МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Предпринимательское и трудовое право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Защита персональных данных работника

Студент Д.Г. Смирнова
(И.О. Фамилия) (личная подпись)

Научный руководитель кандидат юридических наук, доцент Е.В. Чуклова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Оглавление

Введение

Актуальность и научная значимость настоящего исследования. С развитием информационных технологий и внедрением их в повседневную жизнь и работу общества, появляются новейшие средства обработки данных в организациях. Подавляющее большинство предприятий, так или иначе, вынуждены использовать информационные системы, чтобы быть наиболее конкурентоспособными и оптимизировать рабочий процесс сотрудников.

Однако при всей необходимости и полезности таких систем существует обратная сторона. С развитием технологий обработки, хранения, передачи данных, также развиваются технологии их кражи, неправомерной огласки. Все это заставляет организации серьезно подходить к вопросу защиты данных, потому что от этого зависит не только доход, но и престиж компании. Особо стоит выделить среди данного многообразия информации персональные данные. В целях регулирования отношений между субъектами и операторами персональных данных, был разработан и принят федеральный закон № 152-ФЗ от 14 июля 2006 «О персональных данных» [25].

Согласно данному закону, персональные данные – это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу. Кроме этого, оператор – это 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. Таким образом, любая организация уже берет на себя обязательства по сохранению персональных данных. Также не маловажным фактом является обязательное выполнение требований данного нормативного акта.

Среди множества компаний стоит обратить внимание на операторов услуг связи. Данные предприятия обширно работают с абонентами и стремятся постоянно расширить клиентскую базу, из-за чего накапливают персональные данные не только сотрудников, но и потребителей. Поэтому вопрос о правильном соблюдении требований законодательства в области обработки персональных данных стоит наиболее актуально в компании.

Проблемы функционирования систем обеспечения информационной безопасности нашли отражение в трудах А.А. Герасимова, А.А. Грушо, С.В. Дворянкина, В. А. Минаева, С.В. Скрыля, М.П. Сычева и ряда других ученых.

Проблематикой правового регулирования персональных данных работников занималось довольно большое число ученых (А.Б. Агапов, И.Л. Бачило, Л.А. Василенко, Е.К. Волчинская, С.А. Глотов, А.В. Дворецкий, Д.В. Иванов, А.В. Кучеренко, М.В. Лушникова, А.С. Маркевич, Л.А. Сергиенко, И.Л. Петрухин, А.А. Фатьянов и другие), тем не менее данная тема по-прежнему недостаточно исследована.

Проблемы защиты персональных данных рассматривались в трудах российских ученых, таких как: А.В Меньшиковой, где она выделила некоторые проблемы защиты персональных данных работника и определила перспективы и пути их решения; проблемные вопросы понятия и сущности персональных данных в своих трудах рассмотрел А.В Минбалеев.

Диссертационные исследования института персональных данных проводились Ф.А. Абаевым, И.Л. Вельдер, А.В. Дворецким, Н.И. Петрыкиной, Ю.С. Телиной, А.С. Маркевич, Е.Ю. Покаместовой, А.С. Федосиным.

Тема диссертации актуальна, так как лица, ответственные за обработку персональных данных не всегда знают элементарных правил безопасности, доверенной им информации. Поэтому на специалистов по информационной безопасности возлагается не только ответственность за безопасность информационной системы, но система обучения персонала.

Объект исследования – отношения по организации защиты данных работника.

Предмет исследования – совокупность правовых норм, регулирующих отношения в сфере защиты персональных данных.

Целью диссертации является анализ организации защиты персональных данных работников.

Гипотеза исследования состоит в том, что если будет реализован разработанный в диссертации комплекс мероприятий по защите персональных данных, то уровень защищенности персональных данных значительно повысится.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить понятие и состав персональных данных;
2. Охарактеризовать становление института персональных данных в России и мире;
3. Проанализировать регламентирование деятельности работодателя по обработке, хранению, передаче и защите персональных данных работника;
4. Изучить особенности защиты персональных данных работника;
5. Дать характеристику современным условиям защиты персональных данных работника;
6. Проанализировать проблемы защиты персональных данных работника, а также перспективы и пути решения;
7. Проанализировать проблема ответственности за нарушение правил работы с персональными данными.

Теоретико-методологическую основу исследования составили современные методы научного познания, общенаучный метод познания объективной действительности. Применялись также дедукция, индукция, сравнительный, исторический, логический, системный, документальный и прочие научные методы.

Научная новизна исследования заключается в практических рекомендациях, предлагаемых автором в качестве устранения проблем правовой защиты персональных данных.

Теоретическая значимость исследования заключается в том, что сформулированные автором теоретические выводы, практические рекомендации и предложения вносят определенный вклад в правовую науку, систематизируют научные знания по вопросам правового регулирования защиты персональных данных, а также могут быть использованы в дальнейших научных изысканиях.

Практическое значение исследования состоит в том, что сформулированные в нем выводы и предложения могут быть использованы в ходе дальнейшего реформирования правовых основ защиты персональных данных.

Нормативной базой исследования стали Конституция Российской Федерации, федеральные конституционные законы, федеральные законы, международные правовые акты о правах человека в сфере защиты персональных данных, Указы Президента Российской Федерации и др.

Основные положения, выносимые на защиту:

1. Автором предложено следующее определение персональных данных работника: персональными данными работника являются сведения индивидуального характера об определенном работнике (работниках), которые основаны на законе, предъявляемые работнику работодателем в определенных целях, способствующих трудоустройству работника и защищаемые способами, предусмотренными действующим законодательством, в целях запрета несанкционированного распространения персональных данных работника.

2. Нормативно-правовое обеспечение защиты персональных данных представлено достаточно разветвленной системой правовых актов. Нормы материального права находят свое отражение в Конституции РФ, Федеральном законе «О персональных данных» и Трудовом кодексе РФ,

нормы процессуального права в подзаконных нормативных актах: Указы Президента РФ, Постановления Правительства РФ, приказы ФСТЭК России, ФСБ России. При этом, немаловажная роль отведена локальным нормативным актам, издаваемым операторами персональных данных. На практике, именно они определяют конкретные процедуры обработки персональных данных работников в организации.

3. Система защиты персональных данных включает в себя меры организационного и технического характера, которые определяются с учетом актуальных угроз безопасности для персональных данных и информационных технологий, используемых в системе обработки информации организации.

4. Создание единого информационного пространства является глобальной идеей о том, как в рамках одной программы объединить не только всю информацию о работниках, но и максимально закрыть доступ к такой информации для служащих, которые не уполномочены осуществлять работу с такой информацией. Безусловно, положительными чертами предлагаемой системы является наличие специальных компетентных работников, которые будут в строгом соответствии осуществлять работу с системой и нести за это ответственность, минусом данной системы будет являться необходимость обучить персонал качественной работе с такой системой, также предоставить доступ к информации программистам, которые будут осуществлять программное сопровождение, но представителей сторонних организаций можно всегда путем повышения квалификации заменить на работников организации. В свете предложенного в рамках представленного исследования был разработан ряд предложений по совершенствованию законодательства в области защиты персональных данных.

5. По мнению автора представленного исследования на сегодняшний день необходимо создание оптимального правового механизма обороты и защиты персональных данных работника. Решение данной

проблемы в должном ключе предполагает обширный мониторинг состояния современного рынка информационных технологий, IT - продуктов, услуг, отслеживания общих тенденций развития информационного общества Российской Федерации. Исследуемый рынок не стоит на месте, работодателю предлагаются все новые и новые системы для обработки, хранения и работы с персональными данными, каждый работодатель заинтересован в ведении своей деятельности соблюдая нормы действующего законодательства и поэтому в первую очередь работодатель должен быть заинтересован в лицензировании и «легальности» предлагаемых программ.

6. Статья 90 Трудового кодекса РФ за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, предусматривает дисциплинарную, административную, гражданско-правовую и уголовную ответственность.

Личный вклад автора в организацию и проведение исследования состоит в непосредственном участии во всех этапах диссертационного исследования, в планировании научной работы, наборе материала, углубленном анализе отечественной и зарубежной научной литературы, анализе и интерпретации полученных данных, их систематизации, статистической обработке с описанием полученных результатов, написании и оформлении рукописи диссертации, основных публикаций по выполненной работе.

Апробация и внедрение результатов работы велись в течение всего исследования. Основные теоретические и практические выводы, сформулированные в результате проведенного исследования, были:

1. Обсуждены на международной научно-практической конференции «Актуальные проблемы права и правоприменения», 21-22 ноября 2019 года, по адресу: Самарская область, г. Тольятти, ул. Ушакова, д. 57, корпус Э (в здании Института права ТГУ).

2. Отражены в публикациях автора (Смирнова Д.Г. Организация режима защиты конфиденциальной информации на предприятии // Молодой ученый. – 2020. - № 5 (295). – С. 229-232).

Структура магистерской диссертации. Работа состоит из введения, трех глав, заключения, списка используемой литературы и используемых источников.

Глава 1 Персональные данные: общая характеристика

1.1 Понятие и состав персональных данных

Понятие «конфиденциальность» является дискуссионным вопросом в современном обществе. Связанное с этой категорией понятие «персональные данные» не менее спорно и неопределенно. XXI век открывает перед человечеством новые горизонты – технологии развиваются высокими темпами, с огромной скоростью врываясь в жизнь обычного человека. И тем значимее становится вопрос защиты персональных данных человека (и в частности, работника) в современном мире. Так, например, работодатели сегодня используют современную технику для организации аудио- и видеоконтроля на рабочем месте. При организации такого рода контроля могут быть нарушены права граждан (в нашем случае – работников). В частности, такими правами (заметим – конституционными), которые могут быть прямо или косвенно нарушены работодателем при организации аудио- и видеоконтроля, являются:

– право на неприкосновенность частной жизни, личную и семейную тайну (ст. 23 Конституции Российской Федерации (далее – Конституция РФ [15]));

– право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (хотя судебная практика «говорит», что «тайна связи имеет совершенно иной правовой статус, чем персональные данные») (ст. 23 Конституции РФ);

– запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24 Конституции РФ);

– можно усмотреть косвенное нарушение ст. 17 Конституции РФ, согласно которой «в Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права (курсив наш – В.С.) и в

соответствии с настоящей Конституцией». Дело в том, что во Всеобщей декларации прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948 г.) [9] закрепляются права человека, имеющие непосредственное отношение к нашей проблеме, как-то: на личную неприкосновенность (ст. 3), никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» (ст. 12).

Следует заметить, что само понятие персональных данных в Трудовом Кодексе РФ [52] (далее – ТК РФ) не раскрывается. Содержащееся ранее в статье 85 ТК РФ понятие персональных данных работника не раз подвергалось критике со стороны научного сообщества.

Действительно, основания для критики имелись. Понимание персональных данных как «информации, необходимой работодателю в связи с трудовыми отношениями» было слишком широким [11].

В 2013 г. понятие персональных данных работника было исключено из ТК РФ, в том числе, в связи с принятием Федерального закона от 27.07.2006 г. «О персональных данных» [26]. Содержащееся в данном Федеральном законе понятие персональных данных по справедливому замечанию А.В. Дворецкого не учитывает специфики трудовых отношений [7, С. 32]. Судебная практика относит к персональным данным работников фамилию, имя, отчество и место жительства физического лица [27].

Считаем данный перечень недостаточно полным.

Как нам кажется, наше трудовое законодательство не содержит общих положений о персональных данных работников, ограничиваясь частными сферами (обработки, хранения и т.п.). В связи с этим, нам видится целесообразным включение в ТК РФ: во-первых, понятия персональных данных, которое подразумевало бы под собой «любую информацию, которая

связана или может быть связана с личной или профессиональной жизнью работника, а также информацию, которая позволит ее обладателю персонифицировать работника»; во-вторых, было бы целесообразно выделить общие принципы работы с персональными данными [54, С. 737]. Понятие «обработка персональных данных» следовало бы заменить на понятие «работа с персональными данными».

Одним из возможных вариантов видится изменение структуры ТК РФ в части, связанной с персональными данными. Возможно, следовало бы выделить регулирование персональных данных в отдельный раздел ТК РФ, в рамках которого выделить отдельные главы, посвященные общим вопросам (таким, как сама дефиниция персональных данных), вопросам обращения с персональными данными, представленными в электронном варианте, на бумажных носителях и т.д. Подобного рода изменения подчеркнут важность вопроса защиты персональных данных и, в целом, будут соответствовать духу времени [19, С. 15].

Используя в качестве основы теорию права, можно проанализировать институт персональных данных. Предметом института персональных данных являются общественные отношения, связанные с их обработкой. Данная обработка может производиться муниципальными и государственными органами, юридическими и физическими лицами. В процессе обработки могут применяться средства автоматизации, включая информационно-телекоммуникационные сети и вычислительную технику. Также обработка может производиться без различных средств автоматизации. Однако обязательным является защита от неправомерного доступа к персональным данным, уничтожения или их блокирования, что подразумевает конфиденциальность, целостность и доступность информации.

Институт персональных данных оперирует достаточно широким набором понятий. Например, в статье 3 Федерального закона «О персональных данных» раскрыто содержание ключевых определений, в число которых входит само понятие персональных данных, понятие

оператора, понятие обработки персональных данных, содержание понятий «автоматизированная обработка персональных данных», «обезличивание персональных данных», «информационная система персональных данных», «трансграничная передача персональных данных» и многие другие.

Помимо этого, институт персональных данных и всю связанную с ним сферу в настоящее время можно считать относительно обособленной. Она располагает широким спектром источников, которые включают различные нормы материального права на уровне федеральных законов и нормы процессуального права на уровне подзаконных нормативных актов. Они описывают все процедуры, которые входят в состав обязательных при обработке персональных данных оператором с целью защиты обрабатываемой информации.

В Федеральном законе № 197-ФЗ «Трудовой кодекс Российской Федерации» от 30.12.2001 под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ч.1 ст.85 ТК РФ).

В статье 5 закона «О персональных данных» установлены шесть ключевых принципов, лежащих в основе обработки персональных данных. К числу таковых относятся.

1. Добросовестность обработки персональных данных, законность способов и целей их обработки.

2. Цели обработки персональных данных должны соответствовать тем целям, которые были заранее определены и заявлены при их сборе. Также полномочия оператора должны соответствовать всем заявленным параметрам.

3. Объем персональных данных, способ обработки и характер обрабатываемых персональных данных должен соответствовать целям обработки.

4. Недопустимой является обработка данных, которые являются избыточными по отношению к заявленным при сборе данных целям.

Достоверность и достаточность персональных данных для целей обработки являются обязательным требованием.

5. Объединение информационных баз персональных данных, которые были созданы для несовместимых между собой целей, является недопустимым.

6. Форма хранения персональных данных должна позволять определять субъекта этих данных. Кроме того, срок хранения данных не должен превышать сроки, определенные целями их обработки. Персональные данные должны быть уничтожены после того, как будут достигнуты цели их обработки, а также при отсутствии необходимости в их достижении.

Все вышеперечисленные принципы обработки персональных данных должны применяться во всех видах правоотношений. В их состав могут быть включены и гражданские, и трудовые, и процессуальные правоотношения. Также принципы применяются независимо от оператора, осуществляющего обработку.

Стоит отметить, что институт защиты персональных данных использует по большей части императивный метод регулирования. Данный вывод базируется на анализе перечисленных в ст. 5 ФЗ № 152 принципов и условий, а также на основе анализа подзаконных и иных НПА, которые были изданы в соответствии с указанным законом.

Таким образом, рассмотрев весь объем правовых норм, которые регулируют общественные отношения в области обработки и защиты персональных данных, можно утверждать, что она имеет все признаки, которые характеризуют ее как самостоятельный правовой институт, обладающий отличительными чертами.

Обращение к классификации позволит определить место указанного института в системе права России. Право делится на частное и публичное, материальное и процессуальное. Институт персональных данных можно отнести к публичной отрасли права, что подтверждает анализ, проведенный

выше. При этом, ряд норм указанного института можно найти в трудовом праве, которое традиционно относится к частной отрасли [45, С. 18-20].

Институт защиты персональных данных связан с регулированием общественных отношений, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому, институт персональных данных следует рассматривать в качестве самостоятельного межотраслевого института права.

Сказанное позволяет сделать вывод, что институт персональных данных представляет собой сложно-структурный элемент информационного законодательства, обладающий институциональным единством в силу неразрывной связи с человеком, но имеющий в качестве вектора своего развития усиление внутренней дифференциации, отражающей многообразие этой информации.

1.2 Становление института персональных данных в России и мире

Вопрос роли и места института персональных данных в системе права, на текущем этапе является недостаточно изученным и очень актуальным. Стоит отметить, что в юридической науке практически полностью отсутствуют работы, направленные на его изучения, даже несмотря на особую значимость изучаемого института с практической точки зрения.

На наш взгляд, возможными причинами послужили следующие. Во-первых, большинство экспертов и специалистов защиту персональных данных понимают только как техническую задачу, которая включает следующие аспекты: защита от несанкционированного доступа и от кражи, защита от утечки информации по техническим каналам и так далее. В данной позиции происходит изменение полюса внимания в исключительно техническую область. Стоит отметить, что защита персональных данных – это, прежде всего, защита прав субъекта (физического лица). А именно, того

лица, которое владеет и предоставляет свои персональные данные частной организации либо государственному органу.

Во-вторых, нормы, которые регулируют обработку персональных данных, принято считать частью института неприкосновенности частной жизни, что также может являться возможной причиной.

Институт персональных данных является достаточно молодым по правовым меркам. В первую очередь, его становление очень тесно связывают с развитием прав и свобод человека, его правом на неприкосновенность частной жизни.

Английский термин «privacy» обозначает все стороны частной жизни и не имеет буквального эквивалента в русском языке. Известные американские юристы Сэмюэл Уоррен и Луис Брандейс в конце 19 века одними из первых попытались сформулировать суть понятия «privacy» и определили его как «the right to be alone» - право быть оставленным в покое. Они сделали вывод, что приватность ставится под угрозу посредством новейших изобретений в своей статье «Право на приватность», выпущенной в журнале о праве в Гарварде. Тем самым обозначили необходимость создания специального «права приватности» [58, С. 297].

Примерно схожие рассуждения о самостоятельности как института персональных данных в сравнении с правом на неприкосновенность частной жизни можно встретить и у целого ряда зарубежных авторов [59], что еще раз подтверждает общий вектор развития права в этом направлении, который ориентирует нас на самостоятельность правового института персональных данных.

Известно, что в европейских странах право на защиту персональных данных «выводится» из права на защиту частной жизни [61].

В дальнейшем в XX веке, судами в США была сформирована так называемая «концепция прайвеси», ставшая основой формирования права человека на неприкосновенность частной жизни. После, была принята Всеобщая Декларация прав человека, которая провозгласила «никто не

может подвергаться произвольному вмешательству в его личную и семейную жизнь...» [9]. Так выражено право на тайну личной жизни, корреспонденции, неприкосновенность чести и репутации, сообразно с правом на неприкосновенность жилища. Помимо этого обозначено право на защиту законом от такого вмешательства. В статье 8 Европейской конвенции о защите прав человека и основных свобод сказано: «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции». Данные документы закрепили право на неприкосновенность частной жизни в качестве неотъемлемого права каждого человека.

В российском законодательстве еще в дореволюционный период были закреплены некоторые элементы права на неприкосновенность частной жизни. Например, Телеграфный устав 1876 г. закреплял тайну корреспонденции, Уголовное Уложение 1903г. устанавливало запрет на вмешательство должностных лиц в личную и семейную жизнь человека при отправлении правосудия. После революции 1917 года и до начала политической оттепели конца 1950-1960-х гг. в законодательстве СССР закрепление прав и свобод граждан в нормативно-правовых актах носило скорее формальный характер, и, напротив вмешательство в частную жизнь людей оправдывалось мерами, необходимыми для обеспечения государственной безопасности.

Природа прав субъекта персональных данных, его личной свободы, неприкосновенность частной жизни - объемная многогранная проблема.

Развитие информационного пространства и включение России в процессы глобализации, с одной стороны, обеспечивает и поддерживает функционирование важнейших сфер жизнедеятельности общества, с другой формирует зону риска для частной жизни человека и его персональных данных [1, С. 4].

История развития законодательства о персональных данных в мире насчитывает не одно десятилетие. В ряде Конституций европейских стран с

начала 30-х годов XX века уже были закреплены нормы о защите информации личного и семейного характера (Конституция Ирландии (1937 г.), Исландии (1944 г.), Италии (1947 г.), Хартия испанцев (1945 г.) и другие [58, С. 18].

Только в 70-80-х гг. XX в. появились законодательные акты, содержащие специальные нормы о защите персональных данных работника (Швеция (1973 г.), Франция (1978 г.) и др.).

Во 70-х годах XX века в Гессене, принимается первый специальный закон о защите персональных данных, в последствии в течении 30 лет такие законы были приняты практически во всех европейских государствах. В них закреплялись реальные механизмы регулирования оборота персональных данных [46].

В 1981 г. Совет Европы принял Конвенцию о защите физических лиц при автоматизированной обработке персональных данных и Дополнительный протокол к Конвенции, касающийся наблюдательных органов и трансграничной передачи данных. Были приняты также две директивы Европейского парламента и Совета Европейского союза (Директива 95/46/ЕС от 24 октября 1995г. о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных и Директива 97/66/ЕС от 15 декабря 1997г., касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций); а также Рекомендации Комитета министров государствам - членам Совета Европы по защите неприкосновенности частной жизни в Интернете (19 февраля 1999г.). А в 2015 году выпустил рекомендации с изложением принципов, которым они должны следовать в своем национальном законодательстве в отношении обработки персональных данных наемных работников и кандидатов на рабочие места, - например, в отношении данных о состоянии здоровья или мониторинга использования средств связи на рабочем месте. Рекомендации нацелены на решение проблем с обеспечением неприкосновенности частной

жизни, возникающих в результате использования новых информационно-коммуникационных технологий.

В Российской Федерации первоначальный проект такого разрабатывался в 1998 г. Законопроект носил рабочее название «Об информации персонального характера». Но в тот период данный законопроект до рассмотрения Государственной Думой не дошел. По прошествии двух лет Советом безопасности Российской Федерации была сформирована другая рабочая группа, подготовившая окончательный вариант впоследствии принятого Федерального закона «О персональных данных» от 27.07.2006г. № 152-ФЗ, который и является основным регулятором отношений в данной сфере [5, С. 35].

Обеспечение конфиденциальности персональных данных, при помощи которых можно идентифицировать лицо – главное требование закона. Для идентификации необходимо дополнение ФИО гражданина иными персональными данными, такими как номер телефона, адрес, дата рождения. Например, ФИО совместно с датой рождения или ФИО вместе с номером телефона будут являться персональными данными, при помощи которых можно идентифицировать лицо, а сочетание даты рождения и номера телефона – нет, потому что их принадлежность к определенному лицу не установлена [6, С. 94].

В юридической литературе представлена неоднозначная классификация охраняемой законом информации (сведений). Рассмотрим несколько классификаций, приводящихся в исследованиях Копылова, Смольковой.

В.А. Копылов приводит классификацию на основании доступа к информации, т.е. открытая информация и информация ограниченного доступа [16].

Открытая информация согласно Копылову: массовая информация, информация о выборах, официальные документы, обязательно

представляемая (экземпляры документов, регистрационная и другая), научно-юридическая и пр.

Информация ограниченного доступа согласно В.А. Копылову – составляющая коммерческую тайну, государственная тайна, персональные данные и др. В.А. Копылов поясняет, что персональные данные и другая личная информация производятся в процессе повседневной деятельности, осуществлением гражданами их права на труд, медицинскую помощь, свободу слова и др. в процессе которого они предоставляют сведения о себе другим субъектам персональных данных.

Согласно И.В. Смольковой классификация защищаемой информации выглядит так [46]:

- государственная (в том числе военная) тайна;

- конфиденциальная информация (в которую входят личная, семейная, профессиональная, служебная и коммерческая тайны).

В целом в мире, по данным организации Прайваси Интернэшенал, законодательство о защите персональной информации принято более чем в 100 странах, в число которых вошла и Россия [60].

Рассмотрев несколько мнений ученых-юристов на классификацию информации, требующей защиты, мы можем сделать вывод, что правовое регулирование данной сферы общественных отношений находится в процессе развития. Углубленное изучение проблем, встающих перед учеными, обеспечивает наиболее тщательную проработку вопроса защиты персональных данных, получение более полных знаний о способах такой защиты, видах информации, нуждающихся в ней. Впоследствии на основе полученных в ходе таких исследований знаниях формируется законодательство, обеспечивающее эффективную защиту незыблемых прав человека, защиту информации имеющей определяющее значение для государственной безопасности и других ее видов. К сожалению, на данный момент нельзя утверждать, что потребности современного общества по защите личных данных удовлетворяются в полной мере. Законодательство,

регулирующее эту сферу отношений, развивается, отвечая на новые вызовы, диктуемые бурной модернизацией информационных технологий, возникновением новых правоотношений между субъектами защиты персональных данных.

Таким образом, на основе всего вышеперечисленного можно отметить широкое развитие отечественного и международного законодательства в области защиты персональных данных, его постоянное совершенствование, связанное с внедрением новых способов контроля, отслеживанием передовых технологий сбора, хранения и обработки информации.

Законодатель выделяет широкий спектр прав субъекта персональных данных в отношении информации, касающейся его, и, напротив определяет строгие требования к оператору персональных данных, особенностям его работы.

1.3 Регламентирование деятельности работодателя по обработке, хранению, передаче и защите персональных данных работника

Основным законом в сфере защиты персональных данных, которым руководствуются организации, и который обязателен для выполнения – это Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных» (далее закон «О персональных данных) [25]. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Можно сказать, что это основной закон, который регулирует отношения в области обработки персональных данных. Однако, при всей своей глубине и ширине, в данном акте очень много статей, которые вносят много неясностей и ставят в тупик многие организации в вопросах реализации требований, предписываемых данным законом. Поэтому не исключены случаи вольной трактовки статей в процессе их выполнения.

С этой целью рассмотрим еще несколько нормативно-правовых документов, которые расширяют и дополняют закон «О персональных данных».

Для начала рассмотрим постановление Правительства от 1 ноября 2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее постановление Правительства №1119) [20]. Согласно тексту документа, его цель − это установление требований к защите персональных данных при их обработке в информационных системах и уровней защищенности таких данных. Также в пятом пункте данного акта подробно рассмотрены информационные системы, которые обрабатывают разные категории персональных данных. Одновременно, много внимания уделено типам угроз, актуальных для данных ин формационных систем и соответственно подробно приведены необходимые уровни защищенности, которые необходимо обеспечить при обработке персональных данных. В завершении, указаны требования к операторам, которые необходимо выполнить в соответствии с типами угроз [20].

Данное постановление Правительства РФ содержит немало ссылок как на закон «О персональных данных», так и на другие нормативные правовые акты, например, на приказ ФСТЭК от 18 февраля 2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [21].

Рассмотрим последний нормативно-правовой документ. Как следует из названия, в нем устанавливаются состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для каждого из уровней защищенности персональных данных, установленных в требованиях к защите ПДН при их обработке и информационных системах, утвержденных постановлением Правительства №1119.

Стоит отметить, что в данном приказе обширно и подробно расписаны меры по обеспечению безопасности персональных данных, а также кроме списка этих мер приведены пояснения и указания, как они должны выполняться в организации.

Как было сказано ранее, приказ ФСТЭК № 21 поясняет требования к защите и обеспечению безопасности персональных данных, указанных в Постановлении Правительства №1119.

Рассмотрим также приказ ФСБ России от 10.07.2014 №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке при их обработке в информационных системах с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее приказ ФСБ №378). Данный нормативно-правовой документ является расширением и дополнением для постановления Правительства №1119, о чем и говорится в пятом пункте приказа. Далее в документе подробно расписаны состав и содержание организационных и технических мер для каждого класса защищенности [20].

Документ расширяет и поясняет постановление Правительства №1119 и обязателен для выполнения в организациях, которые используют криптографические средства защиты персональных данных.

Тем не менее, на многих предприятиях не повсеместно реализованы автоматические системы обработки персональных данных и используются материальные носители информации. Например, при трудоустройстве на работу. Для таких случаев было разработано постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждения перечня Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее постановление Правительства № 687).

Документ объясняет принцип обработки неавтоматизированной обработки персональных данных, также поясняет подробно, какие меры должны быть предприняты при обработке персональных данных вручную людьми и хранении их на материальных носителях.

При рассмотрении нормативных правовых актов, которые поясняют и дополняют закон «О персональных данных», стоит обратить внимание на следующий документ: постановление Правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее постановление Правительства №211) [22].

В данном постановлении Правительства РФ подробно изложен список нормативных и правовых мер, направленных на обеспечение безопасности персональных данных и выполнении требований, указанных в законе «О персональных данных» [25]. В документе содержатся названия и содержание документов, которые должны быть приняты в организации, кроме этого приведен список мероприятий, направленных на предупреждение угроз безопасности персональных данных.

Хотя документ и предназначен для государственных или муниципальных органов, тем не менее, требования, которые он предъявляет к организации, стоит рассмотреть и принять во внимание и в дальнейшем использовать в работе предприятия.

Необходимо также рассмотреть нормативно-правовой акт в области трудового законодательств – это «Трудовой кодекс Российской Федерации» от 30.12.2001 №197-ФЗ, а именно 14 глава «Защита персональных данных работника». Данный акт регулирует отношения между работодателем и работником в области обеспечения безопасности персональных данных сотрудника и определяет требования в данной области.

Необходимо выделить требования, которые данные акты предъявляют к организациям. Условно их можно разделить на административные и технические. К административным относятся требования организационного характера, создание внутренних нормативных правовых актов. К техническим требованиям относят внедрение программных и аппаратных средств защиты, а также средства контроля и ограничения доступа.

В таблице 1.1 внесены требования законодательства Российской Федерации в области персональных данных, предъявляемые организациям.

Таблица 1.1 - требования законодательства Российской Федерации в области персональных данных, предъявляемые организациям

Название документа	Административные требования	Технические требования
1	2	3
Федеральный закон от 27.07.2006 № 152 - ФЗ «О персональных данных»	Назначение оператором ответственного за обработку персональных данных	Обнаружение фактов несанкционированного доступа и принятие мер
	Издание оператором документов, определяющим его политику безопасности в области обработки персональных данных	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
	Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных	Создание информационной системы обработки персональных данных

Продолжение Таблицы 1.1

1	2	3
	Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных	
	Публикация или осуществление беспрепятственного доступа к документу, определяющего политику безопасности в области обработки персональных данных оператора	
	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы	
	Учет машинных носителей персональных данных	Обеспечение сохранности носителей персональных данных
Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных	Организация режима обеспечения безопасности помещений	Использование средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз
	Утверждение руководителем документа, определяющего перечень лиц, допущенных к обработке персональных данных	Наличие электронного журнала безопасности
	Ограничение доступа к журналу безопасности	
	Определение класса информационной системы персональных данных	
Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Идентификация и аутентификация субъектов доступа и объектов доступа	Ограничение программной среды
	Управление доступом субъектов доступа к объектам доступа	Защита машинных носителей
	Регистрация событий безопасности	Управление конфигурацией информационной системы
	Контроль безопасности персональных данных	Антивирусная защита
	Выявление инцидентов	Системы Обнаружения вторжений (ids/ips)
		Защита среды виртуализации

Продолжение Таблицы 1.1

1	2	3
Приказ ФСБ России от 10.07.2014	Утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях	Оснащение помещений входными дверьми с замками
	Ведение журнала учета носителей персональных данных	Обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей на получение персональных данных
	Поддержание в актуальном состоянии документ, определяющий перечень лиц, допущенных к работе с персональными данными	Обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений
	Назначение обладающего достаточными навыками должностного лица оператора ответственным за обеспечение безопасности персональных данных в информационной системе	обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения
	Обеспечение периодического контроля работоспособности автоматизированных средств	Полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе
	Назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям	Оборудование окнами и дверьми Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц

Продолжение Таблицы 1.1

1	2	3
	Утверждение перечня лиц, имеющих право доступа в Помещение	Хранение носителей персональных данных в сейфах, оборудованных внутренними замками
Постановление Правительства от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»	Необходимо обеспечивать раздельное хранение персональных данных, обработка которых осуществляется в различных целях	
	Не допускается фиксация на одном материальном носителе персональных данных, цели обработки заведомо не совместимы	
	Лица, осуществляющие обработку, должны быть проинформированы о факте обработки ими персональных данных	
Постановление Правительства от 21.03.2012 №211 «Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами являющимися государственными или муниципальными органами	Должны быть утверждены правила обработки персональных данных, устанавливающие процедуры, направление на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных	
	Должны быть утверждены правила рассмотрения запросов субъектов персональных данных или их представителей	
	Должны быть утверждены правила обезличивания персональных данных	
	Должны быть утверждены правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	
	Должен быть утвержден должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных	
	Должна быть утверждена типовая форма согласия на обработку персональных данных сотрудников или иных субъектов персональных данных	

Продолжение Таблицы 1.1

1	2	3
«Трудовой кодекс Российской Федерации» от 30.12.2001 №197-ФЗ	Работники должны быть ознакомлены под роспись с документами организации, устанавливающие порядок обработки ПДн	

Некоторые нормативные правовые акты, такие как постановление Правительства №211, предназначены для государственных и муниципальных организаций, но, тем не менее, требования, содержащиеся в них, также будут рассмотрены и адаптированы для работы в коммерческих организациях. Большинство требований, указанных в данной таблице остаются очень общими. Что приводит к вольной трактовке и страдает качество их выполнения внутри организации.

Жизнедеятельность человека в связи с необходимостью вступления в трудовые взаимоотношения, так или иначе, предполагает предоставлении информации о себе другим членам общества - в нашем случае работодателю.

В условиях нынешних социально-экономический условиях и волнений в стране, возможность эффективного управления поведением работника в процессе его трудовой деятельность представляется возможным лишь при наличии достоверных сведений о его личности, которые должны предоставляться в исчерпывающем объеме.

По нашему мнению, именно в Трудовом кодексе Российской Федерации это обстоятельство нашло наиболее четкое из всех возможных закреплений.

Одной из актуальных на сегодняшний день задач любого работодателя является построение наиболее прозрачных и урегулированных законом трудовых отношений между ним и работником. Работник, в свою очередь, как никто другой заинтересован в том, чтобы сведения личного характера, которые он предоставляет работодателю обрабатывались и хранились в

соответствии с действующим законодательством, исключая возможность незаконного и противоправного пользования этой информацией.

По нашему мнению, необходимо вернуть отражение понятие о персональных данных работника в положения действующего Трудового законодательства Российской Федерации, также необходимо применить расширенное толкование перечня документов, которые содержат персональные данные работника.

Таким образом, можно сделать ряд выводов. Для российской действительности институт персональных данных является относительно новым. Он пришел из института тайны частной жизни, являясь адаптацией, так называемого, права быть оставленным в покое.

Зарубежный опыт и история становления института персональных данных в значительной степени сказались на тенденциях и особенностях развития данного института в России. Наша страна в полной мере восприняла международные тенденции. Был учтен зарубежный накопленный правовой опыт. Кроме того, значительное внимание было уделено общественным реалиям российской жизни, произошедшим политическим преобразованиям, а также общим актуальным направлениям развития права. Особенно стоит отметить, что в России с учетом национальных условий реализации правовых норм были использованы возможности изменения и преобразования ключевого акта международного уровня анализируемой сферы – 108 Конвенции Совета Европы о защите прав физических лиц в отношении персональных данных 1981 года. Данный факт подтверждает готовность государства обеспечивать эффективное функционирование института персональных данных, а также способствовать его развитию.

Персональные данные представляют собой информацию, зафиксированную на любом материальном носителе о конкретном человеке, которая отождествлена или может быть отождествлена с ним. Нормативно-правовая база защиты персональных данных включает международное законодательство, Конституцию Российской Федерации, Федеральные

законы, в том числе Федеральный закон № 152 ФЗ «О персональных данных», Федеральный закон № 149 ФЗ «Об информации, информационных технологиях и о защите информации», различные подзаконные акты.

Таким образом, институт персональных данных регулирует общественные отношения, которые относятся к нескольким отраслям права. С одной стороны, институт персональных данных можно отнести к публичной отрасли права, с другой стороны – ряд норм указанного института можно найти в трудовом праве, которое традиционно относится к частной отрасли. Следовательно, институт персональных данных регулирует отношения, находящиеся на стыке отраслей, поэтому его следует рассматривать как межотраслевой.

Глава 2 Правовой механизм защиты персональных данных работника

2.1 Особенности защиты персональных данных работника

Ключевой целью ФЗ РФ № 152-ФЗ «О персональных данных» является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. Данная цель также включает защиту прав на неприкосновенность частной жизни, личную и семейную тайны. Обращаясь к ст.3 ФЗ РФ № 152–ФЗ «О персональных данных» можно сформулировать определение персональных данных. «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 и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация» – персональные данные.

Действующее законодательство выделяет несколько видов персональных данных, в числе которых общедоступные, обезличенные, специальные и другие. Общедоступные персональные данные – это данные, доступ к которым производиться с согласия субъекта персональных данных. На эту категорию персональных данных не распространяется принцип конфиденциальности. Доступ к ним предоставляется неограниченному кругу лиц. Если рассматривать более подробно принцип конфиденциальности, то в данном аспекте он включает в себя тайну фамилии, имени, отчества, год и место рождения, адрес, абонентский номер, сведения о профессии и иные.

К категории специальных персональных данных относятся данные, которые касаются национальной либо расовой принадлежности, философских убеждений, религиозных убеждений, политических взглядов, состояния здоровья, интимной жизни. Обработка специальных персональных данных допускается только в следующих случаях:

- имеется согласие субъекта персональных данных на обработку этих данных;

- допускается обработка общедоступных персональных данных; допускается обработка данных, относящихся к состоянию здоровья субъекта, когда получение его согласия на обработку не представляется возможным;

- допускается обработка данных, относящихся к состоянию здоровья субъекта, когда она производится лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Среди основных прав и свобод человека, реализуемых им в процессе труда, можно выделить достоинство личности, право на свободу и личную неприкосновенность, запрет на хранение, использование и распространение информации о частной жизни без согласия.

Все права, предоставленные субъекту персональных данных, возникают у субъекта единовременно. Стоит отметить, что реализация каждого права субъекта персональных данных зависит от этапа развития правоотношения, связанного с обработкой персональных данных. По мнению автора Кучеренко А.В. классификация прав субъекта персональных зависит от времени их реализации и включает три группы.

1. Группа прав, которые субъект персональных данных может реализовать до начала их обработки. К правам данной группы могут быть отнесены следующие: давать согласие на обработку, право дать согласие включить в общедоступные источники персональные данные, право получать сведения об операторе данных.

2. Группа прав, которые субъект персональных данных может реализовать во время обработки данных. В состав прав данной группы включается право иметь доступ к обрабатываемым персональным данным, право направить оператору запрос о наличии соответствующих данных у оператора, право требовать от оператора уточнения, блокирования и уничтожения персональных данных. Кроме того, в данную группу входят

права отзывать согласие на обработку персональных данных и требовать исключения персональных данных из общедоступных источников, право обращаться в Роскомнадзор как в Уполномоченный орган по защите прав субъектов персональных данных в случае их нарушения.

3. Группа прав, которые субъект персональных данных может реализовать после их обработки. В состав данной группы включено право обжаловать в судебном порядке неправомерные действия оператора, право обращаться в Роскомнадзор как в Уполномоченный орган по защите прав субъектов персональных данных в случае их нарушения [17, С. 59].

Субъект персональных данных обладает правом потребовать от оператора уточнить или заблокировать персональные данных, а также уничтожить их. Данное право реализуемо, если персональные данные, которыми располагает оператор, неполные, устаревшие, неточные либо если они получены незаконно, также не являются необходимыми для заявленной цели обработки. Срок внесения изменений и удаления данных составляет семь рабочих дней с момента обращения субъекта персональных данных либо его законного представителя, что соответствует нормам ч. 3 ст. 20 ФЗ–152. Оператор персональных данных обязан уведомить субъекта персональных данных о всех изменения и предпринятых им мерах.

Для обеспечения защиты указанных прав граждан при обработке их персональных данных российским законодательством закреплен государственно-правовой механизм, включающий в себя:

1) систему нормативно-правовых актов, устанавливающих требования к защите прав субъектов персональных данных на международном, национальном уровнях, перечень субъектов, уполномоченных вести обработку персональных данных, права и обязанности субъектов, принципы и условия обработки, меры контроля и ответственности за нарушение законодательства.

2) государственные органы, осуществляющие полномочия по защите прав субъектов персональных данных, по контролю и надзору за

выполнением требований, по обеспечению безопасности информационных систем [55, С. 251].

Исходя из опыта защиты персональных данных различных стран, можно определить два типа систем правового регулирования: децентрализованная и централизованная.

С учетом социального назначения трудового права персональные данные работников могут регулироваться коллективно-договорным и локальным актам.

На локальном уровне работодатель принимает правовые, организационные и технические меры при обработке персональных данных для их защиты от неправомерного или случайного доступа к ним и иных неправомерных действий в отношении них. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку данных только с их согласия, поскольку это может повлечь причинение ущерба.

Оператор, как субъект персональных данных наделен определенными обязанностями.

Первое, что должен сделать оператор, это уведомить соответствующий орган – Роскомнадзор – о производстве обработки персональных данных лица. Оператор обязан направить данное уведомление до начала обработки данных и указать в нем наименование, адрес оператора, категории персональных данных, цель обработки, правовое основание обработки данных, категорию субъектов, которые подлежат обработке, наименование физического или юридического лица, дату и сроки обработки персональных данных.

Существуют ситуации, при которых уведомление Роскомнадзора не требуется. Таковым может быть обработка персональных данных работников работодателем. Также в случаях заключения договоров с клиентом не требуется уведомлять Роскомнадзор, если сведения используются организацией исключительно в целях данного договора и не передаются

иным третьим лицам без согласия субъекта персональных данных. При оформлении единоразового пропуска для доступа на территорию оператора персональных данных и при обработке общедоступных персональных данных не требуется уведомление Роскомнадзора. Если оператором используются только ФИО субъекта и другие аспекты. Данные положения определены в ч. 2 ст. 22 закона о персональных данных.

Обязанностью оператора является обеспечение конфиденциальности персональных данных. Он не должен распространять какие-либо известные ему сведения о персональных данных субъекта без согласия лица, в отношении которого ведется обработка персональных данных. Это является основной обязанностью оператора. Без письменного согласия работника работодатель не может сообщить персональные данные какой-либо третьей стороне. Кроме того, необходимо предупреждать третьи лица о том, что передаваемые персональные данные работников могут использоваться только в тех целях, для которых они переданы. Передача персональных данных работников допустима только в пределах одной организации, у одного индивидуального предпринимателя, что должно быть обусловлено одним локальным нормативным актом. Ознакомление с данным актом работника под подпись является обязательным (ст. 88 ТК РФ).

Обязанностью оператора является принятие мер по обеспечению безопасности персональных данных. С данной обязанностью тесно связана другая – по осуществлению внутреннего контроля за соблюдением требований по защите персональных данных. В ст. 22.1 закона о персональных данных определено, что с целью выполнения указанных обязанностей в организации должно быть назначено ответственное лицо. В полномочия и закрепленные обязанности указанного лица входит непосредственный внутренний контроль за тем, как оператор и его работники соблюдают требования о защите персональных данных.

Очевидно, что ответственное лицо должно обладать необходимой экспертной квалификацией, что предполагает принадлежность к особому

профессиональному сообществу. В Европе инспекторы по защите персональных данных существовали и ранее, до введения нормы об обязательном осуществлении соответствующих полномочий [62].

Ответственное лицо обязано информировать работников о всех изменениях в законодательстве о персональных данных, доводить до их сведения его положения и положения локальных актов, связанных с вопросами обработки персональных данных. Также в обязанности лица, ответственного за обработку персональных данных у оператора, входит организация и прием обращений от субъектов персональных данных. С этой целью дополнительно могут применяться и использоваться различные технические меры, обеспечивающие безопасность обработки персональных данных. Ответственное лицо обязано издавать все документы, в которых определена политика компании в области обработки персональных данных.

Уведомлять уполномоченный орган об обработке персональных данных в целях обеспечения соблюдения трудового законодательства является правом, а не обязанностью оператора.

При этом, следует отметить, что на практике часть юристов толкуют данную норму следующим образом: обработка таких категорий как сотрудники и близкие родственники сотрудников, осуществляемая в соответствии с трудовым законодательством, не требует включение в уведомление об обработке персональных данных направляемое в Роскомнадзор.

Проведенный автором, анализ судебной практики показывает, 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 также указал, что ЗАО «ИТС+» добровольно

подавало в уполномоченный орган уведомление о намерении осуществить обработку персональных данных и 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 [42].

Арбитражный суд Астраханской области в решении по делу № А06–1975/2011 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 [43].

Таким образом, арбитражные суды, не отрицая право оператора решать, уведомлять уполномоченный орган о факте обработки персональных данных сотрудников или нет, однозначно высказываются за то, что если оператор обрабатывает иные категории персональных данных, то он обязан направлять уведомление в уполномоченный орган с обязательным указанием всех категорий обрабатываемых персональных данных.

В ч. 2 ст. 18.1 Закона о персональных данных определяется публичность политики обработки персональных данных организации. Способом, который в наибольшей степени позволяет сделать данный документ доступным, является размещение на официальном сайте оператора. Если данный аспект не выполним, то бумажный вариант политики может быть размещен в любом месте, которое является доступным для посетителей организации. Это могут быть специальные информационные доски либо отдельные «кармашки». Те операторы, которые производят сбор персональных данных через Интернет, в обязательном порядке размещают политику на официальном сайте. При этом, должен быть обеспечен доступ к данной политике. Роскомнадзор разместил на своем сайте рекомендации,

позволяющие составить политику в области обработки персональных данных.

Стоит отметить, что на предприятии должно быть два документа, связанных с обработкой персональных данных, которые не следует путать. Так, политика обработки персональных данных распространяет свое действие и предназначена для третьих лиц – клиенты, контрагенты и др. Положение о защите, хранении, обработке и передаче персональных данных работников – иной документ, выступающий в роли локального акта, распространяет свое действие на работников организации. Требования публичности на него не распространяются, но обязательно необходимо под роспись ознакомить с ним каждого сотрудника компании (ст. 22 ТК РФ).

Обязанностью оператора является локализация персональных данных. Оно заключается в том, что все операторы, осуществляющие обработку персональных данных, должны делать это при помощи тех баз данных, которые хранятся в России. Требование вступило в действие с 1 сентября 2015 года и закреплено в ч. 5 ст. 18 закона «О персональных данных». Среди операторов и различных специалистов указанная норма вызвала большое количество споров и стало резонансным. Это связано с неоднозначностью формулировок, которые вызвали вопросы даже у экспертов. Не было ясно, на какие точно персональные данные и на каких операторов распространено действие требования, допустимо ли производить одновременно обработку данных на российском и иностранном сервере, как определяется гражданство субъекта и многие другие.

В большинстве своем указанные вопросы были раскрыты Роскомнадзором до вступления новых требований в действие. В частности, вопрос определения гражданства лица, персональные данные которого обрабатываются оператором, был отнесен к самостоятельному ведению оператора. Он сам должен решить, каким образом будет определяться гражданство, либо применяться требование о локализации к персональным данным всех субъектов. Также Роскомнадзор разъяснил положение о том,

что записанные на в российскую базу данных персональные данные в дальнейшем могут проходить обработку на иностранной базе данных.

Обязанность оператора обеспечивать запись и хранение, систематизацию и накопление, а также обновление и изменение персональных данных российских граждан при помощи тех баз данных, которые расположены в России, должна быть в обязательном порядке закреплена как в политике обработки персональных данных, так и в Положении о защите персональных данных работников. В указанных документах также должно быть определено место нахождения указанных баз данных.

Оператор прекращает обработку персональных данных в следующих случаях: когда достигнута цель обработки персональных данных, а также, когда от субъекта данных поступил отказ в их обработке. Срок, который закреплен законодательно для прекращения обработки, составляет 30 дней. В дополнительном соглашении такой срок может изменяться, что указано в ч. 4-5 ст. 21 закона «О персональных данных».

Таким образом, деление прав субъекта персональных данных производится на три категории. Они включают такие составляющие, как права субъекта персональных данных, которые он может реализовать до обработки, в процессе обработки данных и после их обработки. Помимо возможности отозвать свое согласие на обработку персональных данных субъект имеет еще целый ряд прав, о которых важно знать. В том числе лицо, чьи персональные данные обрабатываются, имеет право получать любую информацию, касающуюся этого, будь то данные оператора (его наименование и место нахождения), перечень обрабатываемых данных, сроки их обработки и хранения и др. Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляющего данную обработку и т. д.

Оператор, который производит обработку персональных данных, должен выполнять ряд обязанностей. К их числу относятся: уведомление об

обработке персональных данных соответствующего органа, обеспечение безопасности персональных данных при их обработке, получение согласия субъекта на обработку его персональных данных и другие.

Организационные меры по защите персональных данных включают в себя:

1) разработку организационно-распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных (Например, Положение об обработке персональных данных, Положение по защите персональных данных, Регламент взаимодействия при передаче персональных данных третьим лицам и т.д.);

2) перечень мероприятий по защите персональных данных:

– определение круга лиц, допущенного к обработке персональных данных;

– разработка должностных инструкций по работе с данными;

– установление персональной ответственности за нарушения правил обработки данных;

– ознакомление работников с действующими нормативами в области защиты персональных данных и локальными актами;

– организация доступа в помещения, где осуществляется обработка данных;

– определение продолжительности хранения персональных данных;

– утверждение порядка уничтожения информации;

– выявление и устранение нарушений требований по защите данных;

– проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

В каждой организации перечень мероприятий и документов может варьироваться в зависимости от специфики обработки персональных данных, организационной структуры и других особенностей конкретной организации.

Технические меры связаны с внедрением технических средств охраны, программных средств защиты информации на электронных носителях и др.

Трудовой кодекс [52] (ст. 89) закрепляет основные права работника по защите данных: получение полной информации о своей личной информации; бесплатный доступ к ней; изменение и исключение неполных или недостоверных данных; обжалование в суде или Роскомнадзор неправомерных действий работодателя связанных с персональными данными.

Правом доступа к персональным данным работника обладают ряд лиц, а именно руководитель организации, работодатель – индивидуальный предприниматель, начальник отдела кадров и сотрудники отдела кадров, сотрудники управлений оплаты труда, если это речь идет о производственных объектах, в число тех, кто обладает персональными данными работника входят бригадиры, мастера, инженеры по охране труда и промышленной безопасности и т.д. Как правило, персональные данные нового работника вскоре сообщаются так называемым третьим лицам: в пенсионный фонд, фонд социального страхования, иные государственные органы, организации, ведущие бухгалтерское, кадровое, информационное сопровождение «на аутсорсинге» (фирмы 1С-франчайзи), помещаются на сайт работодателя на страницу «Наши сотрудники» (когда речь идет о руководителях или менеджерах по работе с клиентами), включаются во внутренние телефонные справочники компании и др.

Цепочка лиц, которые могут так или иначе стать обладателями персональных данных работников в зависимости от предприятия работодателя может варьироваться, но не смотра на это, работодатель при участии работников должны участвовать в их рациональном использовании и

предлагать меры по защите персональных данных работников, как в организации так и на предприятии.

Автор представленной работы считает, что в рамках каждой организации необходимо укомплектовать отдел, который осуществлял бы обработку, хранение, сбор и работу с персональными данными работника. По мнению автора, идеальным вариантом, в плане соблюдения норм действующего законодательства в области защиты персональных данных было бы создание своеобразной кодировки персональных данных работника.

Не для кого не секрет, что все современные предприятия и организации максимально автоматизировали свой трудовой процесс, в первую очередь это создано для того, чтобы освободиться от огромного количества бумажной документации - табели учета рабочего времени, приказы о приеме на работу, переводу как внутри подразделения как и предприятия в целом, расчетные листы, личные карточки работников приходится хранить очень большое количество времени, и отметим отдельно, что материальные документы подвергаются со временем порче и могут быть легко уничтожены посредством пожара или затопления. Информационные системы, используемые на каждом предприятии способны подчас заменить живого человека, ведь именно эти системы на современном предприятий выполняют функции хранения, обработки, актуализации и систематизации документов, введение «кодировки» данных работника позволит исключить как их утечку, так и нежелательное использование.

Считаем необходимым усовершенствовать и обновлять IT продукты, которые осуществляют хранение и систематизацию персональных данных, повышая их коэффициент безопасности и уменьшая при этом как возможность утечки как и взлома, в первую очередь потому, что при обработке персональных данных работников в информационной системе работодатель должен обеспечить:

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

– своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

– постоянный контроль за уровнем защищенности персональных данных.

Примером представленной кодировки может быть так называемая система табельных номеров в организации. В табельном номере достаточно зашифровать фамилию, имя и отчество; отдел в котором работает работник, его дата рождения, и занимаемая должность. Данная система, на наш взгляд позволит избежать утечки информации в тех случаях, где она не исключается но предпочтение отдается не распространять данные о работнике.

Как нами уже было отмечено, работники наравне с работодателем должны участвовать в создании и реализации мер по защите персональных данных работников. Работодатель в свою очередь должен проводить обучение и повышение квалификации персонала, который в соответствии с должностными инструкциями осуществляет работу с персональными данными работников в организации (на предприятии). Обучение должно производиться как при приеме на работу, так и по мере введения новых поправок и изменений в действующее законодательство о защите персональных данных работника. Кроме этого, для того чтобы сформировать четкую политику в области защиты персональных данных работников, рациональные предложения и решения по их защите должны внедряться с

участием мнений представителей администрации организации, управления персоналом, юридического отдела, бухгалтерии.

Всем известна простая истина: незнание закона не освобождает от ответственности, а зачастую работники управления персоналом знают только положения ТК РФ и не способны в полной мере обеспечить защиту персональных данных работников на должном уровне. За нарушение законодательства о защите персональных данных работников работодатель может быть привлечен к серьезной ответственности. Чтобы этого избежать, работодатель должен строго исполнять требования законодательства о защите персональных данных работника.

Согласно п. 8 ст. 86 ТК РФ 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. Во исполнение данного требования при приеме работника работодатель знакомит его под роспись с локальным нормативным актом, определяющим порядок обработки персональных данных работников, его права и обязанности в этой области.

Согласно п. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [25] обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Согласно статье 9 указанного закона субъект персональных данных (в нашем случае – работник) принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

Но, к сожалению, в практике имеют место и случаи, когда обработка персональных данных работников осуществляется вне их интересов и без их согласия. Так, в 2014 году гражданка Посякова С.Н. обратилась в суд с иском, в обоснование которого указала, что в настоящее время работает в Восточно-Сибирской региональной дирекции железнодорожных вокзалов -

структурного подразделения Дирекции железнодорожных вокзалов – филиала ОАО «РЖД» в должности начальника сектора применения законодательства и договорной работы. Поводом для обращения в суд послужили факты обработки (использования и передачи) должностными лицами Восточно-Сибирской РДЖВ персональных данных (фамилия, имя, отчество, а также иных сведений о трудовой деятельности) в порядке и случаях, не предусмотренных действующим законодательством РФ без ее согласия, а именно сбор, использование и передача должностными лицами Восточно-Сибирской РДЖВ материальных носителей – ее заявлений от <дата изъята>, находящихся в отделе кадров предприятия и содержащих ее персональные данные, в целях проведения экспертного исследования и предоставление третьему лицу ООО «СибРегионЭксперт», без уведомления о фактах такой обработки персональных данных и получения ее предварительного согласия [3].

Согласно п. 3 ст. 86 ТК РФ все персональные данные работника следует получать у него самого.

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

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

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

– определение своих представителей для защиты своих персональных данных;

– доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением

требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

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

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

Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя, базируются на главном принципе свободы доступа работника к своим персональным данным, в том числе на праве получения копии любой записи, содержащей такие данные.

На дистанционных работников это положение тоже распространяется, но с учётом особенностей, установленных гл. 49.1 ТК РФ.

Работники также имеют право:

– на полную информацию о своих персональных данных и их обработке;

– на доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского специалиста по его выбору;

– обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите их персональных данных. Защищать свои персональные данные они могут самостоятельно либо через представителя. Таким представителем может выступать профсоюз либо иное лицо (как физическое, так и юридическое);

– требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства.

Статья 21 ФЗ № 152 возлагает на работодателя обязанность по блокированию обработки персональных данных работников в случае:

1) Выявления фактов неправомерной обработки персональных данных – в течение 3 дней проводится проверка по факту неправомерной обработки и прекращается обработка; в течение 10 дней уничтожаются неправомерно обрабатываемые персональные данные.

2) Выявления неточных персональных данных - обработка блокируется, в течение 7 рабочих дней уточняются данные, после чего продолжается обработка (снята блокирование).

3) В случае окончания сроков обработки персональных данных и невозможности их уничтожения (на срок не более 6 месяцев). Решение о блокировании оформляется приказом с обоснованием причин невозможности уничтожения персональных данных.

Стоит обратить внимание на строго целевой характер сбора и иной обработки информации (п.1 ст.86 ТК). С этим связана практическая проблема – у работодателей получила широкое распространение практика получения от работника письменного согласия на обработку его данных одновременно с заключением трудового договора. Эти данные делятся на те, которые прямо предусмотрены законами и те, которые могут понадобиться работодателю, то есть не конкретизированные, любые. В статье 6 Закона «О персональных данных» установлены случаи, когда согласие не требуется и наличие или отсутствие согласие не влияют на права и обязанности работодателя. Напротив, заранее получать согласие на весь период трудового договора нельзя в силу того, что ст. 9 Закона определяет порядок и форму получения согласия, в котором должны быть указаны цель обработки, перечень данных и перечень действий с ними. Это значит, что в согласии могут указываться только конкретные данные конкретного работника. Иные условия будут ничтожными в силу прямого противоречия принципам международного права.

Данное положение соответствует международной практике. Так, Федеральный конституционный суд Германии исключает сбор данных «про запас» для неопределенных или не поддающихся определению целей, устанавливает запрет на использование данных, собранных для достижения одной цели, не в соответствии с ней, а в иных, несовместимых с ней целях [39, С. 18].

При получении персональных данных у третьей стороны без согласия работника нужно уведомить его о предполагаемом получении его персональных данных у иного лица. Если работник отказывается ознакомиться с уведомлением, составляется акт об отказе [36].

Поскольку целями получения персональных данных у третьего лица являются соблюдение законов, содействие работникам в трудоустройстве,

обучение и продвижение по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества. То запрашивать иную информацию от третьих лиц работодатель не вправе даже с согласия работника [37]. Также запрещено работодателям передавать данные своих бывших работников новым работодателям по их запросам, без письменного согласия работников [38], то же требование относится к сторонним организациям (например, банкам).

Работодатель выдает уведомление об отказе в предоставлении информации, если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение такой информации либо нет согласия работника на предоставление сведений о нем лицу, обратившемуся с запросом.

Ст. 86 ТК запрещено получение и обработка персональных данных работника о его убеждениях (политических, религиозных и иных), частной жизни, членстве в общественных объединениях или профсоюзной деятельностью.

Анализ нормативных правовых актов позволяет выделить общие обязанности работника по предоставлению работодателю данных о себе:

1) при приеме на работу перечень данных, установленных в ст. 65 ТК РФ:

а) о стаже работника, подтверждаемом трудовой книжкой (данная информация необходима для определения размера выплачиваемого работнику пособия по временной нетрудоспособности);

б) о регистрации работника в системе государственного пенсионного страхования, подтверждаемой страховым свидетельством государственного

пенсионного страхования;

в) о состоянии работника на воинском учете, подтверждаемую документами воинского учета (для военнообязанных и лиц, подлежащих призыву);

г) об образовании, квалификации работника, наличии у него специальных знаний, что подтверждается документами об образовании, о квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

д) о возрасте работника, месте его жительства, гражданстве, подтверждаемую паспортом или иным документом, удостоверяющим личность;

е) о наличии или об отсутствии у работника семейных обязанностей, что подтверждается паспортом;

ж) о наличии (об отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергавшиеся уголовному преследованию.

2) документы, подтверждающие право на дополнительные гарантии и компенсации по основаниям, предусмотренным законодательством об

инвалидности, донорстве, нахождении в зоне воздействия радиации в связи с аварией на ЧАЭС и другие;

3) документы о состоянии здоровья обязаны предъявлять инвалиды (медицинская справка и индивидуальная программа реабилитации), государственные гражданские и муниципальные служащие, работники, обязанные проходить медосмотры в силу закона, например управляющие источником повышенной опасности, работающие в области охраны (ст.7) 63;

4) документ о беременности работнице и возрасте детей для предоставления матери условий труда, гарантий и компенсаций (ст.93, 96, 99, 122, 253 ТК РФ);

5) документ о повышении квалификации работника в пределах уровня имеющегося у него профессионального образования (например, педагоги);

6) работники, допущенные к сведениям, составляющим государственную тайну, обязаны своевременно сообщать об изменении своих данных;

7) работодатель вправе располагать информацией о членстве работника в профсоюзе, поскольку его увольнение по вышеуказанным основаниям требует выполнения определенного порядка (ст. 82 ТК РФ).

Так, положение трудового договора об обязательстве работника сообщить о своем членстве в профсоюзе было судом признано законным в связи с тем, что указанная информация, хотя и носит конфиденциальный характер, необходима работодателю для выполнения требований трудового законодательства.

Представление иных документов, необходимых работодателю, является добровольным волеизъявлением работника. Чтобы установить объем информации, которую работодатель вправе получать от работника, нужно иметь в виду важное ограничение – это целевой характер использования персональных данных (п.1 ст. 86 ТК РФ).

На практике часто возникает вопрос о предоставлении работником индивидуального номера налогоплательщика (ИНН). В ст. 65 ТК РФ данный

документ не указан, в силу ст. 57 ТК РФ к обязательным условиям трудового договора не относится. Поэтому в соответствии с действующим законодательством работник не обязан предоставлять ИНН работодателю.

Однако, он необходим для сдачи бухгалтерской отчетности 2-НДФЛ, и работники должны предоставлять ИНН для правильного оформления документов, связанных с его трудовой деятельностью.

К документам, которые работник может представить в случае своего добровольного волеизъявления, относятся свидетельство о заключении (расторжении) брака, о рождении детей, пенсионное удостоверение и т.д.

Порядок хранения и использования персональных данных работников устанавливается работодателем самостоятельно либо с участием работников и их представителей. Может устанавливаться особый порядок хранения и обращения для определенных носителей информации (например, материальные носители биометрических данных).

Персональные данные работника относятся к конфиденциальной информации. Работодатель за счет собственных средств принимает правовые, организационные и технические меры при обработке персональных данных для их защиты от неправомерного или случайного доступа к ним и иных неправомерных действий в отношении персональных данных. Как правило, разработка мероприятий по защите персональных данных работника осуществляется в рамках общих мероприятий по защите информации ограниченного доступа, находящейся во владении работодателя.

В этих целях оператор (работодатель) обязан (ст.18.1 Закона о персональных данных):

– назначить ответственного за организацию обработки персональных данных; издать локальные акты, определяющие политику оператора в отношении обработки персональных данных;

– обеспечить принятие мер по обеспечению безопасности персональных данных;

– осуществлять внутренний контроль соответствия обработки персональных данных законодательству;

– оценить вред, который может быть причинен работникам в случае нарушений;

– ознакомить работников, осуществляющих обработку данных, с положениями законодательства РФ о персональных данных.

Согласно ст. 14 Закона о персональных данных работодатель обязан сообщить работнику (законному представителю) информацию о наличии персональных данных, относящихся к нему и безвозмездно предоставить возможность ознакомления с ними при обращении работника, внести в них необходимые изменения, уничтожить или блокировать их. О принятых мерах работодатель обязан уведомить работника (законного представителя) и третьих лиц, которым данные работника были переданы.

Действующее законодательство не предусматривает конкретных требований к оборудованию помещений, где должны храниться персональные данные. Во избежание несанкционированного доступа помещения следует оборудовать сейфами и запирающимися шкафами, обладающими хотя бы минимальной взломостойкостью, для хранения информации на бумажных носителях. При этом хранить в одном сейфе (шкафу) документы, деньги и другие материальные ценности запрещается.

При этом за необеспечение правильного комплектования, учета, хранения и использование документации прошлых лет предусмотрена административная ответственность работодателя.

Выходом из этой ситуации будет создание в организации архива, который должен соответствовать законодательству об архивном деле в РФ. Для этого выделяется отдельное помещение, где создаются специальные условия хранения документов, а также организуется раздельное хранение документов, содержащие персональные данные работников, от остальных документов архивного хранения. Допускается также передача функций по

хранению архива сторонним организациям, оказывающим услуги по хранению, в том числе хранение в электронном виде.

Таким образом, на работодателя возлагается ответственность по установлению режима конфиденциальной обработки персональных данных в целях их защиты от несанкционированного доступа, изменений или распространения.

Применение законодательства о защите персональных данных зачастую происходит таким образом, что фактически создаются препятствия для реализации прав, гарантированных другими законодательными актами – прежде всего, права на доступ к информации, необходимой для реализации прав конкретного лица. При рассмотрении дел об оценке правомерности отказов в предоставлении информации суды иногда очень своеобразно и не всегда последовательно определяют, какая информация затрагивает права заявителя непосредственно и поэтому должна быть предоставлена несмотря на содержащиеся в ней персональные данные, а в каких случаях защита персональных данных не позволяет предоставить эту информацию.

Так, при проведении конкурса на замещение должности государственной службы суд признал за соискателем должности право получить возможность ознакомиться с протоколом заседания конкурсной комиссии, определяющим уровень профессиональной подготовки победившего кандидата [40]. При этом в рамках самой процедуры конкурса на замещение публичной должности (главы муниципального образования) истребование характеристики на одного из претендентов с прежнего места работы – органа внутренних дел – было признано судом незаконным [41]. Положения законодательства об административных правонарушениях трактуются в судебной практике как предоставляющие абсолютное право лицу, в отношении которого ведется производство, знакомиться со всеми материалами дела, в том числе с заявлением гражданина, инициировавшего это производство. Суды не принимают во внимание опасность

преследований со стороны лица, в отношении которого ведется производство [2].

Суды признают правомерным, вопреки правовой позиции Конституционного Суда РФ от 18.02.2000 № 3-П, даже отказы в доступе к информации о самом заявителе – например, к результатам прокурорских проверок в отношении служащего по сообщениям о нарушении законодательства о государственной службе [44].

На основе проведенного анализа характеристика правового понятия «субъект персональных данных», можно сделать вывод, что любое физическое лицо, не зависимо от каких-либо критериев с наличием информации, является субъектом права. Проблематика заключается в том, что ФЗ «О персональных данных» не содержит конкретного, обобщенного, официально закрепленного понятия субъекта персональных данных. Действующий Закон не разграничивает участников правоотношений, не выделяет четких критериев Федеральный закон № 152–ФЗ дает легитимное определение оператора, организующего и (или) осуществляющего обработку персональных данных.

Оператор – физическое либо юридическое лицо, имеющее доступ к чужим персональным данным. Он самостоятельно может не проводить обработку персональных данных, а может являться только организатором этого процесса. Оператор отвечает за легитимность и качество процесса обработки персональных данных. Закон делит операторов на несколько категорий: физические лица, индивидуальные предприниматели, юридические лица, муниципальные органы, государственные органы.

Субъект права – базовая категория права. Любое лицо является субъектом права, не приобретая этот статус самостоятельно и единовременно, а только из признания данного статуса государством. Говоря иначе, объем правосубъектности лица, который участвует в обороте персональных данных, определяется формулировкой положений

законодательства. Данный факт положен в основу всего правореализационного процесса в сфере обработки персональных данных.

На данный момент в связи с вышесказанным существует потребность законодательного закрепления точных характеристик и четких критериев, которые лягут в основу определения статуса оператора, осуществляющего обработку персональных данных.

Деление прав субъекта персональных данных производится на три категории.

Они включают такие составляющие, как права субъекта персональных данных, которые он может реализовать до обработки, в процессе обработки данных и после их обработки. Помимо возможности отозвать свое согласие на обработку персональных данных субъект имеет еще целый ряд прав, о которых важно знать. В их числе, то, согласно которому, лицо, чьи персональные данные обрабатываются, имеет право получать любую информацию, касающуюся этого, будь то данные оператора (его наименование и место нахождения), перечень обрабатываемых данных, сроки их обработки и хранения и др. Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляемого данную обработку и т. д.

Оператор, который производит обработку персональных данных, должен выполнять ряд обязанностей. К их числу относятся: уведомление об обработке персональных данных соответствующего органа, обеспечение безопасности персональных данных при их обработке, получение согласия субъекта на обработку его персональных данных и другие.

Функции по контролю за соблюдением оператором государственных информационных систем организационных и технических мер по защите персональных данных возложены на Федеральную службу по техническому и экспортному контролю Российской Федерации и Федеральную службу безопасности Российской Федерации (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 Российской Федерации, 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), то она считается государственной информационной системой и оператор становится поднадзорным регуляторам в лице ФСТЭК России и ФСБ России.

Например, если в Министерстве образования Российской Федерации 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 и ФСБ (если для защиты персональных данных используются криптографические средства).

По мнению автора, сложившееся в практике толкование норм ст. 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» является не верным, т.к. в данных нормах содержится два обязательных условия, только одновременное выполнение которых, позволяет относить информационную систему к государственной:

1. Информационная система должна быть создана на основании федерального закона (по мнению автора это означает, что в законе должно

быть прямо указано на это), либо закона субъекта Российской Федерации, либо на основании правового акта государственного органа (автор полагает, что речь идет о правовом акте, прошедшем регистрацию в Министерстве юстиции Российской Федерации).

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. Автор полагает, что указанная норма означает, что информационная система должна быть предназначена для выполнения каких-либо публично-правовых функций.

Например, информационная система, предназначенная для реализации кадровой политики какого-либо государственного органа, которая, безусловно, существует в целях реализации полномочий данного органа. Как правило, в большинстве государственных органов о введении в действие указанной системы имеется «внутренний» приказ (локальный нормативный акт, не зарегистрированный в Министерстве юстиции РФ). По мнению большинства регуляторов, данные информационные системы следует относить к государственным системам.

Автор полагает, что относить информационные системы, в которых обрабатываются персональные данные сотрудников каких-либо государственных органов или государственных учреждений к государственным информационным системам неправомерно.

Следовательно, проводить мероприятия по контролю (надзору) за соблюдением действующего законодательства в информационных системах обрабатывающих персональные данные работников организации вправе только Роскомнадзор.

Поскольку положениями гл. 14 ТК РФ, наравне с Федеральным законом «О персональных данных», определены требования к обработке персональных данных работников и гарантии их защиты, контроль за соблюдением работодателем трудового законодательства, в том числе в

части обработки персональных данных, вправе осуществить и Государственная инспекция труда. Это следует из ст. 353 ТК РФ.

Следует отметить, что Федеральным законом от 21.07.14 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 года.

Внесение указной 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 от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» [23]. Это, в частности, означает отсутствие ограничений на проведение внеплановых проверок. В итоге в соответствии с внесенными изменениями с 1 сентября 2015 года существенно расширится перечень основании, по которым Роскомнадзор РФ может провести проверку. Максимальные сроки длительности проверок также не будут применимы (по общему правилу не более 20 рабочих дней).

При выявлении в ходе государственного контроля нарушений действующего законодательства оператор может быть подвергнут административному штрафу. Конкретные санкции за нарушение правил обработки персональных данных будут рассмотрены в следующем параграфе.

Таким образом, нормативно-правовое обеспечение защиты персональных данных представлено достаточно разветвленной системой

правовых актов. Нормы материального права находят свое отражение в Конституции РФ, Федеральном законе «О персональных данных» и Трудовом кодексе РФ, нормы процессуального права в подзаконных нормативных актах: Указы Президента РФ, Постановления Правительства РФ, приказы ФСТЭК России, ФСБ России. При этом, немаловажная роль отведена локальным нормативным актам, издаваемым операторами персональных данных. На практике, именно они определяют конкретные процедуры обработки персональных данных работников в организации.

Однако, действующее законодательство содержит ряд норм, допускающих неоднозначное толкование. Так, в частности, нормы ст. 22 Федерального закона «О персональных данных» толкуются большинством юристов следующим образом: обработка таких категорий персональных данных как сотрудники и близкие родственники сотрудников, осуществляемая в соответствии с трудовым законодательством, не требует включение в уведомление об обработке персональных данных, направляемое в Роскомнадзор РФ. При этом, сам регулятор (Роскомнадзор) толкует данную норму иначе: если оператор подает уведомление, то необходимо указать все категории персональных данных. Указанная позиция находит свое подтверждение и в судебной практике. Представляется необходимым конкретизировать содержание ст. 22 Федерального закона «О персональных данных».

Основным локальным нормативным актом, определяющим политику организации в сфере защиты персональных данных, является Положение о персональных данных работников. Указанный документ запрашивается в обязательном порядке при проведении государственного контроля (надзора) за соблюдением действующего законодательства о персональных данных.

2.2 Современные условия защиты персональных данных работника

В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи была принята Директива 2002/58/ЕС [10], закрепляющая обязанность государств-членов Европейского Союза (далее – ЕС) в своем национальном законодательстве гарантировать конфиденциальность передаваемых сообщений и относящихся к ним данных трафика посредством сети связи общего пользования и общедоступных услуг электронной связи. В частности, государства-участники должны запретить прослушивание, несанкционированное подключение, хранение или другие виды перехвата или слежки за сообщениями и относящимися к ним данными трафика, кроме случаев получения санкционированного разрешения на осуществление этих действий в соответствии с пунктом 1 статьи 15 настоящей Директивы.

В свою очередь, возможность государств-членов ЕС принять законодательные меры, ограничивающие некоторые права в области защиты конфиденциальности коммуникаций, если такие ограничения представляют собой необходимую, соответствующую и пропорциональную меру в рамках демократического общества для осуществления защиты национальной (государственной) безопасности, обороны и общественной безопасности, предотвращения, расследования, обнаружения и судебного преследования преступных действий устанавливается в п. 1 ст. 15 Директивы 2002/58/ЕС. В связи с этим государства-члены Европейского Союза могут, помимо прочего, принять законодательные меры, предусматривающие сохранение данных на определенный период по основаниям, предусмотренным в настоящем пункте.

Спустя практически 4 года (15.03.2006 г.) была принята Директива 2006/24/ЕС [11], целиком посвященная хранению персональных пользовательских данных.

Исходя из опыта защиты персональных данных в различных странах можно определить два типа систем правового регулирования: децентрализованная и централизованная [33].

Признаки децентрализованной системы (США, Канада, Австралия):

− отсутствие единого подхода к защите персональных данных в рамках отраслевого законодательства;

− регламентация защиты осуществляется посредством профильных нормативных актов комплексных отраслей законодательства (здравоохранение, трудовые отношения) и / или на разных уровнях власти;

− акты рекомендательного характера играют значительную роль;

− отсутствие единого надзорного органа.

К признакам централизованной системы (страны ЕС, Израиль, Мексика, Швейцария, Сингапур) можно отнести:

− прямое действие международных норм, гармонизирующих национальные законодательства государств (Конвенция о защите физических лиц при автоматизированной обработке персональных данных);

− наличие национальных отраслевых законов, содержащих общеобязательные нормы в отношении защиты персональных данных;

− учреждения единого надзорного ведомства («мегарегулятора»).

Также можно говорить и о смешанной системе, когда отмечается наличие одного или нескольких признаков. Так в Японии и на Тайване действуют единые законы о защите персональных данных, но отсутствуют единые надзорные ведомства. В Бразилии регулирование осуществляется на основе общих норм, конституционных принципов и непрофильных законов, при этом отсутствует единый надзорный орган. В Южной Африке нет специальных законов, однако в Конституции закреплено право на конфиденциальность. В Саудовской Аравии в отсутствие применимого законодательства суды руководствуются нормами шариата (исламского права).

В целях защиты прав граждан в области персональных данных Россия обеспечила имплементацию в российское законодательство требований общеевропейского права, создала систему защиты прав субъектов, соответствующую основным принципам межгосударственных нормативных

правовых актах в области персональных данных. В целом российское трудовое законодательство соответствует международным стандартам защиты персональных данных в сфере трудовых отношений.

Нормативная база правового регулирования оборота информации в трудовых отношениях включает в себя федеральный закон общего характера, главу в Трудовом кодексе, ряд актов Президента РФ и Правительства РФ, федеральных ведомственных актов по видам деятельности. С учетом социального назначения трудового права персональные данные работников могут регулироваться коллективно-договорным и локальным актам.

На локальном уровне работодатель принимает правовые, организационные и технические меры при обработке персональных данных для их защиты от неправомерного или случайного доступа к ним и иных неправомерных действий в отношении них. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку данных только с их согласия, поскольку это может повлечь причинение ущерба.

Государство призвано создать наилучшие условия свободного существования и развития личности. Конституцией РФ закреплены свобода поиска, получения, передачи, производства и распространения информации (ч. 4 ст. 29), гарантировано право на неприкосновенность частной жизни, личную, семейную тайну, тайну сообщений и запрещено распространение информации о частной жизни лица без его согласия (ст. 23–24).

Поступая на работу, гражданин представляет документы и заполняет анкеты, в которых содержатся разделы, относящиеся не только к профессиональной деятельности, но и затрагивающие аспекты частной жизни лица. Работодатель намерен получить максимальную информацию о потенциальном работнике, и не разграничивает информацию о частной жизни лица и информацию, которая характеризует лицо непосредственно как работника, то есть с точки зрения его деловых и профессиональных качеств, уровня образования или квалификации. Сложности определения степени

допустимого вмешательства и пределов вторжения в частную жизнь работника затрудняют реализацию норм, определяющих порядок и условия сбора, хранения, использования и распространения соответствующей информации в трудовой сфере и зачастую приводит к правонарушениям.

Персональные данные содержатся в различных документах. Например, к числу необходимых работодателю и не подлежащих разглашению относятся:

− документы, представляемые работником при трудоустройстве (ст. 65 ТК);

− справки о состоянии здоровья, если необходимость их предоставления предусмотрена законодательством (ст. 69, 213 ТК РФ).

Обработка персональных данных должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обрабатывать можно только те персональные, которые отвечают целям их обработки.

Кроме того, обработка персональных данных работников также осуществляется первичной профсоюзной организацией, научными, научно-техническими советами, различными комиссиями и другими специально созданными в организации органами. Деятельность этих подразделений и их специалистов регламентируются положением о нем и инструкциями. Охрана интересов работников по защите их данных в каждом подразделении достигается путем соблюдения двух групп требований: первая направлена на использование сведений о работнике в соответствии с теми целями, для которых они были сообщены (п. 3 ст. 88 ТК РФ); и вторая — соблюдение требований о передаче информации о работниках иным подразделениям и третьей стороне (пп. 2, 5 ст. 88 ТК РФ). Кадровые службы координируют деятельность иных подразделений по указанным вопросам.

На современном этапе происходит модернизация европейского законодательства в области защиты персональных данных, которая

направлена на усиление региональной интеграции. В частности, разрабатывается проект модернизации основополагающего документа Совета Европы - «Конвенции о защите физических лиц при автоматизированной обработке персональных данных» [13, С. 94].

Кроме того, в настоящее время Евросоюзом рассматривается проект нового закона прямого действия о защите персональных данных (взамен Директив, которые реализовывались посредством адаптации и включения их положений в национальное законодательство). Он включает требование к организациям об уведомлении об утечках персональных данных в течение 24 часов.

Нарушающим закон компаниям будет грозить штраф в размере до 4% от их мирового оборота. Закон установит единый набор правил для европейский компаний и компаний за пределами Европы, если они будут предлагать свои услуги в Евросоюзе.

1 июля 2017 года вступил в силу Федеральный закон от 07.02.2017 № 13-ФЗ, который внес поправки в ст. 13.11 КоАП. В частности, он предусматривает расширение перечня оснований для привлечения к административной ответственности за незаконную обработку персональных данных и существенное увеличение штрафов.

При создании системы защиты персональных данных в организациях, на современном этапе развития в РФ, можно выделить следующие последовательные этапы:

− выяснить и определить все случаи, когда необходимо проводить обработку персональных данных в организации; − определить совокупность обрабатываемых персональных данных и круг информационных систем;

− подготовить действующую модель угроз для информационной системы обработки персональных данных;

− разработать техническое задание по созданию необходимой системы защиты;

− подать заявку на получение экземпляров руководящих документов в Федеральную службу по техническому и экспортному контролю России по организации системы защиты персональных данных;

− разработать требования для конкретной системы обработки персональных данных, учитывая класс защиты информационной системы;

− для защиты информационной системы обработки персональных данных и помещений подготовить технический проект;

− для документов в информационной системе защиты персональных данных (регламенты, приказы, положения, инструкции) разработать пакет организационно-распорядительные документы;

− провести внедрение системы защиты персональных данных;

− с субъектов персональных данных взять согласие на обработку персональных данных;

− провести контрольные мероприятия по выявлению нарушений защиты персональных данных; физическому или юридическому лицу иностранного государства, при передаче оператором персональных данных через государственную границу Российской Федерации органу власти иностранного государства, проверить находится ли получатель персональных данных в стране, где осуществляется надлежащая защита персональных данных.

В случае необходимости может привлекаться организация для выбора и реализации методов и способов защиты информации в информационной системе обработки персональных данных, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации оформленную в установленном законом порядке.

Применение законодательства о защите персональных данных зачастую происходит таким образом, что фактически создаются препятствия для реализации прав, гарантированных другими законодательными актами - прежде всего, права на доступ к информации, необходимой для реализации прав конкретного лица. При рассмотрении дел об оценке правомерности

отказов в предоставлении информации суды иногда очень своеобразно и не всегда последовательно определяют, какая информация затрагивает права заявителя непосредственно и поэтому должна быть предоставлена, несмотря на содержащиеся в ней персональные данные, а в каких случаях защита персональных данных не позволяет предоставить эту информацию.

Так, при проведении конкурса на замещение должности государственной службы суд признал за соискателем должности право получить возможность ознакомиться с протоколом заседания конкурсной комиссии, определяющим уровень профессиональной подготовки победившего кандидата. При этом в рамках самой процедуры конкурса на замещение публичной должности (главы муниципального образования) истребование характеристики на одного из претендентов с прежнего места работы – органа внутренних дел – было признано судом незаконным. Положения законодательства об административных правонарушениях трактуются в судебной практике как предоставляющие абсолютное право лицу, в отношении которого ведется производство, знакомиться со всеми материалами дела, в том числе с заявлением гражданина, инициировавшего это производство. Суды не принимают во внимание опасность преследований со стороны лица, в отношении которого ведется производство.

Применение системы защиты информации является не обязательным для всех типов информационных систем обработки персональных данных. Выбор системы защиты информации необходимо осуществлять, учитывая, что конечный набор мер для защиты персональных данных должен отвечать требованиям, предъявляемым к информационной системе обработки персональных данных соответствующего класса, определение которых приведено в Приказе ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных (Зарегистрировано в Минюсте России 14.05.2013 № 28375) (ред. от 23.03.2017).

В соответствии с Указом Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [24] осуществляется подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно телекоммуникационным сетям международного информационного (ред. от 22.05.2015). В каждой организации перечень мероприятий и документов может варьироваться в зависимости от специфики обработки персональных данных, организационной структуры и других особенностей конкретной организации.

Технические меры связаны с внедрением технических средств охраны, программных средств защиты информации на электронных носителях и др. Трудовой кодекс (ст. 89) закрепляет основные права работника по защите данных: получение полной информации о своей личной информации; бесплатный доступ к ней; изменение и исключение неполных или недостоверных данных; обжалование в суде или Роскомнадзор неправомерных действий работодателя связанных с персональными данными.

Таким образом, для системы защиты персональных данных информационная система обработки персональных данных выбирается в зависимости от класса информационной системы с учетом: угроз безопасности персональным данным; структуры информационной системы; наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа (реализуются функции управления доступом, регистрации и учета); обеспечения целостности защиты персональных данных; анализа защищенности персональных

данных; обеспечения безопасного межсетевого взаимодействия; обнаружения вторжений.

Система защиты персональных данных включает в себя меры организационного и технического характера, которые определяются с учетом актуальных угроз безопасности для персональных данных и информационных технологий, используемых в системе обработки информации организации.

Глава 3 Ответственность за разглашение персональных данных работника

3.1 Проблемы защиты персональных данных работника, перспективы и пути решения

Право на неприкосновенность частной жизни принадлежит каждому человеку от рождения, при этом не имеет значение, является человек гражданином, какой-либо страны. Челок сам определяет тот объем информации, которая впоследствии будет общедоступной, а что останется тайной.

Законодательного закрепления понятия «тайна информации» нет, имеется лишь определения различных тайн, к примеру, тайна связи, коммерческая тайна, государственная тайна. Конституция Российской Федерации устанавливает право каждого на неприкосновенность частной жизни. Конституционное положение, закрепляющее правовую защиту личной тайны, семейной тайны и тайны телефонных переговоров, телеграфных и иных сообщений является гарантией неприкосновенности частной жизни.

Тайной информацией можно назвать информацию, которая закрыта от всех пользователей, доступ к которой имеет определенный круг людей. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [25] раскрывает содержание тайны и неприкосновенности персональных данных, который предусматривает, что гражданин имеет право:

– представить свои персональные данные третьим лицам;

– получить сведения об операторе, о месте его нахождения, о наличии у оператора персональных данных;

– осуществить доступ к своим персональным данным;

– дать согласие на обработку персональных данных, отозвать согласие на обработку;

– требовать уточнение своих персональных данных, их блокирования или уничтожения в установленных случаях [25].

Право на тайну и неприкосновенность персональных данных означает право требовать от других лиц не нарушать тайну персональных данных, самостоятельно определять объем и судьбу своих данных, определять круг лиц, которая она будет доступна.

Закон о персональных данных определяет понятие «конфиденциальность персональных данных» — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания (ст. 3). Под распространением персональных данных понимаются действия, направленные на их передачу определенному кругу лиц или на ознакомление с ними неопределенного круга лиц, в том числе обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставления доступа к персональным данным каким-либо иным способом.

Недостаточная урегулированность защиты персональных данных порождает правонарушения, в частности, российское законодательство не определяет правовой статус субъектов интернет-отношений.

Законность проверки кандидата на работу службой безопасности зависит от того, какие именно сведения подлежат проверке. Изучение сведений, которые получаются из открытых источников информации, или тех, которые предоставил сам будущий претендент на должность, не является нарушением закона. Во всех остальных случаях будет иметь место нарушение законодательства. К сожалению, многие работники государственных и коммерческих структур, используя свое должностное положение, раскрывают тайны личной жизни, используя полученную информацию в корыстных или в личных целях.

Для решения этой проблемы необходимо найти баланс между соблюдением основных прав человека и эффективной работой правоохранительных органов. Меры по усилению борьбы с терроризмом не должны ограничивать права и свободы человека и гражданина, как личные, так и политические.

В России механизмами защиты права на неприкосновенность частной жизни от незаконного вторжения со стороны государства, общества или отдельных лиц содержатся в таких нормативно-правовых актах, как Конституция Российской Федерации, Всеобщая декларация прав человека, Международный пакт «О гражданских и политических правах» Уголовный кодекс Российской Федерации, Гражданский Кодекс Российской Федерации. У гражданина Российской Федерации есть выбор, обратится в орган исполнительной власти или в суд. Последний, из которых наиболее распространен. Отдельно стоит выделить прокурорский надзор в соответствии с Законом «О прокуратуре Российской Федерации» осуществляет надзор за исполнением действующих на территории Российской Федерации законов, принимает меры, которые направлены на устранение их нарушений и привлечение виновных к ответственности, осуществляет уголовное преследование [8].

На международном уровне механизм защиты персональных данных заключен в принципе неприкосновенности частной жизни. Указанный принцип содержится в вышеупомянутом международном пакте «О Гражданских и политических правах», ст. 17 гласит, что никто не может подвергаться произвольному или незаконному вмешательству на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства [49].

Под нарушением неприкосновенности стоит понимать воздействие как физическое, так и при помощи электронных средств. Для усовершенствования гражданско-правового механизма защиты

неприкосновенности частной жизни необходимо создать независимый институт, основная цель, которого защита неприкосновенности частной жизни.

Также необходимо, чтобы суды при решении вопроса о назначении способа гражданско-правовой защиты неприкосновенности частной жизни более широко толковали вмешательство в частные дела.

Уделив внимание государства на существующую проблему, обеспечение защиты неприкосновенности частной жизни значительно поспособствует совершенствованию всего отраслевого законодательства.

Создание единой информационной базы в рамках любого предприятия представляется наиболее безопасным и рациональным инструментом работы с персональными данными, их обработке и хранения.

Единое информационное пространство (база) представляет собой автоматизированный информационный банк данных, который содержит персональные данные работников суда. Данное информационное пространство предполагается разработать в соответствии с современными требованиями к безопасности хранения персональных данных работников и в первую очередь должно быть сформировано на основе лицензированных IT продуктов, от известного и проверенного представителя в сфере таких услуг.

Наличие лицензии к программному обеспечению в представленном случае обязательно, так как персональных данные государственных гражданских служащих представляют собой уровень особенной секретности.

Объединяя персональные данные работников в единую систему, необходимо задаться вопросом о том, кто и в каких объема будет совершать работу с вышеуказанными персональным данными. По нашему мнению, приоритет полномочий работы с персональными данными нужно отдать сотрудникам управления персоналом: они осуществляют учет рабочего времени каждого сотрудника; бухгалтерии: данный отдел осуществляет начисление заработной платы, иных отчислений предусмотренных действующим законодательством, осуществляют подготовку различных

справок по месту предъявления. Особенностями работы в такой системе будет являться не то, что она представляет собой единое всем доступное информационное пространство, а то, что работу в ней смогут осуществлять только уполномоченные на это работники, проходящие ежегодное повышение квалификации в аспекте работы с персональными данными работников своего предприятия посредством курсов, семинаров и т.д. Как правило, полномочия такого доступа следует выдать начальникам отделов, в случае если у основного работника отпуск или иные причины отсутствия на рабочем месте, обязанности по работе с персональными данными берет на себя либо заместитель начальника отдела, либо старший специалист, с обязательным составлением приказа о том, что в указанный в приказе период времени, в связи с отсутствием основного работника, обязанности по работе с персональными данными в системе лежит на данном работнике.

Также в обязательном порядке в организации должно быть разработано положение о работе с персональными данными работников, с которым уполномоченные к работе в системе лица должны быть обязательно ознакомлены под роспись.

В положении статьи 42 ФЗ РФ № 79-ФЗ от 27.07.2004 в пункте 1 отражено, что обработка персональных данных гражданского служащего осуществляется в целях в том числе, обеспечения сохранности принадлежащего ему имущества, обеспечения его личной безопасности и безопасности членов его семьи. На наш взгляд, реализация этого положения в указанном управлении является спорной, так как предоставляемые сведения о доходах гражданских служащих, которые в соответствии с Федеральным законом РФ от 25.12.2008 года № 273-ФЗ «О противодействии коррупции» подлежат обязательному опубликованию, кроме того, в документах которые содержат такие сведения, не происходит обезличивание данных о служащих, располагающих тем или иным доходом и имуществом. В рамках реализации единой информационной системы предлагается уделить данному аспекту особое внимание, по причине того, что это является

первоисточником доступности к сведениям, которые касаются непосредственно работника, что может повлечь за собой совершения преступных посягательств на жизнь и здоровье, как служащего, так и членов его семьи.

Создание единого информационного пространства является, безусловно, глобальной идеей о том, как в рамках одной программы объединить не только всю информацию о работниках, но и максимально закрыть доступ к такой информации для служащих, которые не уполномочены осуществлять работу с такой информацией. Безусловно, положительными чертами предлагаемой системы является наличие специальных компетентных работников, которые будут в строгом соответствии осуществлять работу с системой и нести за это ответственность, минусом данной системы будет являться необходимость обучить персонал качественной работе с такой системой, также предоставить доступ к информации программистам, которые будут осуществлять программное сопровождение, но представителей сторонних организаций можно всегда путем повышения квалификации заменить на работников организации. В свете предложенного в рамках представленного исследования был разработан ряд предложений по совершенствованию законодательства в области защиты персональных данных.

Важнейшим шагом в усовершенствовании эффективности и практичности защиты персональных данных работников является всестороннее и своевременное развитие действующего законодательства, регулирующего вопросы внесения изменений в законодательные акты.

Одной из ключевых проблем в отрасли защиты персональных данных работников является отсутствие регламентированного понятия персональных данных, это порождает в свою очередь определенные сложности, в том числе в правоприменительной практике. Поэтому следует дать развернутое и четкое определение персональных данных работников: персональными данными работника являются сведения индивидуального характера об

определенном работнике (работниках), которые основаны на законе, предъявляемые работнику работодателем в определенных целях, способствующих трудоустройству работника и защищаемые способами, предусмотренными действующим законодательством, в целях запрета несанкционированного распространения персональных данных работника.

Кроме того, по мнению автора представленного исследования на сегодняшний день необходимо создание оптимального правового механизма обороты и защиты персональных данных работника. Но решение данной проблемы в должном ключе предполагает обширный мониторинг состояния современного рынка информационных технологий, IT - продуктов, услуг отслеживания общих тенденций развития информационного общества Российской Федерации. Исследуемый рынок не стоит на месте, работодателю предлагаются все новые и новые системы для обработки, хранения и работы с персональными данными, каждый работодатель заинтересован в ведении своей деятельности соблюдая нормы действующего законодательства и поэтому в первую очередь работодатель должен быть заинтересован в лицензировании и «легальности» предлагаемых программ.

В соответствии с пп. 4 статьи 12 Федерального закона Российской Федерации «О лицензировании отдельных видов деятельности» от 04.05.2011 года № 99-ФЗ регламентирует необходимость лицензирования такого вида деятельности, как разработку и производство средств защиты конфиденциальной информации. В области обеспечения конфиденциальности персональных данных работников можно выделить как минимум два основополагающих законодательных акта: ТК РФ и Федеральный закон Российской Федерации «О персональных данных», причем, положения ТК РФ регулируют только обработку персональных данных работников, а ФЗ «О персональных данных» обработку персональных данных всех категорий граждан без исключения.

3.2 Ответственность за нарушение правил работы с персональными данными

В науке неоднократно делались попытки установить систему расчета компенсации морального вреда по трудовым спорам. Например, профессор Аворник предлагал установить нижний и верхний пределы компенсации – в сумме месячной зарплаты и до семи заработных плат работника [47]. Однако степень нравственных страданий личности не зависит от ее доходов и социального статуса. По мнению Феофилактова А.С. логичным было бы закрепление твердых денежных сумм в Трудовом кодексе [56]. Возможно, имеет смысл установить шкалу штрафных платежей, которые выплачиваются в зависимости от оборота компании-работодателя. Шведовым А.Л. предлагалось частное или публичное извинение, оно в большей степени способствует психологической реабилитации потерпевшего [57]. Размер компенсации может быть установлен и соглашением сторон (ст. 237 ТК).

В целях обеспечения работы с персональными данными проводится комплекс мероприятий, закрепляемый в документах организации. В первую очередь руководителем назначается лицо или подразделение, ответственное за данный вид деятельности, и наделяется соответствующими полномочиями. Затем определяется перечень персональных данных, нуждающихся в обработке. Далее – подготавливается и утверждается приказом руководителя список лиц, которые допущены к данной деятельности.

Основным локальным документом, регулирующим защиту информации в организации, является «Положение о работе с персональными данными». В нормативных документах не установлена унифицированная форма и структура текста такого положения, поэтому зачастую оно строится исходя из строения законов, регулирующих обработку персональных данных. Нет и единого заголовка. Уже разработанные в организациях документы называются «О защите персональных данных» или «Об организации работы

с персональными данными». В большинстве своем такие документы состоят из нескольких разделов, в которых раскрываются термины, перечисляется нормативная база, определяется перечень данных, подвергающихся обработке, и прилагаемого образца заявления «О согласии на обработку персональных данных». Отдельным пунктом положения обязательно перечисляется, в каких случаях согласие работника на обработку его данных не требуется.

Надлежащее исполнение правил обработки персональных данных в организации обеспечивается определенной законом ответственности лиц, участвующих в данной деятельности, за нарушение соответствующих должностных инструкций.

Статья 90 Трудового Кодекса РФ за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, предусматривает дисциплинарную, административную, гражданско-правовую и уголовную ответственность.

Дисциплинарная ответственность применяется к работнику, если обработка персональных данных являлась его трудовой функцией и была закреплена в трудовом договоре, должностной инструкции, иных локальных нормативных актах и работник был ознакомлен с ними под расписку [26]. В противном случае ответственность будет возложена на работодателя как не обеспечившего необходимую охрану персональных данных.

Рассмотрим встречающиеся в судебной практике случаи увольнения сотрудников по пп. «в», п. 6, ч.1, ст. 81 ТК РФ.

Увольнение сотрудника за распространение конфиденциальной информации путем отправки сообщений по электронной почте.

Отправка на электронный почтовый ящик третьих лиц сведений, содержащих охраняемую законом тайну, рассматривается как разглашение этих сведений.

Противоречива судебная практика, если такие сведения отправлены работником на свой внешний электронный почтовый ящик. Если сотрудник

производил отправку документов с конфиденциальной информацией на внешние адреса личной: личный почтовый адрес на внешнем сервере и адрес электронной почты супруги, то увольнение по пп. «в», п. 6, ч.1, ст. 81 ТК РФ признано судом законным [27].

Сам по себе факт отправления без доказательств последующей передачи третьим лицам не рассматривается как разглашение этих сведений [28].

Но в некоторых случаях суды приходят к противоположному выводу. Судом признается законным увольнение сотрудника за передачу пароля доступа к программному обеспечению, содержащему конфиденциальную информацию [29].

Кроме того, судом признается законным увольнение сотрудника за разглашение конфиденциальной информации посредством программы «Skype» [48], за сохранение информации на usb-носитель и отправку документов на внешние адреса электронной почты [31], за предоставление в суд документов содержавших конфиденциальную информацию (штатное расписание) [41], за ненадлежащее хранение и утилизацию конфиденциальной информации (оставление документов в мусорных баках) [32].

Трудовой кодекс, помимо замечания, выговора и увольнения работника (предусмотренных статьей 192 ТК РФ), совершившего дисциплинарный поступок предусматривает так же специальное основание расторжения ТД в случае разглашения охраняемой законом тайны оператором персональных данных (п.п. «в» п.6 ст.81).

Работники, совершившие дисциплинарный проступок несут дисциплинарную ответственность. Дисциплинарная ответственность - самостоятельный вид юридической ответственности работников организации. К признакам дисциплинарного проступка относят наличие субъекта проступка, субъективной стороны, а так же объекта проступка и объективной стороны.

Внутренний трудовой распорядок организации – объект дисциплинарного проступка. Объективная сторона – вредные последствия и прямая связь между ними и действием работника.

Субъектом является гражданин, находящийся в трудовых правоотношениях с конкретной организацией и нарушивший трудовую дисциплину. Субъективная сторона такого проступка - вина со стороны работника, форме умысла или по неосторожности.

На основании заключенного трудового договора работодатель требует от работника добросовестного выполнения возложенных на него обязанностей. В соответствии со ст. 192 ТК работодатель имеет право, но не обязан привлекать к дисциплинарной ответственности работника, совершившего дисциплинарный проступок. Так же следует отметить, что в законодательстве Российской Федерации, уставами и положением о дисциплине организации определяются различные правила при совершении дисциплинарного проступка.

Разглашение персональных данных потерпевшего лица может быть совершено среди широкого круга лиц, не имеющих законного доступа к ним. Главные нарушения правил работы с персональными данными: получение конфиденциальной информации, либо ее использование без законных оснований, а так же утрата материальных носителей информации, содержащих такие сведения [51]. За данные нарушения предусмотрена дисциплинарная ответственность, не предусматривающая увольнения, но в случае, если работник совершил разглашение персональных данных какого-либо лица, то ему грозит увольнение. К дисциплинарной ответственности могут быть привлечены только сотрудники кадровой службы, взявшие на себя обязанность исполнять требования правил, обеспечивающих безопасность при работе с персональными данными. Это значит, что они взяли на себя обязанность не разглашать сведения, составляющие персональные данные, что было закреплено в их трудовом договоре, их ознакомили под подпись с локальными нормативными актами, и

работодателем были предоставлены требуемые для осуществления должностных полномочий условия.

В случае отсутствия проведения перечисленных выше мероприятий, специалист, которому доверена работа с персональными данными, ответственности не несет. Факт нарушения правил работы с персональными данными может быть установлен представителем работодателя (например, начальником отдела кадров), самим работником или специалистом государственной инспекции труда.

К правам работников организации в отношении защиты своих персональных данных относятся: осуществление контроля над полноценным выполнением требований по обеспечению конфиденциальности этой информации, наличием всех предусмотренных средств защиты персональных данных; право запретить или приостановить обработку персональных данных в случае их невыполнения [12]. С целью отстаивания своих законных прав работник имеет право обжаловать в судебном порядке любые неправомерные действия (бездействие) работодателя при обработке и защите персональных данных.

Кодекс об административных правонарушениях РФ с 2017 года выделяет 7 статей за нарушение правил работы с персональными данными.

Статья 13.11 КоАП РФ «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных» предусматривает ответственность в виде предупреждения или наложения штрафа для должностных лиц в размере от 3000 до 20000руб., ИП – от 5000 до 20000руб., организации на сумму от 15000 до 75000руб. При этом привлечение к ответственности происходит по нескольким составам правонарушений сразу. Ранее – состав нарушения был один, а максимальный штраф составлял 10000руб.

Защита конфиденциальности такого вида охраняемой законом тайны как персональные данные предусматривается в статье 13.14 КоАП РФ «Разглашение информации с ограниченным доступом».

Информация, имеющая ограниченный доступ является объектом правонарушения.

Объективная сторона данного правонарушения состоит в действиях, в результате которых произошло разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Конфиденциальную информацию определяет административное, гражданское и иное отраслевое законодательство РФ.

Административную ответственность работодатель несет только в случае его привлечения к таковой государственной инспекцией труда или судом.

Также административной ответственности могут быть подвергнуты работодатели или индивидуальные предприниматели, которые используют несертифицированные информационные системы, базы и банки данных для хранения и обработки персональных данных работников, а также использующие несертифицированные средства защиты информации, если они в обязательном порядке подлежат сертификации – это в соответствии с положениями части 2 статьи 13.12 КоАП РФ влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

Предметом преступления являются сведения о частной жизни лица, составляющие его личную или семейную тайну, независимо от того, прочат эти сведения его или нет.

Собирание сведений означает, что виновный тайно или открыто, знакомится с документами, письмами и другими источниками.

Распространение сведений о частной жизни потерпевшего означает сообщение их хотя бы одному лицу, заинтересованному или не заинтересованному в получении таких сведений. Субъектом данного преступления является вменяемое физическое лицо, достигшее возраста 16 лет. Субъективная сторона выражается прямым умыслом.

Далее следует рассмотреть наиболее строгий вид ответственности – уголовная ответственность. Статья 137 УК РФ «Нарушение неприкосновенности частной жизни» предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, в том случае, если такие действия являлись намеренными, в целях корыстной или иной личной заинтересованности. В случае использования виновным своего служебного положения, наказание ужесточается.

Личную или семейную тайну составляют сведения, не подлежащие, по мнению лица, которого они касаются, оглашению, при условии, что ранее они не были опубликованы либо оглашены иным способом.

Виды нарушения неприкосновенности частной жизни (ст. 137 УК): незаконное собирание сведений о частной жизни; незаконное их распространение; незаконное их распространении в публичном выступлении, в СМИ.

В законодательстве не указана связь ответственности за разглашение конфиденциальной информации с конкретным способом такого распространения. Распространением считается любая передача конфиденциальной информации третьим лицам. Незаконным распространением является разглашение конфиденциальной информации лицом (работником организации), обязанным держать ее в тайне в силу трудового договора и законодательства РФ. В некоторых случаях разглашение сведений о частной жизни по УК образует одновременно состав другого преступления, например, разглашение тайны усыновления (ст. 155). В таких случаях содеянное квалифицируется по совокупности со ст. 137 УК.

Обязательный элемент объективной стороны такого преступления согласно ст. 137 УК - вред правам и законным интересам.

По характеру вред разделяется на: моральный, материальный, физический. Установление наличия и характера вреда, причиненного потерпевшему, производится индивидуально с учетом особенностей ситуации и личности.

Законом определено, что, преступлением, посягающим на неприкосновенность частной жизни можно считать только действия, повлекшие за собой причинение соответствующего вреда, то есть материального состава.

Часть 2 статьи 137 УК РФ предусматривает квалифицированный вид преступления, указанного в части 1 статьи 137 УК РФ, а именно лицом с использованием его служебного положения.

Корыстная или иная личная заинтересованность – основной элемент субъективной стороны (мотив). Намерение опорочить конкурента, повлиять на личное продвижение в карьере, месть, демонстрация превосходства и другие виды выгоды за счет потерпевшего называются корыстной заинтересованностью. По ч. 1 ст. 137 УК ответственность несет любое физическое вменяемое лицо, достигшее 16 лет (общий субъект), а по ч. 2 ст. 137 УК - должностное лицо либо служащий государственного или муниципального учреждения, использующий для совершения преступления свое служебное положение (специальный субъект).

Несмотря на то, что приведенное выше законодательство, и предусмотренная за его нарушение ответственность, направлены на обеспечение права человека на неприкосновенность частной жизни, в силу ч. 3 ст. 55 Конституции предусматриваются определенные ограничения права на защиту информации о частной жизни в случаях, когда это является необходимой мерой, направленной на защиту конституционного строя, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Подводя итог, хочется отметить, тот факт, что для того, чтобы на каждом предприятии нашей страны соблюдались установленные действующим законодательством положения о персональных данных работников, у каждого учреждения, организации, предприятия, должно быть положение о работе с персональными данными работников. Данное положение, по мнению автора представленной работы, позволит не только своеобразным образом регламентировать работу с персональными данными работников предприятия, но и сформировать четкий алгоритм действий по их обработке, хранению и передаче. В таком положении, как правило, должны быть прописаны особенности сбора, обработки, хранения, передачи и защиты персональных данных работников, порядок хранения личных дел работников и доступ к ним, отражены права в работников в целях защиты своих персональных данных и ответственность за нарушение норм, регулирующих особенности работы с персональными данными работника. А для того, чтобы работа кадровых служб в области обработки персональных данных проходила с соблюдением всех правил и требований, организациям актуально предложить проводить проверки управления персоналом руководителем организации совместно с представителями юриста (юридической службы, если это крупное предприятие) и службы безопасности.

Заключение

Результатом исследования проблемы, поставленной в магистерской диссертации, стали выводы, сделанные в ходе изучения, структурирования и объединения сведений о действующем законодательстве, исследований правовой, моральной и материально-технической составляющих процесса сбора, обработки, хранения и использования персональных данных в организациях.

1. Персональными данными работника являются сведения индивидуального характера об определенном работнике (работниках), которые основаны на законе, предъявляемые работнику работодателем в определенных целях, способствующих трудоустройству работника и защищаемые способами, предусмотренными действующим законодательством, в целях запрета несанкционированного распространения персональных данных работника.

2. Нельзя утверждать об окончательной сформированности и высоком качестве законодательства в сфере регулирования защиты персональных данных, в силу относительной новизны таких правоотношений, и их постоянного активного развития в последние годы. Скорость и эффективность внесения изменений в нормативные документы уступает разработке новых способов обработки информации, видов ее применения.

3. В обществе не сложилось однозначного мнения о том, как распоряжаться персональными данными на предприятии или в учреждении.

4. Несмотря на несовершенство законодательства, главной причиной утечки персональных данных чаще всего является халатность работников предприятий и организаций в процессе обработки информации, требующей защиты. Нарушения присутствуют на всех стадиях обработки, начиная от некорректного составления/заполнения согласия на обработку персональных данных, пренебрежение ведением отчетной и

сопроводительной документации, заканчивая банальным безответственным отношением к персональным данным.

5. Компетентным государственным органам в сфере защиты персональных данных применяется достаточно широкий спектр мер. Среди которых, право запрашивать у операторов информацию о порядке обработки персональных данных, право по рассмотрению обращений, принятию мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства. Однако большинство полномочий Роскомнадзора не имеет практической реализации, поскольку не урегулированы российским законодательством. Необходимо устранить данные ограничения, что позволит усовершенствовать систему защиты прав и законных интересов субъектов персональных данных. В частности, разработать и принять административный регламент взаимодействия органов Роскомнадзора и Прокуратуры.

В заключении хочется отметить, что заявленная в начале работы цель исследования: «анализ организации защиты персональных данных работников» - достигнута. Обработка и защита персональных данных в организациях и преследует общую цель – не допустить неправомерное использование конфиденциальной информации.

Вопрос обработки и защиты персональных данных будет всегда оставаться открытым, поскольку в соответствии с тенденцией стремительного роста информационных технологий, законодательство просто не сможет успеть за ними, и всегда найдутся недочеты в любой правовой системе, которые необходимо доработать, усовершенствовать, чтобы правовое регулирование отвечало современным требованиям защиты личности, новым вызовам и угрозам. Эта деятельность требует комплексного подхода, сочетающего в себе применение эффективных правовых, организационных и технических мер.

Основной целью создания защиты персональных данных в организациях является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

В целях создания единой, целостной и скоординированной системы информационной безопасности персональных данных и создание условий для ее дальнейшего совершенствования, предлагается комплексный подход, для которого необходимо разработать следующий пакет документов для всех организаций:

– Положение о защите персональных данных.

– Согласие работника образовательного учреждения на обработку своих персональных данных.

– Положение об ответственном лице информационной безопасности организации.

– Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

– Журнал учета персональных данных.

– Обязательство работника о неразглашении персональных данных.

Целесообразно сегментировать слабо взаимодействующие подсистемы информационной системы персональных данных, так необходимо разделить кадровый и бухгалтерский учета персонала и организовать обмен данными между ними с помощью съемных носителей.

Необходимость разработки предложенных выше положений и документов обусловлена стремительным расширением сферы применения информационных технологий и процессов при обработке информации вообще, и персональных данных в частности.

Список используемой литературы и используемых источников

1. Алямкин С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты/ С.Н. Алямкин // Мир науки и образования. – 2016. – № 4 (8). – С. 4-8
2. Апелляционное определение судебной коллегии по гражданским делам Свердловского областного суда от 25.09.2012 по делу № 33 // Архив Свердловского областного суда Свердловской области
3. Апелляционное определение судебной коллегии по гражданским делам Иркутского областного суда от 16.01.2014 по делу № 33 – 219/2014 // Архив Иркутского областного суда Иркутской области
4. Архипов В. В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. - 2018. - № 2. С. 12-18.
5. Важорова М. А. История возникновения и становления института персональных данных // Государство и право: теория и практика: материалы Междунар. науч. конф. — Челябинск: Два комсомольца. - 2011. - С. 33-38.
6. Гуде С.В. Защита персональных данных в Российской Федерации: исторический аспект и современное состояние / С.В. Гуде, П.В. Арбузов, А.Г. Карпика // Юристъ-Правоведъ. – 2015. – № 2 (69). – С. 93-97.
7. Дворецкий А.В. Определение понятия персональных данных работника в Трудовом кодексе РФ // Сибирский юридический вестник. - 2005. - № 2. - С.32-34.
8. Деменева Н.А., Мамай А.Д. Защита персональных данных работников / Проблемы научной мысли. – 2018. - № 1. С. 66-71.
9. Всеобщая декларация прав человека: (принята 10 дек. 1948 г. резолюцией 217А Генеральной Ассамблеи ООН) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.
10. Директива Европейского парламента и Совета Европейского Союза № 2002/58/ЕС

11. Директива Европейского парламента и Совета ЕС № 2006/24/ЕС

12. Иванова М.М. Защита персональных данных работника // Аллея науки. – 2018. - № 4 (20). С. 789-794.

13. Исакова Л.В. Международно-правовое регулирование защиты персональных данных работников / Л.В. Исакова, К.Е. Статуева // Экономика и право: Новый университет. – 2015. – № 4(50). – С. 93-95.

14. Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 27.12.2019) (с изм. и доп., вступ. в силу с 13.01.2020) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

15. Конституция РФ от 12 декабря 1993 г. (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

16. Копылов В.А. Информационное право. М.: Юристъ, 2005. – 512 с.

17. Кучеренко А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – № 12 (31). – Ч.2. – С. 59-60.

18. Латухина В.С. Международные и национальные стандарты уголовно-правовой защиты персональных данных/ В.С. Латухина // Экономика. Социология. Право. – 2017. – No.4. – С. 76.

19. Михайлова И. А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика. 2017. № 10. С. 11–18.

20. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119. – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

21. 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– Доступ из справ.-правовой системы Гарант. – Текст: электронный.

22. Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами, являющимися государственными или муниципальными органами: Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014). – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

23. О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля: Федеральный закон от 26.12.2008 № 294-ФЗ (ред. от 02.08.2019) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

24. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента РФ от 17.03.2008 № 351– Доступ из справ.-правовой системы Гарант. – Текст: электронный.

25. О персональных данных: Федеральный закон от 27.07.2006 152-ФЗ (ред. 29.07.2017) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

26. Определение Московского городского суда от 22.12.2011 № 4г/8-10945/11 // Архив Московского городского суда Московской области

27. Определение Московского городского суда от 20.10.2014 по делу № 4г/9-9007/2014 // Московского городского суда Московской области

28. Определение Верховного суда РФ от 29.08.2018 г. по делу № А53-18685/2017

29. Определение СК по гражданским делам Приморского краевого суда от 24.06.2013 по делу № 33-5273 // Архив Следственного комитета по гражданским делам Приморского краевого суда Приморского края

30. Определение Московского городского суда от 16.10.2014 по делу № 33-35077/2014 // Архив Московского городского суда Московской области

31. Определение Московского городского суда от 08.10.2013 по делу № 11-33789 // Архив Московского городского суда Московской области

32. Определение Московского городского суда от 19.08.2014 № 4г8-7847 // Архив Московского городского суда Московской области

33. Параскевов А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал Кубанского государственного аграрного университета. - 2015. - № 110(06). - С. 6

34. Постановление ФАС Восточно-Сибирского округа от 17.08.2010 по делу № А19-25289/09 // Архив судебных решений Арбитражных судов и судов общей юрисдикции

35. Постановление ФАС Московского округа от 29.04.2010 № КА-А40/4062-10 по делу № А40-159104/09-93-1333 09// Архив судебных решений Арбитражных судов и судов общей юрисдикции

36. Постановление ФАС Волго-Вятского округа от 18.05.2006 по делу № А79-8239/200509 // Архив судебных решений Арбитражных судов и судов общей юрисдикции

37. Проскурякова М.И. Конституционно-правовые основы защиты персональных данных в России и Германии в истолковании органов конституционного правосудия // Сравнительное конституционное обозрение. 2015. № 1. С.18.

38. Решение Головинского районного суда г. Москвы от 08.10.2013 по делу № 2-5055/13 // Архив районного суда Московской области

39. Решение Люберецкого городского суда от 13.12.2011 по делу № 2-7983/2011 // Архив городского суда Московской области

40. Решение Свердловского районного суда города Белгорода от 30.03.2011 по делу № 2-941/2011 // Архив районного суда г. Белгород Свердловской области

41. Решение Пестяковского районного суда Ивановской области от 03.11.2010 по делу № 2- 254/ 10 // Архив Пестяковского районного суда Ивановской области

42. Решение Арбитражного Суда Свердловской области по делу № А60–41475/2011 от 26.12.11 г. // Архив Арбитражного Суда Свердловской области

43. Решение Арбитражного Суда Новгородской области по делу № А44–1867/2011 от 22.07.11 г. // Архив Арбитражного Суда Новгородской области.

44. Решение Центрального районного суда г. Челябинска, дата и номер обезличены; Белов С.А. Согласование законодательства о защите персональных данных с правовым регулированием в других сферах: Законодательство о защите персональных данных / Санкт-Петербургский государственный университет// Мониторинг правоприменения за февраль 2014 года [Электронный ресурс] – Электр. дан. – Заглавие с экрана. URL: http: //monitoring. law.edu.ru /otchety/ 2014/ fevral_ 2014_goda/#_edn50 (дата обращения 20.01.2020).

45. Саматов К.М. Персональные данные как институт права/К.М. Саматов// В сборнике: Новые вопросы в современной науке Материалы Международной (заочной) научно-практической конференции. под общейредакцией А.И. Вострецова. – 2017. – С. 297-230

46. Сергиевич В.А. Проблемы становления и развития института «право быть забытым»/ В.А. Сергиевич, И.В. Смолькова. Проблемы охраняемой законом тайны в уголовном процессе. – М.: 1999. – 346 с.

47. Сосна Б.И., Аворник Г.К. Возмещение морального вреда, причиненного нарушением социальных прав работника // Безопасность бизнеса. – 2004. – № 2. – С.23-25.

48. Статуева К.Е. Правовые основы международного регулирования защиты персональных данных работников: проблемы интерпретации // Сборник материалов XVI всероссийской студенческой научно-практической конференции с международным участием « Актуальные проблемы науки в студенческих исследованиях». – 2015. – С. 130-133.

49. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды института государства и права российской академии наук. – 2018. – № 5. С. 117-150.

50. Тимиршаяхов С.Ю. Правовые проблемы защиты информации при обработке персональных данных/ С.Ю. Тимиршаяхов, Ю.В. Тимиршаяхова // Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. – 2017. – С. 747–750.

51. Тогузова М.Б., Гайтова Л.Х. Ответственность за нарушение норм, обеспечивающих защиту персональных данных (в трудовых правоотношениях) // Аграрное и земельное право. – 2019. - № 1 (169). – С. 84-86.

52. Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 № 197-ФЗ (ред. от 16.12.2019) – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

53. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 18.02.2020).

54. Усманова Е.Ф. Проблемы и особенности формирования правовой культуры в современном правовом государстве / Е.Ф. Усманова// Инновационные тенденции, социально-экономические и правовые проблемы взаимодействия в международном пространстве. Саранск. – 2016. – С. 235–237.

55. Федосин А.С. Проблемы формирования государственно-правового механизма защиты конституционных прав граждан при обработке их персональных данных в автоматизированных информационных системах // Бизнес в законе. - 2007. - № 3. - С. 251-255.

56. Феофилактов А.С. Особенности компенсации морального вреда как способа защиты трудовых прав работника // Трудовое право. - 2010. - № 1. - С.36.

57. Шведов А.Л. Право работника на компенсацию морального вреда // Адвокат. - 2005. - № 3. - С. 24-27.

58. Bennett-Alexander Dawn, Laura Hartman. Employment Law for Business. – 870 p.

59. Beigner B. Le droit de la personnalité / B. Beigner // Collection “Que sais-je?” – P.U.F., 1992. – n°2703; Hustinx, P.J. Right to privacy and data protection: mission impossible? / P.J. Hustinx // European Data Protection Day. – 2010. – 28 January. – (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa384). – Дата обращения: 02.04.2017.

60. Banisar D. National Comprehensive Data Protection / D. Banisar // Privacy Laws and Bills. – 2016. – 28 Nov. – (https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416). – Дата обращения 02.05.2017.

61. Pailler L. Les reseaux sociaux sur Internet et le droit au respect de la vie privee. Bruxelles: Larcier, 2012.

62. Tsoukalas I.A., Siozos D.P. Privacy and Anonymity in the Information Society — Challenges for the European Union // The Scientific World Journal. 2011. №. 11. P. 458.