечке данных*

В крупной российской холдинговой компании Т. произошла утечка персональных данных.

Работником одной из входящих в холдинговую структуру компаний был получен доступ ко всей базе персональных данных работников, произведено ее скачивание к себе на компьютер и передача конкурентам.

Опишите порядок действий службы информационной безопасности. В какие сроки служба информационной безопасности обязана уведомить Роскомнадзор и что должна отразить в данном уведомлении?

Кейс 2. *Услуги телемедицины*

Немецкая компания TeleMedizin GMBH (наименование вымышленное) осуществляет деятельность по оказанию консультационных услуг в области медицины с использованием телекоммуникационных технологий. При этом врачи обмениваются снимками, медицинской документацией, видеоизображениями пораженных частей тела, электронными версиями различных документов, а также осуществляют консультации при помощи Интернета и проводят различные видеоконференции.

Сбор и хранение персональных данных пациентов из России осуществляется российским юридическим лицом ООО «ТМ-Клиника», зарегистрированным и осуществляющим свою деятельность на территории города Екатеринбурга. Серверы баз данных также находятся в Екатеринбурге.

При этом при передаче информации для постановки диагноза и (или) формулирования рекомендаций передаются

только данные, касающиеся клинической симптоматики, наблюдаемой или описываемой конкретным пациентом и (или) диагностируемой врачом ООО «ТМ-Клиника». Например, истории болезни, содержащие только возраст пациента без ФИО и иной идентифицирующей его информации, рентгеновские снимки и (или) видеоизображения пораженных частей тела (не являются биометрическими персональными данными, так как не используются оператором для установления личности) и т.п.

При проведении видеоконсультаций также происходит процесс обезличивания персональных данных — ФИО и иные личные данные пациента врачу также не сообщаются. Он знает лишь номер и имя пациента (которое сообщит сам пациент, может быть вымышленное) и не производит установления личности по передаваемому видеоизображению.

Необходимо подготовить политику в области обработки персональных данных для размещения на официальном сайте организации с учетом требований Федерального закона «О персональных данных» и GDPR.

Кейс 3. *Проведение DPIA*

Проведите Data protection impact assessment для указанной в кейсе 2 копании.

Вместо заключения

Трансформация института персональных данных в условиях цифровой экономики

Исторически выделившись из правового института неприкосновенности частной жизни, персональные данные в настоящее время проходят этап трансформации в совершенно отдельный, самостоятельный институт права. Катализатором указанного процесса должно стать развитие так называемого «информационного общества».

Информационное общество — общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.

Сформулированная государством стратегия роста использования информационных ресурсов в жизни граждан неуклонно приведет к тому, что данные гражданина, позволяющие установить его личность, в ближайшем будущем не смогут составлять тайну частной жизни, так как обмен этими данными будет осуществляться повсеместно.

Необходимо различать два понятия — персональные данные и тайна частной жизни. Тайна частной жизни (личная и семейная тайна) — достаточно широкое понятие, не получившее нормативного закрепления и в ряде случаев охватывающее персональные данные. В то же время отдельно взятые факты о лице, такие как фамилия, имя, отчество, место работы, адрес и т.п., а также сведения о большинстве повседневных событий, связанных с этим лицом, в большинстве случаев не могут быть тайной, поскольку по своему характеру являются неотъемлемым элементом коммуникаций человека.

Библиографический список

1. *Конституция* Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ).

2. *Всеобщая* декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948).

3. *Международный* пакт от 16.12.1966 «О гражданских и политических правах».

4. *Конвенция* Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108) (заключена в г. Страсбурге, 28 января 1981 г.).

5. *Гражданский* кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 31.12.2014).

6. *Кодекс* Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.08.2018).

7. *Налоговый* кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 29.12.2014).

8. *Семейный* кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 04.11.2014).

9. *Трудовой* кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 31.12.2014).

10. *Уголовный* кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 05.05.2014).

11. *О банках* и банковской деятельности: закон РФ от 02.12.1990 № 395-1 (ред. от 29.12.2014).

12. *О государственной* тайне: закон РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013).

13. *Об информации*, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003).

14. *О Федеральной* службе безопасности: федер. закон от 03.04.1995 № 40-ФЗ (ред. от 22.12.2014).

15. *О международных* договорах Российской Федерации: федер. закон от 15.07.1995 № 101-ФЗ (ред. от 12.03.2014).

16. *Об оперативно-розыскной* деятельности: федер. закон от 12.08.1995 № 144-ФЗ (ред. от 21.12.2013).

17. *О Всероссийской* переписи населения: федер. закон от 25.01.2002 № 8-ФЗ (ред. от 02.07.2013).

18. *О техническом* регулировании: федер. закон от 27.12.2002 № 184-ФЗ (ред. от 23.06.2014).

19. *О связи:* федер. закон от 07.07.2003 № 126-ФЗ (ред. от 21.07.2014, с изм. от 01.12.2014).

20. *О коммерческой* тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014).

21. *Об архивном* деле в Российской Федерации: федер. закон от 22.10.2004 № 125-ФЗ (ред. от 04.10.2014).

22. *О ратификации* Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ.

23. *О персональных* данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014).

24. *Об информации*, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014).

25. *О защите* прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля: федер. закон от 26.12.2008 № 294-ФЗ (ред. от 31.12.2014).

26. *Об организации* предоставления государственных и муниципальных услуг: федер. закон от 27.07.2010 № 210-ФЗ (ред. от 31.12.2014).

27. *Об обязательном* медицинском страховании в Российской Федерации: федер. закон от 29.11.2010 № 326-ФЗ.

28. *Об электронной* подписи: федер. закон от 06.04.2011 № 63-ФЗ (ред. от 28.06.2014).

29. *О внесении* изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ.

30. *Об основах* охраны здоровья граждан в Российской Федерации: федер. закон от 21.11.2011 № 323-ФЗ (ред. от 08.03.2015).

31. *О бухгалтерском* учете: федер. закон от 06.12.2011 № 402-ФЗ (ред. от 04.11.2014).

32. *О внесении* изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных»: федер. закон от 07.05.2013 № 99-ФЗ (ред. от 28.12.2013).

33. *О внесении* изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: федер. закон от 21.07.2014 № 242-ФЗ (ред. от 31.12.2014).

34. *Об утверждении* Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005).

35. *Об утверждении* Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела: указ Президента РФ от 30.05.2005 № 609 (ред. от 01.07.2014).

36. *О мерах* по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента РФ от 17.03.2008 № 351 (ред. от 25.07.2014).

37. *О стратегии* развития информационного общества в Российской Федерации на 2017–2030 гг.: указ Президента РФ от 09.05.2017 № 203.

38. *О подписании* Конвенции о защите физических лиц при автоматизированной обработке персональных данных: распоряжение Президента РФ от 10.07.2001 № 366-рп.

39. *Об утверждении* Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии: постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012).

40. *Об утверждении* требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных: постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012).

41. *Об утверждении* Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства РФ от 15.09.2008 № 687.

42. *Об утверждении* требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 № 1119.

43. *Об утверждении* перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014).

44. *О плане* подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»: распоряжение Правительства РФ от 15.08.2007 № 1055-р.

45. *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 Российской Федерации в области персональных данных: приказ Роскомнадзора от 01.12.2009 № 630.

46. *Об утверждении* Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных: приказ Роскомнадзора от 19.08.2011 № 706 (ред. от 14.03.2014).

47. *Об утверждении* Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»: приказ Минкомсвязи России от 21.12.2011 № 346 (ред. от 24.11.2014).

48. *О Консультативном* совете при уполномоченном органе по защите прав субъектов персональных данных: приказ Роскомнадзора от 20.06.2012 № 621.

49. *Об утверждении* Положения об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций: приказ Роскомнадзора от 03.12.2012 № 1255.

50. *Об утверждении* Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17.

51. *Об утверждении* Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21.

52. *Об утверждении* состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: приказ ФСБ России от 10.07.2014 № 378.

53. *Об утверждении* унифицированных форм первичной учетной документации по учету труда и его оплаты: постановление Госкомстата РФ от 05.01.2004 № 1.

54. *Об утверждении* Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных

органов, органов местного самоуправления и организаций, с указанием сроков хранения: приказ Минкультуры России от 25.08.2010 № 558.

55. *О применении* судами Российской Федерации Трудового кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 17.03.2004 № 2 (ред. от 28.09.2010).

56. *Определение* об отказе в передаче дела в Президиум Высшего Арбитражного Суда Российской Федерации от 04.10.2012 № ВАС-12575/12.

57. *Постановление* Федерального Арбитражного Суда Уральского округа от 26.06.2012 № Ф09-4994/12.

58. *Постановление* Семнадцатого Арбитражного Апелляционного Суда от 14.03.2012 № 17АП-1205/2012-АК.

59. *Решение* Арбитражного суда Астраханской области по делу № А061975/2011 от 24.06.2011.

60. *Решение* Арбитражного Суда Новгородской области по делу № А441867/2011 от 22.07.2011.

61. *Решение* Арбитражного Суда Свердловской области по делу № А6041475/2011 от 26.12.2011.

62. *Авдеев М. Ю.* Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. № 1. С. 49–54.

63. *Алексеев С. С.* Структура советского права. М.: Юрид. лит., 1975. 264 с.

64. *Алистархов В.* Выбор вида наказания работнику за разглашение сведений с ограниченным доступом // Трудовое право. 2014. № 9. С. 37–48.

65. *Амелин Р. В., Богатырева Н. В., Волков Ю. В. и др.* Комментарий к Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (постатейный) // СПС «КонсультантПлюс».

66. *Бадьина А.* Обработка, порядок хранения и передвижения персональных данных // Кадровик. Кадровое делопроизводство. 2012. № 1. С. 162–171.

67. *Бархатова Е. Ю.* Комментарий к Конституции Российской Федерации (постатейный). 2-е изд., перераб. и доп. М.: Проспект, 2015. 272 с.

68. *Борисов А. Н.* Первичные документы: оформление, использование, хранение, выбытие. М.: Юстицинформ, 2007. 336 с.

69. *Давыдова Е. В.* Что работодателю необходимо знать о персональных данных работников? // Отдел кадров коммерческой организации. 2015. № 3. С. 33–42.

70. *Егорова О. А., Беспалов Ю. Ф.* Настольная книга судьи по трудовым делам: учеб.-практ. пособие. М.: Проспект, 2013. 248 с.

71. *Заведенская А. А.* Влияние GDPR на российских операторов персональных данных. URL: https://www.ussc.ru/news/id/400/ (дата обращения: 24.08.2018).

72. *Ипатов А. Б.* К вопросу о месте страхового права в системе права // Юрист. 2005. № 7. С. 7–14.

73. *Изменения* в порядке обработки персональных данных в информационно-телекоммуникационных сетях в 2015 г. // СПС «КонсультантПлюс».

74. *Кайль А. Н., Новиков Е. А.* Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный) // СПС «КонсультантПлюс».

75. *Ковалева Н. Н., Холодная Е. В.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный) // СПС «КонсультантПлюс».

76. *Ковалева Н. Н.* Информационное право России: учеб. пособие. М.: Дашков и К°, 2007. 360 с.

77. *Кодекс* Российской Федерации об административных правонарушениях. Главы 11–18. Постатейный научно-практический комментарий / И. А. Аксенов, С. Н. Антонов, О. В. Гречкина и др.; под общ. ред. Б. В. Россинского. М.: Библиотечка «Российской газеты», 2014. Вып. 9–10. 880 с.

78. *Комментарий* к Кодексу Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (постатейный) / Р. В. Амелин, Е. А. Бевзюк, Ю. В. Волков и др. // СПС «КонсультантПлюс».

79. *Комментарий* к Трудовому кодексу Российской Федерации (постатейный) / С. Ю. Головина, А. В. Гребенщиков, Т. В. Иванкина и др.; под ред. А. М. Куренного и др. 3-е изд., пересмотр. М.: НОРМА; ИНФРА-М, 2015. 848 с.

80. *Комментарий* к Трудовому кодексу Российской Федерации (постатейный) / М. А. Бочарникова, З. Д. Виноградова, А. К. Гаврилина и др.; отв. ред. Ю. П. Орловский. 6-е изд., испр., доп. и перераб. М.: ИНФРА-М, 2014. 1680 с.

81. *Комментарий* к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков и др.; под ред. А. В. Бриллиантова. 2-е изд. М.: Проспект, 2015. Т. 1. 792 с.

82. *Королев А. Н., Плешакова О. В.* Комментарий к Федеральному закону «Об информации, информационных технологиях и о защите информации» (постатейный). М.: Юстицинформ, 2007. 128 с.

83. *Конституция* Российской Федерации. Доктринальный комментарий (постатейный) / М. П. Авдеенкова, А. Н. Головистикова,

Л. Ю. Грудцына и др.; науч. ред. Ю. И. Скуратов. 2-е изд., изм. и доп. М.: Статут, 2013. 688 с.

84. *Киримова Е. А.* Правовой институт. Понятие и виды: учеб. пособие / под ред. И. Н. Сенякина. Саратов: Саратов. гос. акад. права, 2000. 55 с.

85. *Кистяковский Б. А.* Государственное право (общее и русское). М., 1908–1909.

86. *Покровский И. А.* Основные проблемы гражданского права. Пг.: Право; Правда, 1917.

87. *Кротов А. В.* Некоторые аспекты права на неприкосновенность частной жизни при реализации информационных прав // Законодательство и экономика. 2013. № 4. С. 51–54.

88. *Кузнецова Т. В.* Организация работы с персональными данными // Трудовое право. 2011. № 5. С. 77–83.

89. *Курбатов А. Я.* Защита прав и законных интересов в условиях «модернизации» правовой системы России. М.: Юстицинформ, 2013. 172 с.

90. *Кухаренко Т. А.* Комментарий к Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (постатейный) // СПС «КонсультантПлюс».

91. *Лаптев В. В., Шахматов В. П.* Цели правового регулирования и система права // Правоведение. 1976. № 4. С. 26–35.

92. *Левина М. И.* Система российского законодательства теоретическая конструкция и действующая модель. URL: http://ecsocman.hse.ru/data/165/680/1219/004.LEVINA.pdf.

93. *Максимов И. В.* Административные наказания. М.: Норма, 2009. 464 с.

94. *Медведева Т. М.* О работе с персональными данными работников // Актуальные вопросы бухгалтерского учета и налогообложения. 2014. № 21. С. 77–88.

95. *Панкова О. В.* Рассмотрение в судах общей юрисдикции дел об административных правонарушениях. М.: Статут, 2014. 440 с.

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

97. *Поворова Е. А.* Проблемы «управления» информацией в государственных органах исполнительной власти // Информационное право. 2008. № 2. С. 33–34.

98. *Путеводитель* по кадровым вопросам. Персональные данные работников // СПС «КонсультантПлюс».

99. *Новиков В. А.* Неприкосновенность частной жизни как конституционное право и объект уголовно-правовой охраны // Юридический мир. 2014. № 7. С. 18–21.

100. *Разъяснения* Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакант-

ных должностей, а также лиц, находящихся в кадровом резерве». URL: http://rkn.gov.ru.

101. *Разъяснения* Роскомнадзора «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки». URL: http://25.rsoc.ru.

102. *Савельев А. И.* Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. № 9. С. 51–68.

103. *Серков П. П.* Административная ответственность в российском праве: современное осмысление и новые подходы. М.: ИНФРА-М, 2012. 480 с.

104. *Саматов К. М.* Персональные данные работников организации и их защита: учеб. пособие. S.l.: Изд. решения, 2016. 88 с.

105. *Саматов К. М.* Как подготовиться к проверке регулятора по персональным данным (пошаговая инструкция) // Information Security (Информационная безопасность). 2016. № 6. С. 45–47.

106. *Свирин Ю. А.* Дивергенция в системе права: монография. М.: Астра Полиграфия, 2012. 392 с.

107. *Ситникова Е. Г., Сенаторова Н. В.* Трудовой договор: некоторые основания прекращения. М.: Библиотечка «Российской газеты», 2014. Вып. 2. 192 с.

108. *Ситникова Е. Г., Сенаторова Н. В.* Трудовой кодекс Российской Федерации. Раздел III. Трудовой договор: постатейный науч.-практ. ком. М.: Библиотечка «Российской газеты», 2013. Вып. 7–8. 720 с.

109. *Ситникова Е. Г., Сенаторова Н. В.* Расторжение трудового договора по инициативе работодателя (п. 1–6 ч. 1 ст. 81 Трудового кодекса РФ). М.: Библиотечка «Российской газеты», 2013. Вып. 1. 192 с.

110. *Терещенко Л. К.* Доступ к информации: правовые гарантии // Журнал российского права. 2010. № 10. С. 46–53.

111. *Терещенко Л. К.* Модернизация информационных отношений и информационного законодательства. М.: ИНФРА-М, 2013. 227 с.

112. *Терещенко Л. К.* Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3–13.

113. *Терещенко Л. К., Тиунов О. И.* Правовой режим персональных данных // Журнал российского права. 2014. № 12. С. 42–49.

114. *Хужокова И. М.* Эволюция содержания права на неприкосновенность частной жизни в России // Адвокатская практика. 2006. № 4. С. 2–5.

115. *Якушев В. С.* О понятии правового института // Правоведение. 1970. № 6. С. 62–63.

Учебное издание

Назаров Дмитрий Михайлович,
Саматов Константин Михайлович

Основы обеспечения безопасности персональных данных в организации

Учебное пособие

Редактор и корректор *Л. В. Матвеева*
Компьютерная верстка *М. Ю. Ворониной*

Поз. 13. Подписано в печать 30.05.2019.
Формат 60 × 84/16. Гарнитура школьная. Бумага офсетная.
Печать плоская. Уч.-изд. л. 5,4. Усл. печ. л. 7,0. Печ. л. 7,5.
Заказ 351. Тираж 38 экз.
Издательство Уральского государственного экономического университета
620144, Екатеринбург, ул. 8 Марта/Народной Воли, 62/45

Отпечатано с готового оригинал-макета
в подразделении оперативной полиграфии
Уральского государственного экономического университета