Министерство образования и науки Российской Федерации
«Южно –Уральский государственный университет»
Юридический институт
Кафедра «Трудовое, социальное право и правоведение»

ДОПУСТИТЬ К ЗАЩИТЕ
Зав.кафедрой ТСПиП
к.ю.н., доцент
_____Г.Х. Шафикова
_____ 2017 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧАСТНИКОВ КОРПОРАТИВНЫХ ОТНОШЕНИЙ

ЮУрГУ – 40.03.01.2017. – 013 –1401 – 043 – Ю – 453

Научный руководитель выпускной
квалификационной работы
доцент кафедры
_____Шафиков А.М.
_____2017 г.

Автор выпускной
квалификационной работы
студент группы Ю–453
_____Калашников О.А.
_____ 2017 г.

Нормоконтролер
доцент кафедры
_____Филиппова Э.М.
_____2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

Информация, непосредственно связанная с конкретным человеком (факты его биографии, номинативные (назывные) данные, национальность, место жительства, сведения о заболеваниях, о профессиональных знаниях и навыках, о семейной жизни, привычках, увлечениях, нравственные, политические, сексуальные и религиозные пристрастия и многое другое составляет большую или даже большую часть циркулирующей в обществе информации. Человек оставляет соответствующие «информационные следы» в отделах кадров, в социальных службах, органах исполнительной власти, в сфере услуг, различных организациях. Очень часто сообщение подобной информации находится в рамках интересов самого индивида или является необходимым условием получения конкретного социального статуса либо определенных услуг. Распространение такой информации без согласия самого человека может способствовать формированию его положительного имиджа, а может нанести непоправимый урон, моральный или материальный вред.

Особенно важно значение стоит уделить информационной безопасности в сфере защиты персональных данных участников корпоративных отношений. Хозяйственное общество в процессе осуществления своей деятельности сталкивается с необходимостью обработки персональных данных не только своих работников, но и особой категорией лиц, с которыми общество также находится в постоянных отношениях, — его акционеров и членов органов управления и контроля. Несмотря на то, что в последнее время тема обработки персональных данных востребована, вопросы защиты персональных данных участников корпоративных отношений, по большей части работников, остаются наименее проработанными, особенно в тех случаях, когда это касается обработки персональных данных членов органов правления.

Несмотря на наличие отдельных судебных актов, которые отказывают акционерам в получении конфиденциальной информации, в настоящее время очевидным образом прослеживается превалирующая направленность судебной

практики в защиту прав акционеров на получение такой информации. Особенно важно стоит отметить то, что персональные данные генерального директора используются на практике гораздо чаще, чем данные любого другого сотрудника. Однако, это не удивительно, ведь генеральный директор действует от имени общества, имеет право представлять интересы общества, делегировать другим работникам полномочия на осуществление определенных действий, которые непосредственно связаны с деятельностью общества. Персональные данные генерального директора могут содержаться в различных документах, например, в доверенностях на исполнение обязанностей, договорах, распорядительных документах, анкетах.

В соответствии законодательством передача персональных данных работника третьей стороне без письменного согласия сотрудника запрещена, за исключением предусмотренных законом случаев. Генеральный директор общества признается работником, на него распространяются все положения трудового законодательства. С ним, как и с другими сотрудниками, заключается договор, издается приказ о его назначении, соответствующие записи о трудовых отношениях вносятся в трудовую книжку.

Актуальность данной работы обуславливается тем, что у акционеров возрастает потребность в запросе персональных данных работников общества в целях защиты своих законных прав и интересов. Однако, общество не вправе предоставлять такие данные в целях защиты интересов работников. Таким образом, возникает конфликт двух сторон, за разрешением которого акционеры зачастую обращаются в судебные органы.

Проблемами информационной безопасности в сфере защиты персональных данных участников корпоративных отношений, в частности работников общества на сегодняшний день занимается достаточное количество ученых, к числу которых можно отнести: И. В. Михайлюк, В.Г. Дасько, М.А. Важорова, В.Н. Белова, А.В. Минбалеев, У.М. Станскова и другие исследователи.

Основной проблематикой данной работы является то, что акционеры общества имеют право запрашивать информацию о самом общества, в том числе и документы, которые содержат персональные данные работников. Защита данной информации является одним из наиболее сложных вопросов, возникающих при обеспечении защиты персональных данных в акционерном обществе. Ее возникновение обусловлено столкновением разнонаправленных интересов двух категорий субъектов: с одной стороны, субъектов персональных данных, заинтересованных в обеспечении их конфиденциальности, с другой — интересов акционеров, заинтересованных в получении наиболее полной информации об обществе.

Именно поэтому тема настоящей выпускной квалификационной работы выбрана с той целью, чтобы всесторонне изучить данную правовую категорию персональных данных участников корпоративных отношений в отношении работников (персонала) и лиц, занимающих управленческие должности, выявить и произвести анализ современных позиций ученых по вопросам, связанных с обеспечением защиты персональных данных, произвести обобщение судебной практики по данному вопросу и внести предложения об устранении пробелов и коллизий.

Цель настоящего исследования состоит в проведении комплексного научного анализа теоретических и практических проблем в области защиты персональных данных участников корпоративных отношений, уделяя особое внимание проблеме обеспечения конфиденциальности персональных данных работников общества при запросах таких данных акционерами.

Объектом исследования являются правовые отношения по предоставлению персональных данных работников, возникающие при реализации своих прав акционерами.

Предметом исследования являются правовые нормы, которые определяют понятие, содержание персональных данных, а также условия и принципы их обработки.

В целях реализации подробного рассмотрения данной проблемы были обозначены такие задачи:

1) Изучить научную литературу и законодательство в сфере информационной безопасности;

2) Раскрыть правовую сущность персональных данных;

3) Охарактеризовать защиту персональных данных работника;

4) Изучить, классифицировать и дать понятие участникам корпоративных отношений;

5) Выявить проблемы при использовании и обработке персональных данных работника в корпоративных отношениях;

6) Определить направления дальнейшего совершенствования правового регулирования защиты персональных данных участников корпоративных отношений.

Методологическую основу исследования составляют различные общенаучные и частные методы познания: диалектический, историко–правовой, логический, сравнительно–правовой, метод системного подхода и анализа.

Нормативной базой исследования явились международно–правовые акты, Конституция Российской Федерации, законы и подзаконные нормативные правовые акты, а также материалы правоприменительной практики.

Практическая значимость данного исследования заключается в разработке конкретных предложений по разрешению двустороннего конфликта конфиденциальности персональных данных работников общества в целях устранения пробелов и коллизий.

Цели и задачи исследования предопределили следующую структуру данной дипломной работы: Введение, две главы, заключение, список использованной литературы.

# ГЛАВА 1 ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1.1 Понятие и виды персональных данных

В настоящее время у человечества появляется все больше новых объектов, которые нуждаются в защите путем закрепления соответствующих норм в законе. Основной объект на сегодняшний день – это информация. В наше время общество в большинстве ситуаций зависит от получаемых, обрабатываемых и передаваемых данных. Таким образом, данные становятся высоко оцениваемым объектом.

Институт персональных данных считается еще молодым по правовым меркам институтом. Его развитие неотъемлемо связано со становлением конституционных прав и свобод человека и гражданина, в том числе, и с правом на неприкосновенность частной жизни[1].

Важно отметить, что самостоятельное право на неприкосновенность частной жизни как юридическая категория зародилась в США. Одна из первых попыток сформулировать суть понятия «частная жизнь» была предпринята в 1890 году не малоизвестными американскими юристами Сэмюэлем Уорреном и Луисом Брандейсом, которые в свою очередь определили его как «the right to be alone» – право быть оставленным в покое или же право быть предоставленным самому себе[2]. В их статье «Право на приватность», изданной в Гарвардском правовом журнале он утверждали, что сама суть приватности подвергается огромной опасности со стороны новейших изобретений и нестандартных способов ведения бизнеса, и таким образом обосновывали необходимость создания специального «права приватности» или «права частной жизни».

---

[1]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. 34.

[2]Балашкина И.В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации // Право и политика. – 2007. – №7. – С. 95.

Учитывая скорость и темпы развития научного и технического прогресса в целом мы все больше убеждаемся в справедливости указанных положений.

В настоящее время защите персональных данных уделяют особо важное значение. Таким образом, нормативные акты, регулирующие защиту персональных данных предусмотрены как национальным законодательством, так и различными международными актами.

Одним из основных международных актов, построивших фундамент для развития законодательства в сфере персональных данных является Конвенция о защите прав человека и основных свобод принятая 10 декабря 1948 года. В ней говорится, что «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»[1].

Право на защиту и неприкосновенность личной жизни содержится также и в Конвенции о защите прав человека и основных свобод, которая гласит что «Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц».[2] Данная Конвенция была принята Советом Европы 4 ноября 1950 года в г. Риме. Российская Федерация же ратифицировала ее немного позже, приняв Федеральный закон № 54–ФЗ от 30 марта 1998 года.

[1]Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. – 1995. – № 67.
[2]Конвенция о защите прав человека и основных свобод от 4 ноября 1950г. // Собрание законодательства Российской Федерации. – 1998. – № 20. – Ст. 2143.

Через некоторое время положив в свою основу Всеобщую декларацию прав и свобод человека был принят Международный пакт о гражданских и политических правах в декабре 1966 года в г. Нью–Йорке[1]. В последствии данный пакт был подписан СССР в марте 1968 года.

Спустя определенный период, Директива о защите неприкосновенности частной жизни и международных обменов персональными данными от 23 сентября 1980 года узаконила основные принципы неприкосновенности частной жизни и личностных свобод[2]. В директиве заключались такие положения, как:

– объем собираемых персональных данных должен ограничиваться пределом;

– персональные данные должны соответствовать целям, ради которых они будут использоваться;

– запрет на разглашение персональных данных.

Все эти международные правовые акты послужили основой для создания многих национальных правовых систем в области защиты персональных данных. В Российской Федерации, в том числе и в соответствии с международными правовыми актами, сохранность и защита персональных данных обеспечивается отечественным законодательством.

Таким образом, Россия, является прямым правопреемником принятых еще в Советском Союзе международных правовых договоров, которые в соответствии с ч. 4 ст. 15 Конституции Российской Федерации[3] (далее Конституция РФ) являются составной частью российской правовой системы. Так в ч. 1 ст. 23 Конституции РФ прямо указывается, что «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту

---

[1]Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. – 1976. – № 17. – Ст. 291

[2]Кафтанникова В.М. Принципы защиты персональных данных в России и за рубежом // Вестник ЮУрГУ. Серия: Право. – 2013. – №2. – С. 99.

[3]Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с поправками от 21 июля 2014 г.) // Российская газета – 1993. – 25 декабря.

своей чести и доброго имени». Важно отметить, что в соответствии со ст. 2 Конституции РФ «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства». Таким образом, государство не только устанавливает право, но также и обязуется защищать это право. Неотъемлемо сказать, что и ст. 24 Конституции РФ, где говорится что «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Данная норма ограничивает использование информации о частной жизни лица, что безукоризненно служит фундаментом для реализации защиты персональных данных.

Все вышесказанное служит для того, что Конституция РФ обладает высшей юридической силой и ее прямое воздействие применяется на всей территории Российской Федерации, а также что любые законы, которые применяются в стране не должны противоречить Конституции.

Один из основных и особо значимых нормативно–правовых актов в области информационной безопасности в сфере защиты персональных данных был принят 27 июля 2006 года. История Федерального закона «О персональных данных[1]» (далее закон о персональных данных) началась в далёком 1981 году, когда Совет Европы опубликовал Конвенцию о защите физических лиц при автоматизированной обработке персональных данных»[2]. Конвенция подразумевает, что страна, которая подписала документ, имеет право предъявлять собственные технические требования к защите и обработке персональных баз данных своих контролёров, то есть компании, которые обрабатывают персональные данные. Стоит учесть, что для полной реализации этого страна должна принять закон о персональных данных, который бы эти требования закреплял. Закон о персональных данных был принят 27 июля 2006

[1]Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.
[2]Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. – 2014. – № 5. – Ст. 419.

года и получил порядковый номер 152. В нем перечислены организационные меры, такие как назначение ответственных, разработка набора корпоративных документов, регистрация в реестре операторов персональных данных.

В соответствии со ст. 2 закона о персональных данных его целью «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». Данный закон, также, раскрывает понятие «персональных данных», закрепляет принципы и условия обработки персональных данных, права субъектов персональных данных, права и обязанности операторов, и ответственность за нарушение требований вышеуказанного Федерального закона.

Говоря об информационной безопасности в сфере защиты персональных данных необходимо выделить и Федеральный закон «Об информации, информационных технологиях и о защите информации»[1] (далее закон об информации) принятый 27 июля 2006 года так как любые персональные данные являются информацией. Стоит отметить, что данный закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, а также закладывает правовые начала для обеспечения защиты информации.

Прежде чем раскрыть понятие персональных данных необходимо дать определение информации. Так, согласно закону об информации в соответствии со ст. 2 под информацией понимается «сведения (сообщения, данные) независимо от формы их представления». В свою очередь информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, и на информацию, доступ к которой ограничен федеральными законами или же информация ограниченного доступа. Можно сделать вывод, что под общедоступной информацией понимается информация, которую

[1]Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

трудно скрыть от общества. Ярким примером может послужить информация о состоянии окружающей среды или о деятельности органов государственной власти. Под информацией ограниченного доступа понимается та информация, которая представляет некую ценность для ее владельца, доступ и защита которой ограничивается федеральным законодательством. Необходимо отметить и то, что информация ограниченного доступа подразделяется на информацию, которая составляет государственную тайну и информацию, соблюдение конфиденциальности которой установлено федеральными законами или ее еще называют «конфиденциальная информация».

Говоря о персональных данных не стоит забывать и о персональных данных работника. Трудовые отношения в Российской Федерации и в государствах–участниках СНГ, которые входили в состав СССР в качестве союзных республик, в 70–90–х годах регулировались Основами законодательства о труде СССР 1970 года. Также, на каждую союзную республику распространялся свой Кодекс законов о труде (далее КЗоТ), который соответствовал Основам законодательства СССР.

Кодекс законов о труде РСФСР[1](далее КЗоТ РСФСР) был принят 9 декабря 1971 года. В КЗоТ РСФСР, как и в остальных кодексах других союзных республик, отсутствовала специальная глава, которая была бы посвящена персональным данным работника. Тем не менее во всех кодексах содержалась специальная статья, которая прямо запрещала требовать при приеме на работу любые документы, содержащие в себя персональные данные работника, помимо тех, которые были предусмотрены законодательством.

В настоящее время данная сфера отношений регулируется гл. 14 Трудового кодекса Российской Федерации[2] (далее ТК РФ). В данной главе устанавливается порядок работы с персональными данными работника, общие

[1]Кодекс законов о труде Российской Федерации (утв. ВС РСФСР 9 декабря 1971 г.) // Ведомости ВС РСФСР. – 1971. – № 50. – Ст. 1007. (утратил силу)
[2]Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197 - ФЗ // Российская газета. – 2001. – № 256.

правила регулирования процесса обработки персональных данных, ответственность работодателя за нарушение информационной безопасности персональных данных. Раскрывая данный вопрос, стоит сказать, что в процессе трудовой деятельности, а также при приеме на работу, работодатель начинает собирать персональные данные работника и тем самым создавая некий «архив данных» работника, которые составляют личное дело работника. Информация, содержащаяся в личном деле, зачастую носит конфиденциальный характер. Такая информация о работнике или его персональные данные представляет собой сведения о фактах, событиях и иных обстоятельствах жизни и деятельности работника, по средствам которых возможно идентифицировать его личность[1].

В юридической литературе классификация охраняемой законом информации или сведений крайне неоднозначна. Так, Сизоненко А.Б. в соответствии с законодательством подразделяет информацию на общедоступную и ограниченного доступа[2]. К общедоступной информации он относит «общеизвестные сведения и иную информацию доступ к которой неограничен». Под информацией ограниченного доступа он понимает «информацию, возможность получения и использования которой ограничивается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства». В свою очередь, Сизоненко А.Б. классифицирует информацию ограниченного доступа на государственную тайну, коммерческую тайну, персональные данные, личная (семейная) тайна, служебная тайна, профессиональная тайна, тайна следствия и судопроизводства и на тайну сведений о защищаемом лице.

---

[1]Анисимов Л.Н. Персональные данные работника: Требование к передаче // Справочник кадровика. – 2006. – №7. – С. 25

[2]Сизоненко А.Б. Классификация информации ограниченного доступа в соответствии с законодательством Российской Федерации // Вестник КРУ МВД России. – 2010. – №4. – С. 93.

Стоит отметить мнение Копылова В.А., который утверждает что информацию о гражданах или персональные данные создаются самими гражданами в процессе их повседневной деятельности, которые в том числе связаны с реализацией прав и свобод (к примеру, право на труд, на медицинской обслуживание) и выполнением обязанностей и представляются как сведения о своей личности различным субъектам[1].

Также, Мазуров В.А. классифицируют информацию на информацию открытого доступа, ограниченного доступа (семейная тайна, профессиональная тайна, служебная тайна) и на государственную тайну[2].

Все вышесказанное подтверждает тот факт, что в научной литературе не существует единого мнения по поводу персональных данных. Особенно остро стоит вопрос об информации ограниченного доступа и ее классификации.

Российским законодательством термин «персональные данные» был впервые рассмотрен нормами федерального закона от 27 февраля 1995 года №24–ФЗ «Об информации, информатизации и защите информации»[3]. К так называемой информации о гражданах (то есть персональным данным) законодательством были отнесены «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность». В соответствии с этим определением субъектами персональных данных являлись исключительно граждане государства, а информация о лице без гражданства не подпадала под понятие «персональных данных». Также, стоит сказать, что персональные данные не были классифицированы на виды и все без исключения относились к категории конфиденциальной информации.

В настоящее время в законодательстве прослеживает другой подход к определению понятия «персональных данных». Так, в соответствии со ст. 3

---

[1]Копылов, В.А. Информационное право– М.: Юристъ, 2002. – С. 324.

[2]Мазуров, В.А. Уголовно-правовые аспекты информационной безопасности: учебное пособие – Барнаул: Изд-во Алт. Ун-та, 2004. – С. 244

[3]Федеральный закон от 20 февраля 1995 г. №24-ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства РФ. –1995. – № 8. – Ст. 609. (утратил силу)

законом о персональных данных под персональными данными понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

Мы считаем, следует отметить такой положительный момент в ныне действующем законодательстве как расширение субъектного состава: субъектами персональных данных являются физические лица. Данная тенденция во многом упрощает процесс формирования и фиксации персональных данных на практике.

Прежде чем привести классификацию персональных данных стоит упомянуть о том, что в научной литературе встречается разграничение классификаций в зависимости от природы персональных данных физического лица и в зависимости от информационной системы персональных данных[1].

Таким образом, в соответствии с законом о персональных данных можно отследить два подхода к классификации персональных данных:

– в зависимости от содержания обрабатываемых персональных данных;

– в зависимости от вида обработки персональных данных.

Законодатель в зависимости от подхода к классификации персональных данных устанавливает либо дополнительные ограничения на основании обработки персональных данных, либо вовсе вводит особенности обработки таких персональных данных.

Тем не менее, законодатель в зависимости от содержания обрабатываемых персональных данных классифицирует на:

– специальные категории персональных данных, под которыми понимается закрытый перечень данных приведенный в ст. 10 закона о персональных данных, который включает в себя «персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни»;

[1]Белгородцева Н.Г. Теоретико-правовые аспекты защиты персональных данных: дис. ... канд.юрид. наук. – М., 2012. – С. 129.

– общедоступные персональные данные, которые сделаны общедоступным для субъекта способом, под которым в законодательстве понимается процедура письменного согласия субъекта на обработку персональных данных.

Большинство ученых также выделяют и иную специальную категорию. Так в соответствии с ч. 3 ст. 10 законом о персональных данных «Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами», что подразумевает под собой особые требования к обработке персональных данных связанных с судимостью физического лица.

В зависимости от видов и целей обработки персональных данных выделяют:

– биометрические персональные данные, под которыми в соответствии с ч. 1 ст. 11 законом о персональных данных понимаются «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных»;

– трансграничные персональные данные, которые в соответствии с ч. 1 ст. 12 закона о персональных данных представляют собой «трансграничную передачу персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим

Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства»

## 1.2 Принципы и условия обработки персональных данных

В соответствии со ст. 3 закона о персональных данных под обработкой персональных данных понимается «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных». В свою очередь, в соответствии с той же статьей, под распространение персональных данных подразумеваются «любые действия, направленные на раскрытие персональных данных неопределенному кругу лиц».

Важно сказать, что общие принципы обработки персональных данных были приведены еще в Директиве 95\46\ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 года «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных». В Директиве говорится о том, что государства –участники обязаны обеспечивать обработку персональных данных только в случаях, если:

– субъект обработки персональных данных дал свое согласие;

– обработка персональных данных необходима для исполнения обязательств, в которых субъект обработки персональных данных является одной из сторон;

– обработка персональных данных требуется для исполнения юридического обязательства;

– обработка персональных данных необходима для защиты частной жизни субъекта;

– обработка необходима в целях обеспечения законных интересов контролера или третьей стороны (сторон).

Принципы обработки персональных данных заключены в положениях ст. 5 закона о персональных данных и важно отметить, что принципы, которые были сформулированы еще до внесения в нее поправок Законом№ 261–ФЗ[1], были достаточно расплывчатыми. В ныне действующей редакции закона о персональных данных принципы сформулированы более четко и конкретно. Вышеуказанная статья берет свои начала из норм Конституции РФ. Так, в ст. 24 Конституции РФ прямо установлены запрет на хранение, сбор, использование и распространение информации о частной жизни лица без его согласия, в том числе и обязанность со стороны органов государственной власти, органов местного самоуправления, их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы. Кроме этого, согласно ч. 4 ст. 29 Конституции РФ «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Конституция РФ формирует и закрепляет фундаментальные основы правового регулирования обработки персональных данных.

Таким образом, в соответствии с ч. 1 ст. 5 закона о персональных данных «обработка персональных данных должна осуществляться на законной и справедливой основе». Данный принцип подразумевает под собой то, что, осуществляя обработку персональных данных, операторы обязаны исполнять все требования действующего законодательства в области защиты

[1]Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. – 2011. – № 31. – Ст. 4701.

персональных данных, а также соответствовать принципам справедливости по отношению к субъекту персональных данных. То есть, оператор, осуществляя обработку персональных данных должен придерживаться таких правил:

– полное обеспечение конфиденциальности персональных данных;

– запрет передачи персональных данных третьим лицам без согласия субъекта данных;

– обеспечение защиты от несанкционированного доступа и распространения персональных данных;

– субъект персональных данных должен иметь возможность знакомиться с данными.

В соответствии с ч. 2 ст. 5 закона о персональных данных «обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных». Таким образом, давая согласие на обработку персональных данных, субъект таких персональных данных обязан быть проинформирован о целях обработки. Также, такие цели обработки обязательно должны быть включены в форму согласия на обработку персональных данных субъекта.

Стоит упомянуть, что в юридической практике имеет место быть то, что при заключении гражданско–правовых договоров субъекты соглашаются на распространение персональных данных третьим лицам[1]. Однако при заключении такого договора неправомерно требовать у субъекта согласия на распространение его персональных данных, если распространение не обусловлено самим договором или же в силу требований законодательства.

В соответствии с ч. 3 ст. 5 закона о персональных данных «не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой». Данное положение о том, что совмещать базы данных с персональными

[1]Федеральный закон «О персональных данных»: научно-практический комментарий. / под ред. А.А. Приезжевой. – М.: Редакция «Российской газеты», 2015. – Вып. 11. – С. 87.

данными, которые обрабатываются в различных целях представляется нам очевидным. Но не стоит забывать о том, что обработке в данном случае подлежат только персональные данные, которые в полном объеме отвечают целям такой обработки. О данном принципе говорится в ч. 4 ст. 5 закона о персональных данных. Другими словами, для достижения поставленных целей оператор прибегает к обработке исключительно тех данных, которые собраны в целях достижения определенных задач. Ярким примером может послужить то, что работодатель обрабатывает персональные данные работников, которые состоят с ним в трудовых отношениях.

Одним из ключевых принципов законодательства в области персональных данных служит принцип, согласно которому «содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки» в соответствии с ч. 5 ст. 5 закона о персональных данных. Стоит учесть, что законодатель разграничивает понятия «объем персональных данных» и «содержание персональных данных». Таким образом, под содержанием понимается то, что наполняет данные и то, из чего они состоят, то есть именно те данные, которые определяют внутреннее наполнение отдельно взятой категории данных. К примеру, место жительства субъекта персональных данных будет содержать совокупность сведения о стране, городе, улице, доме, квартире, индексе.

В свою очередь объем персональных данных представляет собой количественный показатель. Например, перечень сведений, содержащий персональный данные в целом (к примеру имя, фамилия, дата и место рождения)[1].

Также, остаются актуальными вопросы, которые связанные с избыточностью обрабатываемых персональных данных касательно их целей

[1]Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: дис. ... канд. юрид. наук. – Челябинск, 2010. – С. 110.

обработки. Тем не менее действующее законодательство не содержит критериев избыточности обрабатываемых данных. Однако, мы считаем, что избыточность персональных данных представляет собой нецелесообразность превышения объема обработки персональных данных, который установлен законом или договором.

В соответствии с ч. 6 ст. 5 закона о персональных данных «при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных». Исходя из вышеуказанного, под достаточностью персональных данных мы понимаем то, что данные должны быть полно предоставлены оператору в зависимости от поставленных для таких данных целей и задач и ни в коем случае не превышающие заранее определенный объем.

Систему принципов обработки данных завершает основополагающие положения, относящееся к хранению персональных данных. Так, в ч. 7 ст. 5 закона о персональных данных закреплены требования к длительности хранения персональных данных, а также к порядку завершения такого хранения. Законодатель устанавливает, то хранение персональных данных требуется осуществлять в форме, которая позволяет определить субъект персональных данных не дольше, чем этого требуют цели обработки персональных данных в случаях, если срок хранения таких персональных данных не установлен федеральным законом или договором. Также, обрабатываемые персональные данные подлежат уничтожению или обезличиванию при достижении целей их обработки или же в случаях утраты необходимости в достижении этих целей.

Условия обработки персональных данных закреплены в ст. 6 закона о персональных данных. Данная статья определяет ситуации, при которых

допускается обработка персональных данных, то есть устанавливает условия легитимности деятельности операторов по обработке персональных данных.

Основополагающем положением является п. 1 ч. 1 вышеуказанной статьи, в соответствии с которым необходимым условием обработки персональных данных является наличие согласия субъекта персональных данных на обработку таких данных. Учитывая правоприменительную практику, обработка персональных данных в других случаях не требует согласия субъекта, если иное не предусмотрено федеральными законами. Однако, в постановлении Первого арбитражного апелляционного суда от 12.10.2011 № 01АП–4438/11 говорится о том, что получение согласия субъекта (абонента) на обработку персональных данных, за исключением случаев, установленных действовавшими на момент рассмотрения спора Правилами оказания услуг подвижной связи, утвержденными постановлением Правительства РФ от 25.05.2005 № 328, является обязательным.

Согласно п. 2 ч. 1 ст. 6 закона о персональных данных «обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей».

В настоящее время действует большое количество международных договоров, которые регламентируют порядок и условия обработки персональных данных в различных сферах жизнедеятельности, в том случае и при оказании таких услуг как авиаперевозки, осуществлении реадмиссии, оказании правовой и судебной помощи.

Таким образом, обработка персональных данных в пределах указанных договоров может не только закреплять условия, не схожие с положениями закона о персональных данных, но также и не ставить под сомнение сам факт правомерности осуществления вышеуказанной деятельности.

Касательно условий обработки персональных данных служащих для исполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей важно отметить, что под законодательством Российской Федерации понимается, в широком смысле, совокупность не только законов, но и иных нормативных правовых актов, принимаемых как Президентом РФ, Правительством РФ, министерствами так и их ведомствами, уполномоченными на их принятие.

Ярким примером может послужить то, что в соответствии со ст. 65 ТК РФ при поступлении на работу данные положения обязывают гражданина предоставить работодателю такие документы, как: паспорт или иной документ, который удостоверяет личность, трудовую книжку, страховое свидетельство, документы воинского учета, документ об образовании, справку о наличии или отсутствии судимости. То есть, обработка вышеуказанных сведений при выполнении работодателем возложенных на него трудовым законодательством обязанностей, в том числе и связанных с их передачей в налоговые органы, внебюджетные фонды, подпадает под вышеуказанное основание и, как правило, не требует согласия работника на обработку его персональных данных[1].

Стоит отметить, что такое основание обработки персональных данных необходимая для исполнения полномочий соответствующих органов власти, в том числе и внебюджетных фондов, и функций организаций преимущественно участвующих в предоставлении государственных и муниципальных услуг, которые предусмотрены в соответствии с Федеральным законом от 27.07.2010 № 210–ФЗ «Об организации предоставления государственных и муниципальных услуг»[2] (далее закон об организации предоставления государственных и муниципальных услуг), в том числе и включая регистрацию

[1]Тихомирова Л. В. Защита персональных данных работника: учеб.-практ. пособие. – М., 2013. – С. 35.

[2]Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ. – 2010. –№ 31. – Ст. 4179.

субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг, взаимосвязано с положениями ч. 4 ст. 7 вышеуказанного закона, в соответствии с которой «органам, предоставляющим государственные и муниципальные услуги, и иным органам, участвующим в предоставлении государственных и муниципальных услуг, согласия получателя услуг как субъекта персональных данных не требуется». Важно отметить, что под данное основание также подпадает межведомственное взаимодействие, которое связанно с передачей персональных данных в целях предоставления государственных и муниципальных услуг.

В тех ситуациях, когда для предоставления государственной или муниципальной услуги требуется обработка персональных данных лица, который не является заявителем, и в том случае если в соответствии с данным федеральным законом обработка таких персональных данных может осуществляться с согласия указанного лица, то при обращении за предоставлением государственной или муниципальной услуги заявитель в дополнение представляет документы, которые подтверждают получение согласия указанного лица или же его законного представителя на обработку персональных данных такого лица, о чем говорится в ч. 3 ст. 7 закона об организации предоставления государственных и муниципальных услуг». Необходимо сказать, что в таком случае основание, которое допускает обработку персональных данных без соответствующего согласия в пределах оказания государственных и муниципальных услуг, может распространяться на субъект персональных данных, которым помимо заявителя может быть и иное лицо.

В соответствии с п. 5 ч. 1 ст. 6 законом о персональных данных «обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по

инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем».

Тем не менее, в соответствии с пп. «д», «е», «ж» п. 20 Правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания, утвержденных постановлением Правительства РФ[1], при заключении договора с абонентом в обязательно требуется указать такие сведения об абоненте, как фамилия, имя, отчество, данные документа, удостоверяющего личность, адрес установки пользовательского оборудования, вид информирования о состоянии счета или оказанных услугах. Таким образом, любая компания, которая предоставляет услуги связи в пределах заключенного с субъектом персональных данных договора имеет полное право осуществлять обработку таких персональных данных.

Стоит сказать, что обработка персональных данных, которая необходима для осуществления прав и законных интересов оператора или третьих лиц во многом многогранна по своей правовой природе. Так, в пример можно привести право, принадлежащие на основании обязательства кредитору, которое в последствии может быть передано другому лицу по сделке в соответствии со ст. 382 Гражданского кодекса РФ от 30.11.1994 № 51–ФЗ[2] (далее ГК РФ) именуемое как уступка требования. То есть, кредитные организации вправе при возникновении долгового портфеля переуступить право требования третьему лицу без соответствующего согласия заемщика и в последствие передать персональные данные заемщика.

Немаловажным условием обработки персональных данных в соответствии с п. 9 ст. 6закона о персональных данных является и то, что «обработка персональных данных осуществляется в статистических или иных

[1]Постановление Правительства РФ от 22 декабря 2006 г. № 785 «Об утверждении Правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания» // Собрание законодательства РФ. – 2007. – № 1 (2 ч.). – Ст. 249.
[2]Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

исследовательских целях, при условии обязательного обезличивания персональных данных». В соответствии с вышеуказанным федеральным законом под обезличиванием персональных данных понимаются «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных».

Необходимо также отметить, что обезличивание персональных данных предусмотрено пп. «з» п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, которые предусмотрены законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»[1] (далее Постановление Правительства РФ от 21.03.2012 № 211). То есть, данный подпункт обязывает проводить обезличивание в тех случаях, которые определенны нормативными правовыми актами.

Еще одним из обязательных условий обработки персональных данных в соответствии с ч. 1 п. 11 ст. 6 закона о персональных данных является обработка таких «данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом».

В соответствии с ч. 3 ст. 6 закона о персональных данных вводится такое понятие, как «поручение оператора», которое, в свою очередь, предусматривает

---

[1]Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ. – 2012. – № 14. – Ст. 1626.

возможность передачи поручения обработки персональных данных оператором другому лицу при наличии следующих условий:

– необходимость согласия субъекта персональных данных на поручение обработки другому лицу;

– наличие договора, в том числе государственного или муниципального контракта, между оператором и третьим лицом, одним из условий которого является обработка персональных данных субъекта, либо соответствующего акта государственного или муниципального органа.

При этом в этой же части статьи закреплены требования к лицу, который осуществляет обработку персональных данных по поручению оператора. То есть, указанное лицо обязано соблюдать принципы и правила обработки персональных данных, которые предусмотрены законом о персональных данных.

Таким образом, в поручении оператора должен быть закреплен перечень действий или операций с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, а также цели такой обработки. Кроме этого, в нем должна закрепляться обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, в том числе должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 закона о персональных данных. Лицо, которое осуществляет обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку таких персональных данных. То есть, эта обязанность возложена исключительно на оператора. При отсутствии согласия субъекта персональных данных на поручение оператором обработки данных другому лицу оператор не вправе передавать данные субъекта. При несоблюдении существенных условий договора, содержащего поручение оператора, передача персональных данных субъектов для обработки третьим лицом также недопустима.

## 1.3 Информационная безопасность как фундаментальная основа защиты персональных данных

Основным системообразующим фактором и одним из феноменов конца XX начала XXI века является развитие информационного пространства и информационной сферы. Кириллов А.В. полагает, что современное информационное пространство отличается такими факторами как: увеличение количества информационных ресурсов, появление и становление новейших информационных технологий, преобладание количества населения, занимающегося интеллектуальным трудом.[1]

Информатизация общества предполагает, во–первых, широкое использование интеллектуального потенциала, который содержится в печатном фонде, включая научную, производственную и другие виды деятельности. Во–вторых, речь идет о внедрении информационных технологий в различные виды деятельности, которые способствуют развитию общественного производства и её интеллектуализации. В этот перечень можно отнести и достойный уровень информационного сервиса, т.е. возможность получить доступ к источникам проверенной информации и визуализировать её[2].

Важнейшим фактором, благодаря которому сегодня развивается информационное пространство является рыночная экономика, в которой отдельное место отводится информационным ресурсам. Информатизация современного общества способствовала развитию дискуссий в научной среде по проблемным вопросам обеспечения информационной безопасности. Стоит сказать, что информационная безопасность государства и личности – это одна из важнейших и фундаментальных проблем человечества.

---

[1]Кириллов А. В. Современные проблемы информационной безопасности личности // Известия РАРАН. – 2013. – № 1. – С. 106.

[2]Сайханова Х.И. Информатизация общества как одна из закономерностей современного социального прогресса // Международный журнал гуманитарных и естественных наук. – 2016. – № 1. – С. 195.

Некоторые авторы утверждают, что понятие «информационная безопасность» появилось в российской науке еще в 1990–х гг. XX в., однако исключительно применительно к защите компьютерной информации (баз данных, компьютерных сетей). Более того, Э. И. Атагимова и Р. М. Рамазанова уточняют, что государственное закрепление понятия «информационная безопасность» произошло еще в 1989 г., когда в соответствии с решением Президиума Верховного Совета СССР была организована рабочая комиссия по исследованию и совершенствованию системы национальной безопасности. Так огромную роль в исследовании проблематики информационной безопасности сыграл В. Н. Лопатин, возглавлявший в 1989–1990 г. рабочую группу, как раз отвечающую за вопросы информационной безопасности в составе этой комиссии. В целях наиболее точного определения предметной области законодательства в сфере обеспечения информационной безопасности было предложено выделить три подгруппы объектов защиты. К ним относились: защита информации и прав на нее (включая право на доступ к информации, право на тайну, права на объекты интеллектуальной собственности); защита человека и общества от воздействия «вредной» информации; защита информационных систем и прав на них (в том числе прав и интересов государства по сохранению единого информационного пространства в стране)[1].

Согласно положениям действующего законодательства, под информацией понимаются любые сведения (сообщения, данные) независимо от формы их представления. Как можно отметить, понятие «информация» в новом законодательстве было представлено в более общем виде. Считается, что такое определение лучше охватывает юридический характер данного термина, по сравнению с ранее действовавшим. Стоит отметить, что определить грань перехода отдельных сведений в полноценную информацию сложно, и, по –

[1]Атагимова Э. И. Некоторые аспекты законодательного уровня обеспечения информационной безопасности в Российской Федерации // Правовая информатика. – 2014. – № 2. – С. 15.

видимому, опираться следует на категорию их достаточности для возможности на их основе прийти к определенному умозаключению.

Нормативно–правовое регулирование деятельности по обеспечению безопасности, будь то любая сфере общественных отношений, является первоосновой. В нем (нормативно–правовом регулировании) прежде всего должны формироваться принципы, а на их основе уже и понятийный аппарат[1]. В настоящее время сфера обеспечения информационной безопасности характеризуется тем, что имеет лишь единственное упоминание терминологического аппарата, определенного на уровне законодательства.

Углубляясь в историю, необходимо отметить, что В 2010 г. на смену Федеральному закону «О безопасности» от 1992 г. был принят Федеральный закон № 390–ФЗ «О безопасности»[2]. В ст. 1 Закона «О безопасности» 1992 г. было сказано, что «безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Однако, ряд ученых имеют отличные взгляды от законодательства. Так, например, А. И. Стахов в своих трудах предлагает рассматривать безопасность в широком смысле, то есть в связи с политическими, экономическими, организационными, юридическими и иными негативными условиями и факторами[3]. Безопасность, по его мнению, представляет собой «урегулированное правом состояние защищенности конституционных и иных законных интересов личности, общества, государства и нации, при котором отсутствуют вредоносные природные и техногенные факторы окружающей среды, связанные с санкционируемыми и контролируемыми государством правомерными действиями (деятельностью) физических и юридических лиц по использованию предметов, явлений и процессов – техногенных и природных

---

[1]Майоров В.И. Проблемы обеспечения безопасности в информационной сфере // Вестник Челябинского государственного университета. – 2015. – № 13 (368). – С. 49.

[2]Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Собрание законодательства РФ. – 2011. – № 1. – Ст. 2.

[3]Стахов А. И. Административно-публичное обеспечение безопасности в Российской Федерации: монография. – М.: Юнити-Дана: Закон и право, 2006. – С. 13.

источников опасности конституционным и иным законным интересам, а также исключены правонарушения и юридические казусы, способствующие возникновению и (или) развитию вредоносных природных и техногенных факторов окружающей среды».

Рассмотренные выше понятия «безопасность» и «информация» являются основополагающими для определения категории «информационная безопасность», которая активно изучается правоведами.

В 2000 г. впервые были сделаны попытки законодательно дать понятие определению информационной безопасности, которые содержались в Доктрине информационной безопасности РФ от 2000 г.[1]. Доктрина содержала определение понятия информационной безопасности и формулировала его как «состояние защищенности ее (то есть Российской Федерации) национальных интересов в информационной сфере». Однако в данном случае присутствовала необходимость уточнения определения информационной безопасности, которая сохранялась в силу отсутствия или спорности законодательных формулировок.

На сегодняшний день, понятие информационной безопасности прямо включено в Доктрину информационной безопасности от 2016 года (далее Доктрина), которая утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[2]. Таким образом, в Доктрине информационной безопасности говорится, что под информационной безопасностью Российской Федерации (далее – информационная безопасность) понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и

[1]Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895) // Российская газета. – 2000. – № 187. (утратил силу)
[2]Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

устойчивое социально–экономическое развитие Российской Федерации, оборона и безопасность государства».

Также, в вышеуказанной Доктрине было заключено понятие обеспечения информационной безопасности, под которой понимается «осуществление взаимоувязанных правовых, организационных, оперативно–розыскных, разведывательных, контрразведывательных, научно–технических, информационно–аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления».

Однако, А. В. Минбалеев отмечает, что «интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность»[1].

Мы приходим к выводу о том, что можно согласиться с А. Н. Сагиндыковой и А. Л. Ховалевым, которые утверждают, «что защита – лишь одна из функций безопасности, наравне с такими, как снижение, ослабление, устранение и предупреждение опасности и угрозы[2]». Однако, стоит учесть то, что если понимать информационную безопасность как конечное состояние, то разумно говорить не о функциях безопасности, а о содержании обеспечения безопасности, которое как раз и выражается в вышеперечисленных средствах, закрепленных в Доктрине информационной безопасности РФ, достижения информационной безопасности. Таким образом, непосредственное обеспечение

[1]Минбалеев А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: монография – Челябинск: Цицеро, 2012. – С. 161.

[2]Сагиндыкова А. Н. Конституционно-правовая стабильность общества и государства РФ: состояние, проблемы, перспективы: монография – Екатеринбург: Урал. юрид. ин-т МВД России, 2003. – С. 65.

информационной безопасности осуществляется при помощи функций системы обеспечения информационной безопасности.

Говоря об информационной безопасности как фундаментальной основе защиты персональных данных необходимо определить понятие информационной безопасности личности, так как любые персональные данные есть информация об определенном человеке. Но прежде всего, необходимо выделить, что в ст. 2 Конституции РФ говорится о том, что признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Гарантии прав и свобод человека и гражданина включают условия, средства, меры, направленные на обеспечение осуществления, охрану и защиту этих прав и свобод.

К конституционным правам человека и гражданина в информационной сфере в соответствии с Конституцией РФ традиционно относят:

– право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29);

– запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ч. 1 ст. 24);

– предоставление каждому возможности ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, которую должны обеспечить органы государственной власти и органы местного самоуправления, их должностные лица, если иное не предусмотрено законом (ч. 2 ст. 24);

– право на достоверную информацию о состоянии окружающей среды (ст. 42).

Кроме того, следует учитывать положения ч. 1 ст. 55 Конституции РФ о том, что перечисление в Конституции РФ основных прав и свобод не должно толковаться как отрицание или умаление других общепризнанных прав и свобод человека и гражданина.

Так, мы приходим к выводу о том, что одной из мер обеспечения осуществления прав и свобод человека и гражданина в информационной сфере является поддержание необходимого уровня информационной безопасности и непосредственно одной из ее составляющих, как информационная безопасность личности.

Разделение в Доктрине информационной безопасности национальных интересов в информационной сфере на такие элементы, как интересы личности, общества и государства, можно понимать с определенной долей условности. То есть, применение термина «личность» в данном случае является несомненным синонимом понятия «человек», которое используется в нормативных правовых актах[1]. Важно отметить, что сама Доктрина утверждает, что интересы личности в информационной сфере содержатся в реализации конституционных прав человека и гражданина на свободный доступ к информации, на свободное использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, которая обеспечивает личную безопасность. Таким образом, реализация прав каждого человека в информационной сфере признается одной из составляющих информационной безопасности России. Поэтому мы считаем верным выделение А. А. Стрельцовым таких составляющих информационной безопасности России, как «информационная безопасность человека, общества и государства»[2].

По мнению С. В. Иванова, информационная безопасность личности – это «состояние высокой степени защищенности личности, при котором гарантируется реализация ее прав и свобод в информационной сфере, и

[1]Баринов С.В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. – 2016. – № 4 (65). – С. 101.
[2]Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред. В. А. Садовничего, В. П. Шерстюка – М.: МНЦМО, 2002. – С. 52-57.

максимально снижен риск негативного воздействия на нее внутренних и внешних угроз»[1].

Г. Г. Гафарова и В. В. Смелянская более критичны в подходе к размерам негативного воздействия и полагают, что информационная безопасность характеризуется прежде всего отсутствием угрозы причинения вреда информации, которой владеет личность и угрозы нанесения вреда личности информацией[2].

Таким образом, если считать, что информационная безопасность – это идеальная цель, на достижение которой направлены меры, предпринимаемые субъектами ее обеспечения, то подход Г. Г. Гафаровой и В. В. Смелянской следует признать более приемлемым. Введение С. В. Ивановым такого критерия информационной безопасности, как «максимальное снижение риска негативного воздействия», может быть использовано в качестве установления уровней информационной безопасности в каком–либо конкретном случае.

Однако, на наш взгляд нельзя считать удачным определение понятия информационная безопасность личности как состояние и условия жизнедеятельности личности, при которых бы реализовались информационные права и свободы человека. То есть, реализация информационных прав и свобод личности зачастую может реализоваться при негативных обстоятельствах, прямо или косвенно угрожающих ее интересам.

Необходимо отметить, что в содержании информационной безопасности личности ученые выделяют такие элементы:

– информационно–техническая безопасность, под которой понимается «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или

---

[1]Иванов, С. В. Правовое регулирование информационной безопасности личности в Российской Федерации // Вестник Екатерининского института. – 2014. – № 1 (25). – С. 50.

[2]Гафарова Г. Г. Информационная безопасность личности // Безопасность личности: состояние и возможности обеспечения: материалы междунар. науч.-практ. конференции 10-11 мая 2012 г. Ереван, Пенза, Колин – Социосфера, 2012. – С. 57.

искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры»[1];

– информационно–идеологическая безопасность, определяемая как уровень защищенности личности от предумышленного или непредумышленного информационного воздействия, обладающего результатом нарушения прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащие нравственным и этическим нормам, оказывающие деструктивное воздействие на личность, имеющие негласный (внечувственный, неосознанный) характер, внедряющего в общественное сознание антисоциальные установки[2];

– информационно–психологическая безопасность личности как «состояние защищенности ее психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно – ориентировочной основы социального поведения человека (и в целом жизнедеятельности в обществе), а также адекватной системы его субъективных (личностных, субъективно–личностных) отношений к окружающему миру и самому себе»[3];

– информационно–правовая безопасность личности как «состояние защищенности права человека искать, получать, передавать, производить и распространять информацию, а также права на неприкосновенность информации о частной жизни»[4].

---

[1]Галатенко В. А. Информационная безопасность // Открытые системы. – 1996. – № 1 (15). – С. 39.

[2]Ковалева Н. Н. Информационное право России: учеб. пособие. – М.: Дашков и Ко, 2007. – С. 110-111.

[3]Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты.– М.: Изд-во РАГС, 1998. – С. 15.

[4]Тамодлин А. А. Государственно-правовой механизм обеспечения информационной безопасности личности: дис. … канд. юрид. наук.– Саратов, 2006. – С. 34

Не останавливаясь более детально на различиях в трактовке приведенных выше элементов, стоит отметить, что попытки их теоретического обоснования являются безусловным доказательством сложности и многоаспектности правовой категории «информационная безопасность личности».

Мы приходим к выводу о том, что информационная безопасность является фундаментальной основой защиты персональных данных. То есть защита персональных данных базируется на основных элементах информационной безопасности личности. К примеру, такой элемент информационной безопасности личности как информационно–техническая безопасность раскрывается в законодательно закрепленных принципах обработки персональных данных, беря за основу защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера. В свою очередь, информационно–идеологическая безопасность личности находит свое отражение в основополагающем принципе обработки персональных данных, то есть «содержание и объем персональных данных должны соответствовать заявленным целям обработки». В свою очередь, информационно–правовая безопасность личности проявляется в защите и охране в соответствии с законом оператором персональных данных от непреднамеренного доступа третьих лиц.

# ГЛАВА 2 ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СФЕРЕ КОРПОРАТИВНЫХ ОТНОШЕНИЙ

## 2.1 Обеспечение защиты персональных данных участников корпоративных отношений с приоритетным направлением на работников корпорации

В соответствии с ГК под корпорациями понимаются юридические лица, учредители (участники) которых обладают правом участия (членства) в них и формируют их высший орган, являются корпоративными юридическими лицами (корпорациями). К ним относятся хозяйственные товарищества и общества, крестьянские (фермерские) хозяйства, хозяйственные партнерства, производственные и потребительские кооперативы, общественные организации, общественные движения, ассоциации (союзы), нотариальные палаты, товарищества собственников недвижимости, казачьи общества, внесенные в государственный реестр казачьих обществ в Российской Федерации, а также общины коренных малочисленных народов Российской Федерации.

Корпоративными отношениями прежде всего признаются отношения внутри самой корпорации между различными группами участников корпорации, между ними и профессиональным менеджментом, между директорами и менеджментом, между работниками и самой корпорацией[1]. Характер этих отношений зачастую различный, то есть это могу быть как отношения в сфере управления (которые в свою очередь шире, чем отношения внутриорганизационные), имущественные отношения (к примеру, определение размера вознаграждения членам совета директоров), отношения, связанные с трудовыми обязанностями работников в корпорации. В зависимости от того, как стабильно отлажены механизмы взаимоотношений внутри корпорации, зависит положение корпорации вовне: ее «прозрачность» и привлекательность

[1]Корпоративное право: учебник / под. ред. И.С. Шиткина. – М: КНОРУС, 2015 – С. 22.

для инвесторов. Поэтому, особенно важная составляющая корпоративных отношений – это внешние и внутренние отношения корпорации с партнерами, кредиторами, персоналом, биржами, специалистами фондового рынка, государственными органами, осуществляющими контроль над деятельностью корпорации[1].

Гутников О.В. выделяет таких участников корпоративных отношений как[2]:

– акционеры;

– служащие (работники корпорации);

– органы менеджмента;

– кредиторы;

– органы государственной власти и местного самоуправления;

– потребители и поставщики.

В целях данной работы особое внимание следует уделить таким участникам корпоративных отношений, как работники корпорации, в том числе органы управления и контроля. Стоит сказать, что под субъектами корпоративного управления понимаются органы управления и (или) должностные лица корпорации, которые в силу возложенных на них полномочий, являясь стороной управленческих отношений, осуществляют целенаправленное воздействие на объект корпоративного управления на основании заключенного с ними трудового договора[3].

Корпорация в процессе осуществления своей деятельности сталкивается с необходимостью обработки персональных данных как своих работников, так и

---

[1]Афанасьева Е.Г. Корпоративное право: учебник; отв. ред. И.С. Шиткина. 2-е изд., перераб. и доп. – М: КНОРУС, 2015 – С. 87.

[2]Гутников О. В. Содержание корпоративных отношений // Журнал российского права. – 2013. – №1 (193). – С. 27

[3]Шиткина И.С. Корпоративное право в таблицах и схемах. 2-е изд., перераб. и доп. – М.: Юстицинформ, 2016. – С. 234.

особой категории лиц, с которыми общество также находится в постоянных отношениях – его акционеров и членов органов управления и контроля[1].

Таким образом, в соответствии с законом о персональных данных любое акционерное общество обязано принимать меры по защите и охране персональных данных, при этом перечень таких мер оно вправе самостоятельно определять.

В связи с компьютеризацией сбора персональных данных о человеке, информация о работниках может стать в определенной мере открытой и привести к ущемлению их интересов и прав[2].

Стоит отметить, что любые взаимоотношения между акционерным обществом и работником регулируются ТК РФ. Так, в соответствии со ст. 86 ТК РФ под защитой персональных данных работника понимается обеспечение прав и свобод человека и гражданина, которые обязан соблюдать работодатель и его представители при обработке персональных данных работника.

В соответствии с п. 1 ст. 86 ТК РФ «обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества». Приведенные положения данной статьи в полной мере соответствуют основным международным актам о защите прав и свобод человека, в том числе Международному пакту о гражданских и политических правах от 1996 года, где говорится что «каждый имеет право на защиту закона от такого вмешательства или таких посягательств».

---

[1]Михайлюк И.В. Защита персональных данных участников корпоративных отношений // Журнал «Акционерное общество вопросы корпоративного управления». – 2012. – №9. – С. 71

[2] Шафикова Г.Х. К вопросу о защите персональных данных работника – Челябинск: ЮУрГУ. Сборник научных трудов «Региональная информационная экономика». – 2002. – С.359.

Не стоит забывать о том, что «при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами». Иными словами, объем и содержание обрабатываемых персональных данных не должны превышать поставленные перед такой обработкой цели.

Осуществляя деятельность по трудоустройству работников в корпорацию, специально созданные для этого органы в соответствии с п. 3 ст. 86 ТК РФ имеют право получать все персональные данные работника исключительного у него самого. В случае, если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Таким образом, созданные органы корпорации должны сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

В соответствии со ст. 3 закона о персональных данных, под оператором понимается «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».

Стоит отметить, что в соответствии с ч. 3 ст. 18 закона о персональных данных в случае если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных законом о персональных данных, до начала обработки таких персональных

данных обязан предоставить субъекту персональных данных такую информацию как:

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

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные законом права субъекта персональных данных;

5) источник получения персональных данных.

Не стоит забывать и о том, что оператор может быть освобожден от обязанности предоставить работнику корпорации сведения о наименовании оператора, целях обработки, предполагаемых пользователях и источнике получения персональных данных. Случаи освобождения от такой обязанности указаны в ч. 4 ст. 18 закона о персональных данных и ими являются:

1) если субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) если персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

3) если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) если оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) если предоставление субъекту персональных данных сведений, предусмотренных ч. 3 ст. 18 закона о персональных данных, нарушает права и законные интересы третьих лиц.

Важной обязанностью корпорации (работодателя) является обязанность обеспечивать за счет собственных средств охрану и защиту персональных данных от неправомерного использования и утраты. С данной целью корпорация (работодатель) обязана принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных законодательством и принятыми в соответствии с ним нормативными правовыми актами. Корпорация (работодатель) самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим законодательством и принятыми в соответствии с ним нормативными правовыми актами[1].

В ст. 18.1 закона о персональных данных закреплен перечень мер, направленных на обеспечение выполнения оператором обязанностей, в том числе и защиты персональных данных работника. К таким мерам относятся:

1) назначение оператором, который является юридическим лицом, ответственным за организацию обработки персональных данных;

2) издание оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных.

Стоит отметить, что четкий перечень таких документов законодательно не установлен, и форма их жестко не регламентирована, но, опираясь на положения иных федеральных законов и подзаконных актов, можно сделать вывод, что основополагающим документов является так называемое положение об обработке персональных данных, которое в свою очередь устанавливает цели, задачи деятельности по обработке персональных данных, перечень действий, категории персональных данных, категории субъектов, способы обработки и хранения персональных данных работника. Наиболее полный

[1]Безпрозванный В.И. Правовой механизм предоставления акционерам информации о деятельности акционерного общества, участниками которого они являются: дис. ... канд. юрид. наук. –М., 2012. – С. 123.

перечень таких документов, на который можно было бы взять за основу, представлен в Постановлении Правительства РФ от 21.03.2012 № 211.

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

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

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

Часть 2 вышеуказанной статьи обязывает оператора публиковать или другим способом обеспечивать неограниченный доступ к документам, которые определяют политику корпорации в отношении обработки персональных данных. Ярким примером может послужить размещение соответствующих документов на информационном стенде или на сайте, которые доступны неограниченному кругу лиц.

Говоря об обеспечении защиты персональных данных участников корпоративных отношений стоит упомянуть о мерах по обеспечению безопасности персональных данных при их непосредственной обработке. Перечень таких мер закреплен в ст. 19 закона о персональных данных. Законодатель указывает на то, что оператор обязан принимать необходимые правовые, организационные и технические меры по защите персональных данных от неправомерного или случайного доступа к ним.

В том числе, законодатель определяет условия, при которых обеспечивается необходимая безопасность обрабатываемых персональных данных, однако стоит отметить, что приведенный в ч. 2 ст. 19 закона о персональных данных перечень не является исчерпывающим.

Так, в законе о персональных данных говорится, что обеспечение безопасности персональных данных достигается определением угроз безопасности персональных данных при их непосредственной обработке в информационных системах персональных данных. В соответствии с Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[1] (далее требования к защите персональных данных при их обработке в информационных системах персональных данных)«под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных».

Мерой обеспечения безопасности персональных данных при их обработке также является оценка эффективности принимаемых мер по обеспечению безопасности персональных данных еще до ввода в эксплуатацию информационный системы персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных.

---

[1]Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

Ко всему прочему, оператор обязан заниматься выявлением ситуаций несанкционированного доступа к персональным данным и принятием мер охранительной направленности, в том числе восстановление персональных данных, измененных или уничтоженных вследствие несанкционированного доступа к ним, установлением определенных правил доступа к персональным данным, которые обрабатываются в информационной системе персональных данных, не забывая об обеспечении учета и регистрации всех действий, которые совершаются с персональными данными в такой информационной системе персональных данных.

Правительство РФ учитывая предполагаемый вред субъекту персональных данных, содержания и объема обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, а также актуальности угроз безопасности персональным данным устанавливает уровни защищенности персональных данных, требования к их защите, требования к материальным носителям.

Проблема защиты персональных данных при раскрытии информации и ее предоставлении по запросам акционеров является одной из наиболее сложно разрешимых вопросов, которая возникает при обеспечении защиты персональных данных в акционерном обществе. Возникновение такой проблемы обусловлено столкновением разнонаправленных интересов двух категорий субъектов: с одной стороны, субъектов персональных данных, заинтересованных в обеспечении их конфиденциальности, с другой — интересов акционеров, заинтересованных в получении наиболее полной информации об обществе.

Задача акционерного общества при этом — обеспечить баланс интересов указанных лиц, исходя из предписаний закона.

По мнению Михайлюк И.В. мероприятия по защите персональных данных можно разделить на две подгруппы: меры по внутренней и внешней

защите персональных данных. Она утверждает, что «к мероприятиям по внутренней защите персональных данных относят:

– ограничение и регламентация должностей, предполагающих доступ к персональным данным;

– назначение ответственного лица, обеспечивающего исполнение обществом законодательства в рассматриваемой сфере;

– утверждение перечня документов, содержащих персональные данные;

– издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;

– ознакомление работников с действующими нормативами в области защиты персональных данных и локальными актами, систематическая проверка знаний работников, обрабатывающих персональные данные, требований нормативных документов по защите конфиденциальных данных;

– рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;

– утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;

– утверждение порядка уничтожения информации;

– выявление и устранение нарушений требований по защите персональных данных;

– профилактическая работа с сотрудниками по предупреждению разглашения персональных данных».

Среди мер по внешней защите персональных данных Михайлюк И.В. выделяет:

– введение пропускного режима в виде регламентированного порядка приема и учета посетителей;

– внедрение технических средств охраны, программных средств защиты информации на электронных носителях и другие».

Стоит сказать, что мы полностью согласны с мнением Михайлюк И.В. и ее предложенными мероприятиями по защите персональных данных. Считаем важным отметить, что такие мероприятия как ознакомление работников с действующим законодательством в области защиты персональных данных и локальными актами общества, своевременная проверка знаний работников, которые обрабатывают персональные данные, требований нормативных документов в сфере защиты конфиденциальных данных в данной ситуации будет иметь огромное и первоочередное значение. Благодаря ознакомлению работников с действующими нормативами в области защиты персональных данных у работников корпорации будет развиваться правовая культура, что способствует грамотному развитию их трудовых правоотношений. Однако, не стоит забывать и том, что, делая упор на мероприятия во внутренней защите персональных данных выделенных Михайлюк И.В. не стоит забывать о балансе интересов работников и работодателя.

## 2.2 Защита персональных данных работников при раскрытии информации и ее предоставлении по запросам акционеров

Исходя из анализа действующего законодательства и складывающейся судебной практики появляется возможность сформулировать общее правило предоставления акционерам информации, которая содержит персональные данные. То есть, наличие в документах конфиденциальной информации никак не может являться основанием для отказа в предоставлении различных документов по запросам акционеров, поскольку в соответствии с п. 2 ст. 67 ГК РФ обязанности корпорации представлять такую информацию корреспондируются обязанностью участников корпорации не разглашать конфиденциальную информацию о деятельности такого общества.

Стоит отметить, что для целей защиты режима конфиденциальность общество вправе брать у акционеров расписки, изымать из документов соответствующие данные и применять различные подобные меры.

Однако, в соответствии с п. 15 Информационного письма Президиума ВАС РФ от 18.01.2011 г. № 144 «О некоторых вопросах практики рассмотрения арбитражными судами споров о предоставлении информации участникам хозяйственных обществ»[1], в силу п. 2 ст. 6 закона о персональных данных «не требуется согласия физических лиц, вступивших в правоотношения с обществом, на предоставление участнику хозяйственного общества документов, содержащих персональные данные таких физических лиц (фамилию, имя, отчество и место жительства физического лица, иную информацию, необходимую для обращения в суд в соответствии с требованиями процессуального законодательства, сведения о размере вознаграждения физического лица и т. д.), если эта информация необходима участнику для целей защиты своих прав и законных интересов». Так, примером может послужить оспаривание сделки, заключенной с данным лицом, или же обращения в суд с иском к члену совета директоров (наблюдательного совета) общества, единоличному исполнительному органу общества, временному единоличному исполнительному органу общества, члену коллегиального органа общества (правления, дирекции), равно как и к управляющему о возмещении причиненных обществу убытков.

Зачастую, в судебной практике встречаются ситуации, когда суды принимают позицию обществ, а не их акционеров и таким образом квалифицируют соотношении гражданского законодательства и закона о персональных данных. Суды считают, что законодательство о защите персональных данных является специальным по отношению к нормам закона об акционерных обществах, а также, поскольку в силу ст. 6 закона о

[1]Информационное письмо Президиума ВАС РФ от 18 января 2011 г. № 144 «О некоторых вопросах практики рассмотрения арбитражными судами споров о предоставлении информации участникам хозяйственных обществ» // Вестник ВАС РФ. – 2011. – № 3. – март.

персональных данных обработка таких данных осуществляется исключительно с согласия субъекта персональных данных, а значит предоставление акционеру информации, которая содержит персональные данные возможна только с согласия такого субъекта.

Наиболее ярким примером выражения такой позиции служат случаи запроса акционерами трудового договора с директором общества.

Так, решением Арбитражного суда города Москвы от 30 сентября 2011 г. по делу № А40–79903/2011[1] суд посчитал, что отказ общества от предоставления акционерам копии контракта с председателем правления являлся обоснованным, сославшись на ст. 88 ТК РФ, которой установлен запрет на передачу персональных данных работника третьим лицам. В ходе данного дела суд пришел к выводу о том, что в отношении контракта с Председателем правления общества, административным органом, не было учтено, что в соответствии со ст. 67 ТК РФ и ст. 3 закона о персональных данных, трудовой договор является документом, содержащим персональные данные работника. Также, суд ссылался на то, что ст. 85 – 88 ТК РФ регулируют правоотношения в части обработки, хранения и предоставления персональных данных работника. В силу чего специальным законом, в части предоставления персональных данных работника, являются нормы трудового законодательства, а не закон об акционерных обществах. В силу статей 86, 87 ТК РФ работодатель (общество) обязано обеспечить защиту персональных данных работника. Ст. 88 ТК РФ установлен запрет на передачу персональных данных работника третьей стороне. Поэтому суды пришли к выводу, что нормами специального законодательства регулирующего правоотношения по предоставлению персональных данных работника, установлен запрет на передачу указанных данных третьим лицам.

Кроме того, суды указали, что в рассматриваемом случае ответчиком не представлено доказательств, подтверждающих, что копия трудового договора

[1]Решение Арбитражного суда города Москвы от 30 сентября 2011 г. по делу № А40–79903/2011 // [Электронный ресурс] – URL: http://kad.arbitr.ru/ (дата обращения 10.02.2017)

(контракта) Председателя правления ЗАО «ПроБанк» содержащие персональные данные физического лица (фамилию, имя, отчество) необходима акционеру для защиты своих прав и законных интересов.

Тут мы согласны с позицией суда в части того, что не указание целей защиты своих прав и законных интересов акционера недопустимо.

Однако стоит отметить, что несмотря на наличие отдельных судебных актов, отказывающих акционерам в получении конфиденциальной информации, в настоящее время очевидным образом прослеживается превалирующая направленность судебной практики в защиту прав акционеров на получение информации.

Персональные данные генерального директора используются на практике в разы чаще, чем данные любого другого сотрудника корпорации. Тем не менее, это не удивительно, так как генеральный директор действует от имени общества, имеет право представлять его интересы, дает другим работникам полномочия на осуществление действий, связанных с деятельностью общества. Персональные данные генерального директора могут содержаться в доверенностях на исполнение обязанностей, договорах, распорядительных документах, анкетах.

В соответствии со ст. 88 ТК РФ передача персональных данных работника третьей стороне без письменного согласия сотрудника запрещена, за исключением предусмотренных законом случаев. Таким образом генеральный директор считается работником, на него распространяются все положения трудового законодательства. С ним, как и с другими сотрудниками, заключается договор, издается приказ о его назначении, соответствующие записи о трудовых отношениях вносятся в трудовую книжку. Согласие необходимо оформить в письменном виде, из него должно быть понятно, кому и с какой целью будут передаваться персональные данные. При этом ст. 88 ТК РФ предусматривает, что без согласия работника персональные данные не могут передаваться в коммерческих целях работника.

В качестве примера вышеуказанной направленности имеется возможность привести дело, рассмотренное Президиумом Высшего Арбитражного Суда Российской Федерации под номеромА40–43149/2011[1]. Существо указанного дела сводится к следующему.

Акционеры, которые владели тридцатью восемью процентами обыкновенных акций ОСАО «Ингосстрах» (далее — общество), обратились в общество с требованием о предоставлении копии действующего трудового договора, заключенного с генеральным директором.

Исходя из фабулы дела, копии действующего трудового договора, заключенного с генеральным директором, не были предоставлены акционерам. В последствие чего акционеры обратились в Федеральную службу по финансовым рынкам Российской Федерации (далее — ФСФР) с заявлением о привлечении общества к административной ответственности. После чего ФСФР привлекло общество к административной ответственности, предусмотренной ч. 1 ст. 15.19 Кодекса Российской Федерации об административных правонарушениях[2] (далее КоАП РФ), за непредставление запрошенной акционерами копии трудового договора, заключенного с генеральным директором.

Не согласившись с решением и предписанием ФСФР, общество обратилось в арбитражный суд. Суд первой инстанции, удовлетворяя заявленное требование, исходил из того, что суду не представлено доказательств, подтверждающих, что копия трудового договора необходима акционерам для целей защиты своих прав и законных интересов. Суды апелляционной и кассационной инстанции согласились с правовой позицией суда первой инстанции.

---

[1]Решение Арбитражного суда Московского округа от 25 мая 2011 г. по делу № А40-43149/2011 // [Электронный ресурс] – URL: http://kad.arbitr.ru (дата обращения 10.02.2017)

[2] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. – 2002.– № 1 (ч. 1). – Ст. 1.

Однако Судебная коллегия по гражданским делам Высшего Арбитражного Суда Российской Федерации сочла неправильным столь однозначное решение вопроса. В связи с тем, что трудовой договор мог быть представлен акционерам без открытия персональных данных директора общества, и данным договором могли быть существенно нарушены интересы акционеров общества (в частности, существенным завышением оплаты трудового контракта). В дальнейшем дело было передано в Президиум ВАС РФ для решения вопроса о пересмотре судебных актов в порядке надзора. В свою очередь, в 22.05.2012 г. Президиум ВАС РФ судебные акты первой, апелляционной и кассационной инстанций по делу №А40–43149/2011 отменил и отказал ОСАО «Ингосстрах» в удовлетворении заявленного требования.

Стоит отметить, что из позиции Судебной коллегии ВАС РФ, передавшей дело в надзор, становится ясно, что, по мнению высшей судебной инстанции, наличие в документе персональных данных не должно использоваться акционерными обществами в качестве легального способа уклонения от обеспечения прав акционеров на информацию.

На практике это означает, что акционерное общество имеет возможность предпринять комплекс мер, которые бы, с одной стороны, обеспечивали сохранение конфиденциальности информации, но, с другой стороны, — обеспечивали права уполномоченных субъектов на получение информации об обществе.

Необходимо отметить Постановление Двадцатого Арбитражного Апелляционного суда г. Тула по делу № А62–6393/2014[1] где АО «НК «Роснефть» не согласно с решением суда в части отказа в удовлетворении заявленных требований и не согласно с выводом суда первой инстанции об обязанности общества предоставить копии трудовых договоров с генеральным директором общества, которые могут быть переданы акционеру лишь с

[1]Постановление Двадцатого Арбитражного Апелляционного суда от 24 февраля 2015 по делу № А62-6393/2014 // [Электронный ресурс] – URL: https://rospravosudie.com/ (дата обращения 10.02.2017)

согласия самого генерального директора, учитывая содержащиеся в них персональные данные. Также, полагает, что поведение ООО «МИРИАД РУС» свидетельствует о том, что единственной целью общества является причинение ущерба ОАО «НК «Роснефть», а не получение спорных документов о хозяйственной деятельности последнего, что свидетельствует о злоупотреблении ООО «МИРИАД РУС» своими правами. В данном деле суд руководствовался ст. 88 ТК РФ где установлено, что работодатель не должен передавать персональные данные сотрудника третьей стороне без его письменного согласия, а также разглашать эти сведения в коммерческих целях. Однако, В силу п. 2 ст. 6 закона о персональных данных не требуется согласия физических лиц, вступивших в правоотношения с обществом, на предоставление участнику хозяйственного общества документов, содержащих персональные данные таких физических лиц (фамилию, имя, отчество и место жительства физического лица, иную информацию, необходимую для обращения в суд в соответствии с требованиями процессуального законодательства, сведения о размере вознаграждения физического лица и т.д.), если эта информация необходима участнику хозяйственного общества для целей защиты своих прав и законных интересов, например оспаривания сделки, заключенной с этим лицом, либо обращения в суд с иском к члену совета директоров (наблюдательного совета) общества, единоличному исполнительному органу общества, временному единоличному исполнительному органу общества, члену коллегиального исполнительного органа общества (правления, дирекции), равно как и к управляющему о возмещении причиненных обществу убытков. Таким образом, суд пришел к выводу о том, что акционерное общество не вправе отказывать акционерам в получении информации на том основании, что в запросе акционером не указаны цели получения тех или иных документов.

Тем не менее, в данной ситуации мы не согласны с решением суда по поводу того, что акционерное общество не вправе отказывать акционерам в

получении информации на основании не указания целей получения тех или иных документов. Разумно предположить, что в данной ситуации акционеры были обязаны указать цели получения документов, которые содержат персональные данные.

В дальнейшем, суд установил, что из запроса ООО «МИРИАД РУС» не следует, что копии запрошенных акционером у общества трудовых договоров (контрактов), заключенных между обществом и руководством общества (со всеми дополнениями и приложениями, являющимися неотъемлемыми частями таких договоров), в которых указаны размеры выплат и/или зарплат и(или) вознаграждений с учетом бонусов и/или премий по итогам года и (или) кварталов, необходимы ООО «МИРИАД РУС» для целей защиты своих прав и законных интересов.

В данном случае видно, что суд самостоятельно находит и определяет цели акционеров, что приводит решение дела в пользу акционеров. Мы считаем, что не указание целей запроса персональных данных акционерами можно понимать, как неиспользование своих прав в данной ситуации этими акционерами.

Вместе с тем непредставление обществом по запросу акционера копии трудового договора с генеральным директором общества, в котором могли содержаться, в том числе положения о несоразмерной заработной плате данного лица, существенно нарушает интересы акционера. Также, при разрешении спора суд опирается на позицию Президиума Высшего Арбитражного Суда Российской Федерации в постановлении от 22.05.2012 № 16803/11[1].

То есть, суд приходит к выводу о том, что акционер, делая запрос трудового договора с генеральным директором общества защищал свои интересы как акционер данного общества.

---

[1]Постановление Президиума Высшего Арбитражного Суда Российской Федерации в постановлении от 22 мая 2012 г. № 16803/11 // [Электронный ресурс] – URL: http://www.arbitr.ru/ (дата обращения 10.02.2017)

Для того чтобы разрешить возникшую проблему необходимо:

– разработать систему локальных актов, определяющих состав конфиденциальной информации и порядок доступа к ней;

– предусмотреть в указанных локальных актах конкретные меры по защите персональных данных, которые бы одновременно обеспечивали права акционеров на получение информации о деятельности общества (так, общество вправе в локальном акте установить требование о подписании акционером расписки о неразглашении персональных данных при выдаче ему соответствующих документов).

– при разрешении данной проблемы в судебном порядке принять меры к тому, чтобы суд учитывал указание или не указание целей запроса персональных данных акционерами.

Преобладающие количество вопросов, связанных с защитой персональных данных участников корпоративных отношений, возникает в связи с обязательным раскрытием информации.

Основополагающий момент, который стоит разрешить, это вопрос о необходимости получения согласия участников корпоративных отношений на обработку их персональных данных, которые в свою очередь подлежат обязательному раскрытию в силу требований законодательства.

Прежде всего, опираясь на пп. 2, 11 ч. 1 ст. 6 закона о персональных данных можно сформулировать ответ на данный вопрос. То есть, в соответствии с вышеуказанными нормами обработка персональных данных без согласия субъекта персональных данных допускается:

– в случае если обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– в случае если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом о персональных данных.

Таким образом, при раскрытии акционерным обществом информации, которая содержит в себе персональные данные (годового отчета, ежеквартального отчета, сообщения о существенных фактах, списка аффилированных лиц и иных сведений), во исполнение обязательных требований законодательства письменное согласие членов совета директоров, акционеров, членов коллегиального органа управления, единоличного исполнительного органа, иных лиц в получении не требуется.

Однако стоит отметить, что в случае, если принятая в обществе информационная политика предусматривает обработку и раскрытие большего объема персональных данных, чем предусмотрено законом, имеется возможность предположить, что общество обязано получить письменное согласие физических лиц на обработку соответствующих персональных данных. Также считаем необходимым указать, что, по нашему мнению, в случае обязательного раскрытия информации, предусмотренного законом, субъект персональных данных не вправе запретить обществу осуществить их обработку и обнародование. Подобный запрет на предоставление персональных данных будет противоречить приведенным выше нормам закона о персональных данных и может быть расценен как злоупотребление правом, которое не подлежит судебной защите.

Отдельно хочется отметить, что ст. 17 закона о персональных данных закрепляет у субъекта персональных данных право на обжалование действий или бездействие оператора (то есть лица, который осуществляет обработку персональных данных). В случае, если субъект персональных данных полагает, что оператор осуществляет обработку его персональных данных с какими–либо нарушениями требований законодательства или другим способом нарушает его права и свободы, то субъект персональных данных имеет право обжаловать действия или бездействие оператора в уполномоченном органе, которые осуществляет защиту прав субъектов персональных данных или же в судебном порядке. Стоит сказать, что субъект персональных данных наряду с

указанными выше способами имеет право на защиту своих прав и законных интересов посредством возмещения убытков и (или) компенсации морального вреда.

В настоящее время судебная практика не богата исками о незаконной обработке персональных данных, а иски о незаконном использовании персональных данных в корпоративных отношениях встречаются еще реже.

В заключение хочется отметить, что постановка вопроса защиты персональных данных физических лиц в разряд одного из важнейших вопросов, подлежащих решению и контролю в деятельности любой организации, является неоспоримым достижением как в развитии действующего законодательства, так и в практике работы специально уполномоченных государственных органов.

При этом следует помнить, что популярное сейчас словосочетание «защита персональных данных» не может использоваться произвольно и применяться обществом в качестве «законного» средства уклонения от исполнения обязанностей по раскрытию и предоставлению информации, возложенных законом на общество. Как было отмечено выше, в своей деятельности акционерное общество должно обеспечить баланс интересов в этом вопросе различных категорий субъектов. Во временных условиях неоднозначной судебной практики эта задача может быть решена силами самого общества посредством установления четких правил и процедур работы с конфиденциальной информацией.

## 2.3 Разработка локальных нормативных актов, регламентирующих вопросы защиты персональных данных как способ охраны участников корпоративных отношений

Определение значимости локального нормативного регулирования в современной правовой науке и юридической практике не подлежит сомнению,

в отличие от советских времён[1], когда, по сути, правовая наука искала способы обоснования, осуществляла поиск места в механизме правового регулирования и необходимости реализации актов локального нормотворчества. При этом необходимо обратить внимание, что и сейчас границы локального регулирования чётко не очерчены, существуют споры по используемой терминологии, правовому характеру локального регулирования и иные. Точки зрения отечественных правоведов зачастую расходятся в вопросах определения сущности, места и роли локальных нормативных актов, их иерархии в структуре правового регулирования[2].

Таким образом в настоящее время локальное правотворчество в сфере труда имеет особую значимость, так как, зачастую, образует, организует и гарантирует трудовые отношения, является волей руководства отдельных организаций по закреплению за работниками конкретных прав и обязанностей в сфере общих правил обязательного поведения на предприятии, соответствующих законодательству о труде. Они являются средством в локальном правовом регулировании труда, обеспечивающим организацию, специфику предприятия и общие итоги деятельности его коллектива и отдельных работников. Локальных правовые акты делятся на: устав организации, который определяет порядок избрания на должность, замещение соответствующих должностей по конкурсу и назначение на должность или утверждение в должности; коллективный договор и положение о порядке разработки и заключения коллективного договора; штатное расписание; правила внутреннего трудового распорядка; графики отпусков; акты об индексации заработной платы; акты о формах профессиональной подготовки, переподготовки и повышения квалификации работников; положение об

[1]Самигуллин В.К. Локальное нормативное регулирование в механизме современного правового регулирования общественных отношений // Вестник ВЭГУ. – 2015. – № 4 (78). – С. 72.
[2]Лескова Ю.Г. Источники корпоративного права // Власть Закона. – 2015. – № 3. – С. 54.

аттестации рабочих мест; положение о комиссии по трудовым спорам и некоторые другие.

Тем не менее локальные нормативные акты являются эффективным инструментом, средством установления субъективных прав, обязанностей, льгот, запретов, поощрений и наказаний, связанных с информацией ограниченного доступа в трудовых правоотношениях. Некоторые локальные акты в отношении информации ограниченного доступа названы в ТК РФ (в отношении персональных данных), но без установления требований к порядку их принятия. В связи с чем обозначена проблема реализации требования п. 10 ст. 86 ТК РФ о совместном принятии мер по защите персональных данных работников.

Так, в соответствии с гл. 14 ТК РФ каждая организация обязана разработать и ввести в действие локальные нормативные акты, которые определяют порядок работы с персональными данными ее работников.

Такими локальными актами, как правило, являются:

– положение об обработке и защите персональных данных;

– приказ об утверждении обязательств о неразглашении персональных данных;

– перечень должностей, допущенных к персональным данным;

– приказ о назначении ответственных лиц за организацию обработки персональных данных;

– согласие на обработку персональных данных работника Оператора, иных субъектов персональных данных;

В соответствии со ст. 3 закона о персональных данных персональными данными является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Таким образом, персональные данные – это любая информация, которая позволяет идентифицировать конкретного человека. Исходя из приведенного определения, Михайлюк И.В. полагает, что «в сфере

корпоративных отношений такие сведения могут содержатся в следующих документах:

– анкета акционера;

– журнал регистрации акционеров, прибывших на общее собрание;

– список лиц, имеющих право участвовать в общем собрании акционеров;

– заявления, запросы акционеров в общество;

– доверенности на лиц, уполномоченных акционерами участвовать в общем собрании акционеров;

– бухгалтерские документы (например, платежные поручения могут содержать сведения о счетах акционеров, на которые перечисляются дивиденды);

– протоколы общих собраний и собраний совета директоров;

– ежеквартальные отчеты;

– годовые отчеты (в них содержатся сведения о членах совета директоров (наблюдательного совета), единоличном исполнительном органе, членах коллегиального исполнительного органа, в том числе их краткие биографические данные, доля их участия в уставном капитале и доля принадлежащих им обыкновенных акций);

– списки аффилированных лиц;

– сообщения о существенных фактах;

– документы, полученные или составленные обществом в рамках трудовых правоотношений с директором общества: трудовой договор, документы об образовании, копия паспорта, трудовая книжка, копии свидетельств о заключении брака, рождении детей, документы воинского учета, справка о доходах с предыдущего места работы, документы обязательного пенсионного страхования, приказы по личному составу в отношении директора общества».

Вышеприведенные перечень не является исчерпывающим и каждая корпорация, учитывая ее сферу деятельности, имеет полное право расширить его. Мы считаем, что составление аналогичного перечня документов имеет мест быть необходимым в целях организации правомерного режима доступа к информации, которая содержит персональные данные.

Если не учитывать то, что законом не установлены определенные требования к содержанию и количеству локальных актов, которые должна принимать организация в целях разрешения вопросов обработки и защиты персональных данных, то на практике же сформировался необходимый минимум документов, которые должны быть разработаны и приняты в корпорации.

В первую очередь необходимо составить общий документ, определяющий политику общества в отношении обработки персональных данных, например, положение о персональных данных. В соответствии со ст. 87 ТК РФ «порядок хранения и использования персональных данных работников устанавливается работодателем» с учетом требований ТК РФ и иных федеральных законов, что подразумевает под собой регулирование порядка обработки персональных данных работников локальными нормативными и иными актами. Целью принятия данного положения является определение порядка обработки персональных данных работников, обеспечение защиты прав и свобод работников при обработке их персональных данных, а также определение ответственности лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Данный документ регламентирует в рамках отдельной организации требования к получению, обработке персональных данных работника, установить гарантии их защиты, порядок хранения и использования, а также права работника по защите его персональных данных и ответственность работодателя за их охрану и защиту. Иными словами, организация на основе

российского законодательства и с учетом особенностей кадрового учета создает и закрепляет нормативным актом порядок работы с персональными данными[1].

Отсутствие данного локального нормативного акта может быть квалифицировано государственным и иным органом государственного контроля (надзора) как нарушение работодателем трудового законодательства.

Мы считаем, что в такой локальный акт было бы разумной включить:

– задачи защиты персональных данных и цели их обработки;

– список сведений и документов, которые содержат персональные данные работника;

– перечень сведений, которые относятся к персональным данным (т.е. данные документов, удостоверяющих личность, номера телефонов, размеры оплаты труда и т.д.);

– регламентированное описание процессов обработки персональных данных;

– регламентированный порядок ознакомления работников с персональными данными работодателя, которые у него имеются;

– гарантии защиты персональных данных, а также общие требования при их обработке;

– сроки хранения персональных данных;

– регламентированный порядок работы с персональными данными, включающий в себя обработку, хранение, сбор и уничтожение персональных данных;

– общие правила передачи персональных данных.

Положение об обработке и защите персональных данных работника утверждается единоличным исполнительным органом общества (директором, генеральным директором) или единоличным исполнительным органом общества (директором, генеральным директором) и коллегиальным

[1]Давыдова Е.В. Персональные данные работников // Отдел кадров коммерческой организации. – 2015. – №3. – С. 34.

исполнительным органом общества (правлением, дирекцией) общества или уполномоченное им лицо, а вводится в действие этот документ уже приказом[1].

Положение о защите персональных данных подписывается руководителем кадровой службы. Документ может быть согласован с заинтересованными должностными лицами, например, работниками бухгалтерии, юридической службы, службой безопасности и др. С ним следует ознакомить весь персонал организации под расписку.

Работники акционерного общества должны быть под роспись ознакомлены с данным положением. Факт ознакомления с положением может фиксироваться как в тексте трудового договора (путем перечисления локальных нормативных актов, с которыми работник ознакомлен до подписания договора), так и в отдельном документе (например, в самом положении на листе ознакомления с ним).

В дальнейшем необходимо определить список лиц, обрабатывающих персональные данные. Применительно к акционерному обществу в этот перечень, прежде всего, входит корпоративный секретарь либо лицо, исполняющее его функции.

Важным этапом будет принятие приказа о назначении сотрудника, который будет ответственен за реализацию обработки персональных данных. Такой сотрудник должен обеспечивать своими действиями контроль исполнения законодательства в сфере персональных данных как обществом, так и его работниками, в том числе и обеспечивать контроль требований к защите персональных данных, принимать и обрабатывать запросы или обращения субъектов персональных данных, а также организовывать контрольную функцию таких запросов или обращений.

Необходимо также принять положение о правовых, организационных и технических мерах защиты персональных данных от случайного или неправомерного доступа к ним, включая изменение, блокирование,

[1]Соколова Г.А. Персональные данные работников // Кадровая служба и управление персоналом предприятия.– 2013.– №7. – С. 22

копирование, уничтожения, распространения или иные неправомерные действий с персональными данными. Так, считаем необходимым в данном положении обозначить определенные меры по защите персональных данных, к примеру применение информационных средств защиты (шифрование данных, хранение данных на отдельных материальных носителях или в специальных технически оборудованных помещениях с ограниченным доступом к ним), возможное введение пропускного режима.

Заключительным этапом будет разработка локального акта, устанавливающего процедуры, которые прямо направлены на выявление и предотвращение нарушений законодательства в сфере защиты персональных данных, а также непосредственное устранение последствий таких нарушений. Так, к примеру, в обществе имеет место разработка плана мероприятий по внутреннему контролю безопасности персональных данных, введение инструкций о порядке проведения служебных расследований по вопросам нарушений законодательства в сфере защиты персональных данных, ведение журнала проверок работ с персональными данными, проведение инструктажа и аттестаций по вопросам защиты персональных данных.

В целях сохранения режима конфиденциальности следует вести журнал учета персональных данных, их выдачи и передачи третьим лицам, что обеспечит документальную фиксацию доступа к данным[1]. Также рекомендуется проведение регулярных проверок наличия документов, содержащих персональные данные, во избежание их пропажи.

Получение личных данных работника возможно только у него самого, если это невозможно, то получение личных сведений у третьей стороны осуществляется только с письменного согласия работника, как уже было отмечено ранее.

Данные о религиозных, политических и других убеждений, о членстве в общественных объединениях или профсоюзной деятельности, а также данные о

[1]Беденкова А.А. Правовой статус персональных данных работников // Вестник науки Сибири. – 2014. – №4 (14). – С. 149

частной жизни не подлежат получению и обработке работодателем. Только в случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ, работодатель вправе получать такие данные работника только с его письменного согласия.

В свою очередь, работник обязан предоставить работодателю комплекс достоверных документированных персональных данных и сообщать работодателю в письменной форме об изменении своих персональных данных.

Работник имеет право на свободный и бесплатный доступ к своим данным и получение их копий, требовать исправления неверных данных, обжаловать в суде неправомерные действия работодателя при обработке данных.

Внутренний доступ к персональным данным работников имеют руководитель организации, его заместители, работник отдела кадров, сотрудник бухгалтерии и сам работник. Внешний доступ имеют налоговые органы, правоохранительные органы, органы статистики, страховые агенты, военкоматы, органы социального страхования и пенсионные фонды.

Также, Станскова У.М. считает, что указание в трудовом договоре только на обязанность не разглашать охраняемую законом тайну не охватывает всех требований, которые должен соблюдать работник в отношении информации ограниченного доступа (в том числе и персональные данные работник). Поэтому предлагает включить в трудовые договоры формулировку: обеспечение конфиденциальности (секретности) информации ограниченного доступа. Станскова полагает, «что обеспечение конфиденциальности должно включать комплекс следующих обязанностей: соблюдать требования по обработке (передаче, хранению и т.д.) информации; не использовать ее в своих целях без разрешения обладателя и не разглашать; принимать меры, направленные на ограничение доступа к информации[1]».

[1]Станскова У.М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореферат диссертации, дис. ... канд. юрид. наук. – Екатеринбург, 2014. – С. 12.

В свою очередь, Станскова У.М. затрагивает «вопрос о сохранении обязанностей в отношении информации ограниченного доступа после прекращения трудовых отношений. Российский законодатель в отношении ряда видов информации ограниченного доступа устанавливает императивный запрет разглашения соответствующей информации, который отличается от пакта о неконкуренции, легализованного в зарубежных странах. Представленные механизмы направлены на достижение общей цели – обеспечение информационной безопасности субъектов, но должны иметь различную сферу применения. Представляется, что императивный запрет обязателен для тех видов информации, обязанность по охране и состав которых не зависит от усмотрения работодателя (государственная, служебная, профессиональная тайна, персональные данные, включая сведения о частной жизни). Соглашение о неконкуренции, напротив, уместно в отношении коммерческой тайны и иной информации, режимы которых устанавливаются по желанию обладателя (работодателя)». Она полагает, что «имеется возможность сосуществования в законодательстве двух названных конструкций. При закреплении только императивного запрета представляется, что он должен быть обеспечен обязанностью работодателя информировать о сохранении конфиденциальности, особенно коммерческой тайны, для чего необходимо дополнить ТК РФ статьей 89.1 с указанием такой обязанности».

Подводя итог, хочется добавить, что что работодатель обязан также ознакомить работника с уровнем защиты его персональных данных и условиями обеспечения информационной безопасности его персональных данных. Для этой цели на локальном уровне необходимо разработать локальный нормативный акт информационной безопасности персональных данных.

Механизм защиты оператором персональных данных субъектов позволяет выделить три типа актуальных угроз и определяется в соответствии с

требованиями к защите персональных данных при их обработке в информационных системах персональных данных:

– угрозы 1–го типа – актуальны при наличии недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

– угрозы 2–го типа – актуальны при наличии недокументированных (не декларированных) возможностей в прикладном обеспечении,

– угрозы 3–го типа – актуальны при отсутствии недокументированных

(не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В свою очередь, информационные системы классифицируются по типу персональных данных и по типу субъектов персональных данных:

– обрабатывающие специальные категории персональных данных;

– обрабатывающие биометрические персональные данные;

– обрабатывающие общедоступные персональные данные;

– обрабатывающие иные категории персональных данных;

– обрабатывающие персональные данные сотрудников оператора.

Уровень защищенности определяется с учетом выбранного типа угроз, категории персональных данных и количества субъектов. Настоящие требования устанавливают четыре уровня защищенности персональных данных, которыми устанавливаются условия обеспечения информационной безопасности каждого из уровней.

В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных устанавливается регулярный контроль за выполнением требований безопасности не реже 1 раза в 3 года, который организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Так, благодаря разработке локального нормативного акта информационной безопасности персональных данных работников корпорации появляется возможность улучшить информационную безопасность данных работника и в соответствии с данным актом своевременно и правомерно устранять возникающие нарушения.

# ЗАКЛЮЧЕНИЕ

Проведение настоящего исследования позволило сделать следующие выводы.

Персональные данные являются одним и наиболее важных элементов построения трудовой деятельности в корпорации. Персональные данные работников содержатся в трудовых договорах и иных документах, связанных с трудовой деятельностью, которые в свою очередь носят анонимный характер и служат для защиты информации о работниках. Любое распространение таких данных не допускается законодательством, за исключением случаев, прямо указанных в законе.

Основной проблемой при использовании персональных данных работников корпорации является то, что зачастую акционеры общества запрашивают такие данные в целях защиты своих интересов. Особое внимание уделяется трудовым договорам и иным документам, связанным с трудовой деятельностью органов управления. Таким образом возникает конфликт между обществом и акционерами, в котором одни обязаны защитить персональную информацию работников, а другие защитить интересы акционеров.

Исходя из анализа действующего законодательства и складывающейся судебной практики появляется возможность сформулировать общее правило предоставления акционерам информации, которая содержит персональные данные. Таким образом, наличие в документах конфиденциальной информации никак не может являться основанием для отказа в предоставлении различных документов по запросам акционеров, поскольку в соответствии с п. 2 ст. 67 ГК РФ обязанности корпорации представлять такую информацию корреспондируются обязанностью участников корпорации не разглашать конфиденциальную информацию о деятельности такого общества.

Также, необходимо отметить, что судебная практика по данной проблеме направлена в основном на защиту прав акционеров. То есть, суды приходят к выводу о том, что акционер, делая запрос трудовых договоров с работниками

общества защищает свои интересы как непосредственно участник данного общества.

В целях разрешения данной проблемы в данной работе были предложены такие варианты:

– разработать систему локальных актов, определяющих состав конфиденциальной информации и порядок доступа к ней;

– предусмотреть в указанных локальных актах конкретные меры по защите персональных данных, которые бы одновременно обеспечивали права акционеров на получение информации о деятельности общества (так, общество вправе в локальном акте установить требование о подписании акционером расписки о неразглашении персональных данных при выдаче ему соответствующих документов).

Однако, преобладающие количество вопросов, связанных с защитой персональных данных участников корпоративных отношений возникает в связи с обязательным раскрытием информации.

Прежде всего, опираясь на пп. 2, 11 ч. 1 ст. 6 закона о персональных данных важно отметить, что «обработка персональных данных без согласия субъекта персональных данных допускается:

– в случае если обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– в случае если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом о персональных данных».

Таким образом, можно сказать, что при раскрытии акционерным обществом информации, которая содержит в себе персональные данные работников (годового отчета, ежеквартального отчета, сообщения о существенных фактах, списка аффилированных лиц и иных сведений), во исполнение обязательных требований законодательства письменное согласие

членов совета директоров, акционеров, членов коллегиального органа управления, единоличного исполнительного органа, иных лиц в получении не требуется.

Однако стоит упомянуть, что в случае, если принятая в обществе информационная политика предусматривает обработку и раскрытие большего объема персональных данных, чем предусмотрено законом, имеется возможность предположить, что общество обязано получить письменное согласие физических лиц на обработку соответствующих персональных данных. Также считаем необходимым указать, что, в случае обязательного раскрытия информации, предусмотренного законом, субъект персональных данных не вправе запретить обществу осуществить их обработку и обнародование. Подобный запрет на предоставление персональных данных будет противоречить приведенным выше нормам закона о персональных данных и может быть расценен как злоупотребление правом, которое не подлежит судебной защите.

Обобщая вышесказанное, мы делаем вывод, что для того чтобы разрешить возникшие проблемы, обществам необходимо разрабатывать систему локальных актов, которые бы прямо были направлены на защиту персональных данных работников, а также обеспечивали доступ к такой информации акционером, но предусматривали неразглашение акционерами такой информации. Данное решение позволит миновать множество судебных разбирательств и упростит процесс как защиты персональных данных работников, так и правомерный доступ акционеров к интересующей их информации.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

## Раздел I Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с поправками от 21 июля 2014 г.) // Российская газета – 1993. – 25 декабря.

2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. – 2014. – № 5. – Ст. 419.

3. Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496 –ом пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. – 1976. – № 17. – Ст. 291.

4. Конвенция о защите прав человека и основных свобод от 4 ноября 1950г. // Собрание законодательства РФ. – 1998. – № 20. – Ст. 2143.

5. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. – 1995. – № 67.

6. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197 – ФЗ // Российская газета. – 2001. – № 256.

7. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51 –ФЗ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

8. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195 – ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

9. Федеральный закон от 25 июля 2011 г. № 261 –ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. – 2011. – № 31. – Ст. 4701.

10. Федеральный закон от 28 декабря 2010 г. № 390 –ФЗ «О безопасности» // Собрание законодательства РФ. – 2011. – № 1. – Ст. 2.

11. Федеральный закон от 27 июля 2010 г. № 210 –ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ. – 2010. – № 31. – Ст. 4179.

12. Федеральный закон от 27 июля 2006 г. № 152 –ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

13. Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

14. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

15. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

16. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ. – 2012. – № 14. – Ст. 1626.

17. Постановление Правительства РФ от 22 декабря 2006 г. № 785 «Об утверждении Правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания» // Собрание законодательства РФ. – 2007. – № 1 (2 ч.). – Ст. 249.

18. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр –1895) // Российская газета. –2000. – № 187. (утратил силу)

19. Федеральный закон от 20 февраля 1995 г. №24 –ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства РФ. – 1995. – № 8. – Ст. 609. (утратил силу)

20. Кодекс законов о труде Российской Федерации (утв. ВС РСФСР 9 декабря 1971 г.) // Ведомости ВС РСФСР. – 1971. – № 50. – Ст. 1007. (утратил силу)

Раздел II Постановления высших судебных инстанций и материалы юридической практики

21. Информационное письмо Президиума ВАС РФ от 18 января 2011 г. № 144 «О некоторых вопросах практики рассмотрения арбитражными судами споров о предоставлении информации участникам хозяйственных обществ» // Вестник ВАС РФ. – 2011. – № 3. – март.

22. Решение Арбитражного суда Московского округа от 25 мая 2011 г. по делу № А40 –43149/2011 // [Электронный ресурс] – URL: http://kad.arbitr.ru (дата обращения 10.02.2017)

23. Решение Арбитражного суда города Москвы от 30 сентября 2011 г. по делу № А40 –79903/2011 // [Электронный ресурс] – URL: http://kad.arbitr.ru (дата обращения 10.02.2017)

24. Постановление Президиума Высшего Арбитражного Суда Российской Федерации в постановлении от 22 мая 2012 г. № 16803/11 // [Электронный ресурс] – URL: http://www.arbitr.ru/ (дата обращения 10.02.2017)

25. Постановление Двадцатого Арбитражного Апелляционного суда от 24 февраля 2015 по делу № А62 –6393/2014 // [Электронный ресурс] – URL: https://rospravosudie.com/ (дата обращения 10.02.2017)

Раздел III Литература

26. Анисимов, Л.Н. Персональные данные работника: Требование к передаче / Л.Н. Анисимов // Справочник кадровика. – 2006. – №7. – С. 24 –28.

27. Атагимова, Э. И. Некоторые аспекты законодательного уровня обеспечения информационной безопасности в Российской Федерации / Э. И. Атагимова, Р. М. Рамазанова // Правовая информатика. – 2014. – № 2. – С. 14 – 19.

28. Афанасьева, Е.Г. Корпоративное право: учебник / Е.Г. Афанасьева, В.Ю. Бакшинскас, Е.П. Губин и др.; отв. ред. И.С. Шиткина. 2 –е изд., перераб. и доп. – М: КНОРУС, 2015 – 500 с.

29. Балашкина, И.В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации / И.В. Балашкина // Право и политика. – 2007. – №7. – С. 92–105.

30. Баринов, С.В. О правовом определении понятия «информационная безопасность личности» / С. В. Баринов// Актуальные проблемы российского права. – 2016. – № 4 (65). – С. 97 –105

31. Беденкова, А.А. Правовой статус персональных данных работников/ А.А. Беденкова, И.С. Хоменко // Вестник науки Сибири. – 2014. – №4 (14). – С. 148 –151

32. Важорова, М. А. История возникновения и становления института персональных данных / М.А. Важорова // Государство и право: теория и практика: материалы Междунар. науч. конф. – Челябинск: Два комсомольца. – 2011. – С. 33 –38.

33. Галатенко, В. А. Информационная безопасность / В.А. Галатенко // Открытые системы. – 1996. – № 1 (15). – С. 38 –43.

34. Гафарова, Г. Г. Информационная безопасность личности / Г.Г. Гафарова, В.В. Смелянская // Безопасность личности: состояние и возможности обеспечения: материалы междунар. науч. –практ. конференции 10 –11 мая 2012 г. Ереван, Пенза, Колин– Социосфера, 2012. – С. 57 –62

35. Гафурова, А.Х. Федеральный закон «О персональных данных»: научно –практический комментарий. / А. Х. Гафурова, Е. В. Доротенко, Ю. Е.

Контемиров; под ред. А.А. Приезжевой. – М.: Редакция «Российской газеты», 2015. – Вып. 11. – 176 с.

36. Грачев, Г. В. Информационно –психологическая безопасность личности: состояние и возможности психологической защиты. / Г.В. Грачев – М.: Изд –во РАГС, 1998. – 67 с.

37. Гутников, О. В. Содержание корпоративных отношений / О. В. Гутников // Журнал российского права. – 2013. – №1 (193). – С. 26 –39

38. Давыдова, Е.В. Персональные данные работников / Е. В. Давыдова // Отдел кадров коммерческой организации. – 2015. – №3. – С. 33 –42.

39. Иванов, С. В. Правовое регулирование информационной безопасности личности в Российской Федерации / С. В. Иванов // Вестник Екатерининского института. – 2014. – № 1 (25). – С. 50 –55.

40. Кафтанникова, В.М. Принципы защиты персональных данных в России и за рубежом / В. М. Кафтанникова // Вестник ЮУрГУ. Серия: Право. – 2013. – №2. – С. 99 –100.

41. Кириллов, А. В. Современные проблемы информационной безопасности личности / А. В. Кириллов, С. А. Матяш // Известия РАРАН. – 2013. – № 1. – С. 104–110.

42. Ковалева, Н. Н. Информационное право России: учеб. пособие. / Н. Н. Ковалева – М.: Дашков и Ко, 2007. –362 с.

43. Копылов, В.А. Информационное право 2 –е изд., перераб. и доп. / В. А. Копылов – М.: Юристъ, 2002. – 512 с.

44. Лескова, Ю.Г. Источники корпоративного права / Ю. Г. Лескова, А.А. Диденко // Власть Закона. – 2015. – № 3. – С. 49 – 65.

45. Мазуров, В.А. Уголовно–правовые аспекты информационной безопасности: учебное пособие / В. А. Мазуров – Барнаул: Изд –во Алт. Ун –та, 2004. – 323 с.

46. Майоров, В.И. Проблемы обеспечения безопасности в информационной сфере / В. И. Майоров, Е. В. Дорогова // Вестник Челябинского государственного университета. – 2015. – № 13 (368). – С. 48–55.

47. Минбалеев, А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: монография / А. В. Минбалеев – Челябинск: Цицеро, 2012. – С. 374

48. Михайлюк, И.В. Защита персональных данных участников корпоративных отношений / И.В. Михайлюк, В. Н. Белова// Журнал «Акционерное общество вопросы корпоративного управления». – 2012. – №9. – С. 71 –79

49. Сагиндыкова, А. Н. Конституционно –правовая стабильность общества и государства РФ: состояние, проблемы, перспективы: монография / А. Н. Сагиндыкова, А. Л. Ховралев. – Екатеринбург: Урал. юрид. ин–т МВД России, 2003. – 144 с.

50. Сайханова, Х.И. Информатизация общества как одна из закономерностей современного социального прогресса / Х. И. Сайханова // Международный журнал гуманитарных и естественных наук. – 2016. – № 1. – С. 195 –198.

51. Самигуллин, В.К. Локальное нормативное регулирование в механизме современного правового регулирования общественных отношений / В. К. Самигуллин // Вестник ВЭГУ. – 2015. – № 4 (78). – С. 68 –77.

52. Сизоненко, А.Б. Классификация информации ограниченного доступа в соответствии с законодательством Российской Федерации / А. Б. Сизоненко // Вестник КРУ МВД России. – 2010. – №4. – С. 91 –96.

53. Соколова, Г.А. Персональные данные работников / Г. А. Соколова // Кадровая служба и управление персоналом предприятия. – 2013. – №7. – С. 20-33.

54. Стахов, А. И. Административно –публичное обеспечение безопасности в Российской Федерации: монография / А. И. Стахов; науч. ред. Б. В. Россинский. – М.: Юнити –Дана: Закон и право, 2006. – 200 с.

55. Стрельцов, А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред. В. А. Садовничего, В. П. Шерстюка – М.: МНЦМО, 2002. – 86 с.

56. Тихомирова, Л. В. Защита персональных данных работника: учеб. – практ. пособие / Л.В. Тихомирова. – М., 2013. – 57 с.

57. Шафикова, Г.Х. К вопросу о защите персональных данных работника / Г. Х. Шафикова – Челябинск: ЮУрГУ. Сборник научных трудов «Региональная информационная экономика». – 2002. – С. 359 – 362.

58. Шиткина, И.С. Корпоративное право в таблицах и схемах. 2 –е изд., перераб. и доп. / И. С. Шиткина– М.: Юстицинформ, 2016. – 556 с.

## Раздел IV Диссертации и авторефераты диссертаций на соискание ученой степени

59. Безпрозванный, В.И. Правовой механизм предоставления акционерам информации о деятельности акционерного общества, участниками которого они являются: дис. ... канд. юрид. наук / В. И. Безпрозванный. –М., 2012. – 210 с.

60. Белгородцева, Н.Г. Теоретико –правовые аспекты защиты персональных данных: дис. ... канд. юрид. наук / Н. Г. Белгородцева. – М., 2012. – 201 с.

61. Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: дис. ... канд. юрид. наук. / А.В. Кучеренко. – Челябинск, 2010. – 212 с.

62. Станскова, У.М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореферат

диссертации, дис. ... канд. юрид. наук. / У. М. Станскова. – Екатеринбург, 2014. – 23 с.

63. Тамодлин, А. А. Государственно –правовой механизм обеспечения информационной безопасности личности: дис. … канд. юрид. наук. / А.А. Тамодлин– Саратов, 2006. – 175 с.