ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

ИСТОРИКО-ФИЛОЛОГИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА РОССИЙСКОЙ ИСТОРИИ И ДОКУМЕНТОВЕДЕНИЯ

ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ ООО «ТИТОВСКИЙ КИРПИЧНЫЙ ЗАВОД»)

Выпускная квалификационная работа
обучающегося по направлению подготовки
46.04.02 Документоведение и архивоведения
заочной формы обучения, 02031656 группы
Табунщиковой Анны Ивановны

Научный руководитель
кандидат политических наук,
доцент Половнева Л.С.

Рецензент
кандидат исторических наук,
доцент Смоленская О.А.

БЕЛГОРОД 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Согласно ст. 23 Конституции Российской Федерации каждый человек имеет право на неприкосновенность частной жизни, личную, семейную тайну, защиту своей чести и доброго имени. Реализация этих основополагающих правовых положений обеспечивается ст. 24 Конституции РФ, устанавливающей, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Эти правовые положения применительно к работникам получили свое развитие в главе 14 Трудового Кодекса Российской Федерации, федеральных законах и иных нормативных актах, содержащих нормы трудового права.

Право на защиту персональных данных работником является его неотъемлемым правом, проявлением конституционного права на неприкосновенность и уважение частной жизни.

Жизнедеятельность человека предполагает предоставление информации о себе другим членам общества. Эффективное управление поведением работника в процессе труда возможно лишь при наличии достоверных сведений о его личности, представленных в достаточном объеме. Отношения по предоставлению и охране информации регулируются нормами российского права.

Проблема обеспечения желаемого уровня защиты информации весьма сложная, требующая для своего решения целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов по защите персональных данных человека. Поэтому чем больше современных технологий будут применяться в качестве защиты персональных данных, тем меньше риски утечки или потери таковых.

Законодательная база урегулирования правоотношений связанных с защитой персональных данных работников в нормативно-правовом плане достаточно обусловлена, но должного их обеспечения не происходит. Не редко получаемая информация работодателем становится известной заинтересо-

ванным лицам, зачастую ответственные за сохранение данных в тайне служащие пренебрегают своими должностными обязанностями вследствие чего, и происходит распространение данных.

Ввиду особой важности документов по защите персональных данных, руководство каждой организации должно учитывать, что отсутствие определенного пакета документов регулирующих эту защиту расценивается как нарушение трудового законодательства РФ.

Злободневность выбранной темы обуславливается еще и тем, что в своем большинстве коммерческие организации уделяют недостаточно внимания вопросам документационной защиты персональных данных. Многие работодатели не учитывают все особенности делопроизводства в этой сфере и зачастую не в полном объеме исполняют требования законодательства, ссылаясь на рекомендательный характер нормативно-методических документов, обеспечивающих документационную защиту персональных данных в коммерческих организациях. Все эти факторы обусловливают актуальность настоящего выпускного квалификационного исследования.

Степень изученности проблемы. Проблемы документационной защиты персональных данных в коммерческих организациях составили труды общетеоретического и отраслевого характера, в частности: М.И. Басакова[1], Т.А. Быковой[2], Т.А. Гугуевой[3], Д.Л Кузнецова[4], И.Н. Кузнецова[5] Н.Н. Куняева[6], Ю.А Панасенко[7], О.П. Сологуб[8], М.В. Стенюкова[9] и др. Представите-

---

[1] Басаков М.И. Документационное обеспечение управления (Делопроизводство): Учебник. - Рн/Д., 2013. - 350 с.

[2] Быкова Т.А. Делопроизводство: Учебник / Под ред. Т.В. Кузнецова. - М., 2013. - 364 с.

[3] Гугуева Т.А. Конфиденциальное делопроизводство: Учебное пособие. - М., 2012. - 192 с.

[4] Кузнецов Д.Л. Кадровое делопроизводство (правовые основы): Практическое пособие. - М., 2013. - 239 с.

[5] Кузнецов И.Н. Документационное обеспечение управления. Документооборот и делопроизводство: Учебник и практикум. - Люберцы, 2016. - 477 с.

[6] Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: Учебник. - М., 2015. - 500 с.

[7] Панасенко Ю.А. Делопроизводство: документационное обеспечение управления: Учебное пособие. - М., 2013. - 112 с.

[8] Сологуб О.П. Делопроизводство: составление, редактирование и обработка документов: Учебное пособие. - М., 2013. - 207 с.

лей науки трудового права: З.С. Богатыренко[10], С.А Борисовой[11], О.М. Крапивина[12], А.С. Маркевича[13], А.Я. Петрова[14] и др.

Исследования, посвященные вопросам правового регулирования в информационной сфере: А.В. Кротова[15], И.В. Минаевой[16] и др. А также труды ученых в области документационной защиты персональных данных: К. В. Васильевой[17], Ю.С. Корякиной[18], Т.В. Кузнецовой[19], М.Н.Малеиной[20], А.В.Меньшиковой[21], С.А Румянцевой[22], В. Сафонова[23], М.А. Федосовой[24], С.С. Хачатуровой[25], Ю.А. Хачатурян[26] и др.

---

[9] Стенюков М.В. Делопроизводство. Организация документационного обеспечения предприятия. - М., 2007. - 176 с.

[10] Богатыренко З. С. Новейшие тенденции защиты персональных данных работника в российском трудовом праве // Трудовое право. - 2006. - № 10. - С. 29-51.

[11] Борисова С. А. Общие требования при обработке персональных данных работника и гарантии их защиты // Трудовое право. - 2005. - № 11. - С. 30-36.

[12] Крапивин О. М. Трудовой договор. Заключение. Изменение. Прекращение. Защита персональных данных работников. - М., 2006. - 223 с.

[13] Маркевич А. С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях: дис. ... канд. юрид. наук. - Воронеж, 2006. - 170 с.

[14] Петров А. Я. О персональных данных работника: современное состояние правового регулирования // Трудовое право. - 2008. - № 4. - С. 90-96.

[15] Кротов А. В. Опыт обработки персональных данных работника в компании // Информ. право. - 2007. - № 2. - С. 21-24.

[16] Минаева И. В. Электронная база данных по оценке деловых и личностных качеств работника // Газовая промышленность. - 2007. - № 3. - С. 78-80.

[17] Васильева К. В. Правила работы с персональными данными сотрудников // Делопроизводство и документооборот на предприятии. - 2008. - № 9. - С. 32-52.

[18] Корякина Ю.С. Разрабатываем Положение о защите персональных данных // Справ. по упр. персоналом. - 2007. - № 7. - С. 90-92.

[19] Кузнецова Т.В. Организация работы с персональными данными // Трудовое право. - 2011. - № 5. - С. 75 - 80.

[20] Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. - 2010. - № 11. - С. 19 - 24.

[21] Меньшикова А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения // Экономика и менеджмент инновационных технологий. - 2014. - № 11. - С.156.

[22] Румянцева С. А. Конфиденциальная информация. Правовые основы конфиденциальности // Справочник секретаря и офис-менеджера. - 2008. - №8. - С. 16-20.

[23] Сафонов В. Использование персональных данных работника // Кадровик. - 2015. - № 8. - С. 28-34.

[24] Федосова М. А. Защита персональных данных работника // Финансовые и бухгалтерские консультации. - 2010. - № 11. - С. 71-74.

[25] Хачатурова С.С. Персональные данные под защиту! // Международный журнал прикладных и фундаментальных исследований. - 2016. - № 5-4. - С. 666-668.

[26] Хачатурян Ю.А. Право работника на защиту персональных данных: проблемы применения законодательства // Кадровик. - 2015. - № 9. - С. 23-29.

Однако в связи с рекомендательным характером большинства нормативно-методических документов, регулирующих документационную защиту персональных данных в коммерческих организациях, а также постоянными изменениями законодательства проблемы организации и вопросы совершенствования работы по защите персональных данных оставляют широкое поле для исследований.

Объектом исследования является документационное обеспечение защиты персональных данных в коммерческих организациях.

Предметом выступает документационное обеспечение защиты персональных данных, на примере ООО «Титовский кирпичный завод».

Цель работы - изучение нормативных правовых актов обеспечивающих охрану персональных данных в коммерческих организациях, на примере документационного обеспечения защиты персональных данных в ООО «Титовский кирпичный завод» и выявление основных направлений его совершенствования.

Указанная цель обусловила определение **следующих задач выпускного квалификационного исследования:**

- рассмотреть понятие, виды и специальные категории персональных данных;
- ознакомиться с принципами и условиями защиты персональных данных работников;
- проанализировать конфиденциальность персональных данных и особенности их обработки;
- определить меры по обеспечению безопасности персональных данных при их обработке в ООО «Титовский кирпичный завод»;
- выявить процедуры документирования при защите персональных данных работников общества;
- разработать положение о защите персональных данных в ООО «Титовский кирпичный завод»;

- разработать инструкцию пользователя по работе с персональными данными в обществе.

Источниковая база. Для полного раскрытия темы исследования были изучены нормативные правовые акты, методические указания, регламентирующие документационную защиту персональных данных:

1. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных»[27];

2. Конституция Российской Федерации[28] - основной закон государства, определяющий основные права и свободы человека и гражданина, в частности право осуществлять поиск и получение любой информации в любых формах и из любых источников. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

3. Гражданский кодекс Российской Федерации[29] положения которого регламентирует порядок защита нематериальных благ, посредством компенсации морального вреда;

4. Кодекс РФ об административных правонарушениях[30] содержит положения, определяющие ответственность за нарушения законодательства по защите персональных данных;

---

[27] «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Бюллетень международных договоров. - 2014. - № 4.

[28] Конституция Российской Федерации от 12.12.1993 (с изм. в ред. от 21.07.2014) // Собрание законодательства РФ. - 04.08.2014. - № 31. - Ст. 4398.

[29] Гражданский кодекс Российской Федерации (часть вторая) (ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 01.09.2018) // Собрание Законодательства Российской Федерации. - 1996. - № 5. - Ст. 410.

[30] Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30 декабря 2001 г. (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Собрание законодательства РФ. - 2002. - № 1 (ч. 1). - Ст. 1.

5. Уголовный кодекс РФ[31] предусматривает уголовную ответственность за нарушения законодательства по защите персональных данных;

6. Трудовой кодекс РФ[32] устанавливает объем персональных данных, их хранение и распространение осуществляется только с согласия сотрудника. Никакая информация не может быть передана 3-м лицам без указания причины и получения письменного подтверждения согласия. Любые данные могут использоваться руководителем и кадровой службой только в предусмотренных законом случаях;

7. Федеральный закон «Об информации, информационных технологиях и о защите информации»[33] настоящий Федеральный закон регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации;

8. Федеральный закон «О персональных данных»[34] регулирует отношения, связанные с защитой информации – персональных данных физического лица при их обработке; содержит положения, ограничивающие доступ к документам, в том числе при возникновении трудовых отношений между работодателем и работником;

9. Федеральный закон «Об архивном деле в Российской Федерации»[35] настоящий Федеральный закон регулирует отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов независимо от

---

[31] Уголовный кодекс Российской Федерации № 63-ФЗ от 13 июня 1996 г. (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Собрание законодательства РФ. - 1996. - № 25. - Ст. 2954.

[32] Трудовой кодекс Российской Федерации № 197-ФЗ от 30 декабря 2001 г. (ред. от 27.12.2018) // Собрание законодательства РФ. - 2002. - № 1 (ч. 1). - Ст. 3.

[33] Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. (ред. от 18.12.2018) // Собрание законодательства РФ.- 2006. - № 31 (1 ч.). - Ст. 3448.

[34] Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 г. (ред. от 31.12.2017) // Собрание законодательства РФ. - 2006. - № 31 (1 ч.).- Ст. 3451.

[35] Федеральный закон № 125-ФЗ «Об архивном деле в Российской Федерации» от 22 октября 2004 г. (ред. от 28.12.2017) // Собрание законодательства РФ. - 2004. - № 43. - Ст. 4169.

их форм собственности, а также отношения в сфере управления архивным делом в Российской Федерации в интересах граждан, общества и государства;

10. Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[36] регулирует сбор и обработку персональных данных при предоставлении государственных и муниципальных услуг;

11. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»[37] в котором установлен перечень сведений носящих конфиденциальный характер;

12. Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[38] настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных;

13. Постановление Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»[39] регламентирует особенности обработки персональных данных, осуществляемой без использования средств автоматизации во исполнение ФЗ № 152- ФЗ;

14. Постановление Правительства РФ №772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометриче-

---

[36] Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 г. (ред. от 29.07.2018) // Собрание законодательства РФ. - 2010. - №31. - Ст. 4179.

[37] Указ Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г. (ред. от 13.07.2015) // Собрание законодательства РФ. -1997. - № 10. - Ст. 1127.

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

[39] Постановление Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. // Собрание законодательства РФ. - 2008. - №38. - Ст. 4320.

ских персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации»[40] определяет состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающий обработку, включая сбор и хранение, биометрических персональных данных;

15. Приказ ФСТЭК России №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[41.] Данный документ регламентирует организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

16. Приказ Минкультуры РФ №558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»[42] содержит сроки хранения документов содержащих персональные данные;

---

[40] Постановление Правительства РФ №772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» от 30 июня 2018 г. // Собрание законодательства РФ. - 2018. - №28. - Ст. 4234.

[41] Приказ ФСТЭК России №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. (Зарегистрировано в Минюсте России 14.05.2013 № 28375) (ред. от 23.03.2017) // Российская газета. - 2013. - 22 мая.

[42] Приказ Минкультуры РФ №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» от 25 августа 2010 г. (Зарегистрировано в Минюсте РФ 08.09.2010 №18380) // Бюллетень нормативных актов федеральных органов исполнительной власти. - 2011. - №38.

17. «ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов»[43] устанавливает основные правила оформления документов, требования к содержанию информации бланка, порядок адресования, согласования, подписания и утверждения документов;

18. «ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»[44] устанавливает термины и определения понятий в области делопроизводства и архивного дела на современном этапе;

19. «ГОСТ Р ИСО 15489-1-2007. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»[45] содержит положения, регламентирующие основные процессы управления документами всех форматов на любых видах носителей в соответствии с международными стандартами ИСО 9001 и ИСО 14001; методические рекомендации по проектированию и внедрению системы управления документами;

Важнейшими источниками сведений, так же стали локальные акты, регламентирующие защиту персональных данных ООО «Титовский кирпичный завод».

Методологическую основу выпускного квалификационного иссле-

---

[43] ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 08.12.2016 № 2004-ст) (ред. от 14.05.2018). - М.: Стандартинформ, 2017. - 18 с.

[44] ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст). - М., 2014. - 26 с.

[45] «ГОСТ Р ИСО 15489-1-2007. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования» (утв. Приказом Ростехрегулирования от 12.03.2007 № 28-ст). - М., 2007. - 19 с.

дования составляют концептуальные положения диалектической теории познания, а также основанные на ней общенаучные и частнонаучные методы исследования**:** сравнительный, изучение документов, метод наблюдения, опрос, беседа, аналитический, статистический и графический методы.

Апробация результатов выпускного квалификационного исследования. Выпускная квалификационная работа выполнена, рассмотрена и одобрена на кафедре архивоведения и документоведения НИУ Белгородский государственный национальный исследовательский университет. Отдельные выводы и предложения исследования нашли отражение в форме докладов и сообщений на научных, научно-практических конференциях по вопросам защиты персональных данных различного уровня.

Отдельные теоретические положения настоящего исследования получили отражение в научных публикациях автора и находятся в электронном архиве открытого доступа НИУ "БелГУ"[46].

Научное и практическое значение исследования заключается в систематизации документационной защиты персональных данных в ООО «Титовский кирпичный завод», разработке методических документов, основанных на использовании современной нормативно-правовой базы, регламентирующей защиту персональных данных работников общества. Материалы исследования могут использоваться также и сотрудниками отдела кадров обществ с целью совершенствования делопроизводства в сфере защиты персональных данных.

Структура, объем, и содержание выпускной квалификационной работы определены целями и задачами исследования. Работа состоит из введения, трех глав, включающих в себя семь параграфов, заключения, библиографического списка и приложений.

---

[46] Табунщикова, АИ. Нормативно - правовые акты, регулирующие защиту персональных данных работника // Электронный архив открытого доступа Белгородского государственного университета. - Белгород, 2018. - Режим доступа: http://dspace.bsu.edu.ru/handle/123456789/22499; Табунщикова, А.И. Становление и развитие делопроизводства в России // Электронный архив открытого доступа НИУ БелГУ. - Белгород, 2016. - Режим доступа: http://dspace.bsu.edu.ru/handle/123456789/16714 и др.

Во введении дается обоснование актуальности выбранной темы, анализируется степень ее изученности, определяется объект, предмет, цель и задачи исследования; раскрываются методы исследования, научная и практическая значимость работы, дается анализ использованных источников.

В первой главе выпускной квалификационной работы «Организация защиты персональных данных в коммерческой организации» раскрыто содержание понятия «персональные данные», рассмотрены признаки и критерии для классификации персональной информации, исследованы принципы и условия защиты персональных данных, охарактеризован порядок обеспечения конфиденциальности таких данных при их обработке.

Вторая глава выпускной квалификационной работы «Организация работы с персональными данными в ООО «Титовский кирпичный завод»» посвящена характеристике основных и дополнительных мер обеспечения безопасности персональных данных при их обработке, а также документированию процедур защиты персональных данных в данном Обществе.

В третьей главе выпускной квалификационной работы «Совершенствование работы с документами, регламентирующими защиту персональных данных в ООО «Титовский кирпичный завод»» содержатся предложения по совершенствованию организации делопроизводства Общества в сфере защиты персональных данных.

Заключение выпускной квалификационной работы содержит выводы и практические рекомендации по результатам проведенного исследования.

В приложении к выпускной квалификационной работе содержатся: Акты, Приказы, Согласие на обработку персональных данных, а также разработанные проекты Положения о защите персональных данных ООО «Титовский кирпичный завод» и Инструкции пользователя по работе с персональными данными.

ГЛАВА 1.
ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

1.1. Понятие и виды персональных данных

Конституция РФ[47], как Основной Закон государства, в соответствии со ст. 23 гарантирует право каждого на неприкосновенность частной жизни. Одним из важнейших направлений обеспечения права на неприкосновенность частной жизни является защита персональных данных граждан, поскольку каждый из них в процессе своей жизнедеятельности вынужден вступать во взаимоотношения с различными предприятиями, организациями, учреждениями. В результате этого у них накапливаются данные о конкретном индивиде, начиная с самых простых (фамилии, имени, отчества, даты и места рождения и т.п.) и заканчивая очень специфическими (сведениями о заболеваниях, судимостях, размерах доходов, имуществе и пр.). При этом гражданин желает, чтобы сведения о нем являлись конфиденциальными, изнеизвестными широкому кругу лиц. В целях защиты всей этой информации используется специальный правовой режим персональных данных[48].

Примечателен тот факт, что в развитых странах персональные данные защищаются на государственном уровне уже давно на протяжении нескольких десятилетий и постоянно совершенствуются. Так, например, в апреле 2016 года Европейский парламент только одобрил реформу о конфиденциальности данных и уже в мае 2016 года в ЕС был принят Общеевропейский регламент о персональных данных (General Data Protection Regulation, GDPR) - замена Data Protection Directive (официально Директива 95/46 / ЕС о защите

---

[47] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 2014. - №31. - Ст. 4398.

[48] Стрельников В. Персональным данным - особую защиту // ЭЖ-Юрист. - 2013. - №12. - С. 6.

физических лиц в отношении обработки персональных данных и о свободном движении таких данных)). Документ вступил в действие с 25 мая 2018 года.

Следует отметить, что GDPR применяется ко всем компаниям, обрабатывающим персональные данные резидентов и граждан ЕС, независимо от местонахождения такой компании. Персональные данные согласно GDPR - это любая информация, относящаяся к физическому лицу или данные, которые могут прямо или косвенно идентифицировать этого человека. Например: Имя, адрес электронной почты, адрес проживания, номер телефона; Персональная информация (например, сексуальная ориентация, расовая принадлежность, политические пристрастия); Банковские сведения; IP-адрес компьютера, cookie ID[49].

Согласно данному закону потребители получили более широкий контроль над своими данными. Физические лица теперь имеют следующие права: Право доступа - знать, какая информация о них хранится и как она обрабатывается; Право на исправление - вносить изменения в личные данные, если они являются неточными или неполными; Право на забвение - удалить свои личные данные без необходимости указания конкретной причины; Право на ограниченную обработку - блокировать или запрещать обработку своих персональных данных; Право на перенос данных - сохранять и повторно использовать свои личные данные для собственных целей; Право на возражение - возражать против использования персональных данных. Например, в целях маркетинга, научных и исторических исследований и т.д.

Несоблюдение требований нового регламента GDPR может привести к наложению надзорным органом в области защиты персональных данных штрафа в размере до 20 млн. евро или до 4% от годового оборота компании (в зависимости от того, какая сумма будет больше)[50].

---

[49] Регламент Евросоюза о персональных данных. - URL: http://www.tadviser.ru/index.php/ (дата обращения: 05.01.2019).

[50] Защита персональных данных в Евросоюзе и США. - URL: http://www.tadviser.ru/index.php/(дата обращения: 05.01.2019).

Действие GDPR распространяется на операции по обработке персональных данных в контексте присутствия на территории ЕС их оператора или обработчика, независимо от того, производится ли такая обработка на территории ЕС или нет. Также Действие GDPR распространяется на обработку персональных данных, находящихся на территории ЕС субъектов, которая осуществляется оператором или обработчиком, не имеющим присутствия на территории ЕС (например, российские юридические лица), в тех случаях, когда такая деятельность по обработке относится к: предложению товаров или услуг находящимся на территории ЕС субъектам персональных данных, как на возмездной, так и на безвозмездной основе; отслеживанию их действий при условии, что таковые осуществляются в пределах ЕС. Примечателен тот факт, что в критериях отсутствует привязка к гражданству субъекта персональных данных. Под защиту GDPR попадают персональные данные всех субъектов в момент нахождения их внутри ЕС (включая граждан РФ).

Цифровая трансформация государства, бизнеса и общества несет новые риски и угрозы информационной безопасности граждан США и Великобритании. Корпоративные базы данных, содержащие имена, даты рождения, номера удостоверений личности и другую чувствительную информацию о сотрудниках или клиентах, все чаще становятся объектом посягательства. Такие правонарушения в этих странах именуются «кража личности». Так, например, в США в качестве удостоверения личности используют SSN (Social Security Number), который запрашивают большое количество организаций для подтверждения личности граждан. Похитив номер SNN, злоумышленники способны, например, испортить кредитную историю своей жертвы. В Англии для осуществления «кражи личности» используются страховые идентификаторы NINO (National Insurance number) и NHS (National Health Service Number)[51]. Как видим, на безопасность персональных данных граж-

[51] Защита персональных данных в Евросоюзе и США. - URL: http://www.tadviser.ru/index.php/(дата обращения: 05.01.2019).

дан не влияет ни политический режим в стране, ни уровень ее экономического развития.

В отличие от иностранных правопорядков, отечественное законодательство, регламентирующее сбор, хранение и обработку персональных данных берет свое начало только с 2006 года, с момента принятия Федерального закона РФ № 152-ФЗ «О персональных данных»[52]. Следует признать, что до 2006 года нормативная правовая база, регулирующая персональные данные, носила разрозненный характер, существовало множество нормативных правовых актов, предусматривающих различные условия и правовые основания обработки персональных данных субъектов. На данный момент российской системе защиты прав субъектов персональных данных исполнилось почти тринадцать лет. В течение указанного периода было были созданы: национальное законодательство в области персональных данных, уполномоченный орган, обладающий контрольно-надзорными полномочиями в области персональных данных, система санкций, предусматривающих ответственность за нарушение требований законодательства и прав граждан-субъектов персональных данных. Всё это позволило гражданам обрести реальную возможность защитить свои персональные данные от угроз, возникающих при обработке их персональных данных. Тем не менее, отечественная правовая система еще далека от идеала и нуждается также как и иностранные модели в постоянном совершенствовании. Об отрицательной динамике свидетельствует и то, что на протяжении последних лет идет тенденция к увеличению числа правонарушений в сфере оборота персональных данных, и как следствие росту направляемых в суды материалов об административных правонарушениях. Так, например, согласно последним открытым данным, полученным с официального сайта Роскомнадзора, в 2016 году по результатам плановых проверок было выявлено 2 134 нарушения обязательных требований законо-

[52] Федеральный закон РФ № 152-ФЗ «О персональных данных» от 27 июля 2006 г. (ред. от 31.12.2017) / / Собрание законодательства РФ. - 2006. - № 31. - (1 ч.). - Ст. 3451.

дательства Российской Федерации в области персональных данных[53]. Анализ результатов контрольно-надзорной деятельности территориальных органов Роскомнадзора показал, что наиболее частыми нарушениями, выявленными при проведении плановых мероприятий, в 2016 году явились: Представление в Уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения (ч. 3 ст. 22 Федерального закона № 152-ФЗ) - примерно 11% от общего количества выявленных в 2016 году нарушений. Несоответствие содержания письменного согласия субъекта персональных данных на обработку персональных данных требованиям законодательства Российской Федерации (ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») - примерно 9% от общего количества выявленных в 2016 году нарушений. Отсутствие в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных (ч. 3 ст. 6 Федерального закона № 152-ФЗ) - примерно 8% от общего количества выявленных в 2016 году нарушений. В 2016 году территориальными органами Роскомнадзора было проведено 99 внеплановых проверок, из которых около 80% проведено в целях проверки исполнения ранее выданных предписаний.

По результатам 24 внеплановых проверок было выявлено 41 нарушение обязательных требований законодательства Российской Федерации в области персональных данных, из которых 75% касались невыполнения в установленный срок законного предписания Уполномоченного органа по защите прав субъектов персональных данных, осуществляющего государственный надзор (контроль), об устранении нарушений законодательства Российской Федерации в области персональных данных. По результатам контрольно-надзорных мероприятий в 2016 году было выдано 619 предписа-

[53] Сайт Роскомнадзора. - URL: - https://rkn.gov.ru/docs/Otchet ZPD 2016.pdf (дата обращения: 12.12.2018).

ний об устранении выявленных нарушений. Территориальными органами Роскомнадзора составлено и направлено на рассмотрение в суды 6 930 протоколов об административных правонарушениях, по результатам рассмотрения которых в 2016 году сумма взысканных административных штрафов в области персональных данных составила 3 713 814,56 рубля, или 62% от общей суммы наложенных судами административных штрафов, которая составила в 2016 году 5 982 200 рублей.

В свою очередь, территориальными органами Роскомнадзора в 2015 году были проведены 1 292 контрольно- надзорных мероприятия, из них 883 проверки в целях выполнения плана деятельности территориальных органов Роскомнадзора, что составляет 91% от количества запланированных проверок, и 99 внеплановых проверок, что составляет 10% от количества проведенных мероприятий. В процессе проведения данных проверок предметом исследования являлась деятельность по обработке персональных данных, изучались информационные системы персональных данных, а также проводился анализ документов, характер информации в которых предполагает включение в них персональных данных. В рамках реализации функции по осуществлению государственного контроля и надзора в 2015 году проведено 1 160 плановых и 104 внеплановых проверки, а также 132 плановые проверки в отношении государственных органов, муниципальных органов, организующих и (или) осуществляющих обработку персональных данных. Анализ результатов проведенных контрольно- надзорных мероприятий территориальными органами Роскомнадзора в 2015 году показывает, что каждая вторая проверка оператора выявляет нарушения. Так, при проведении 461 плановой проверки, что составляет 52% от проведенных плановых проверок, было выявлено 1 397 нарушений. Количество выявленных нарушений при проведении плановых проверок в 2015 году на 37% больше числа выявленных нарушений в 2014 году. Одним из наиболее частых нарушений, выявляемых при проведении плановых проверок, является представление в уполномоченный орган уведомления об обработке персональных данных,

содержащего неполные и (или) недостоверные сведения, что показывают результаты 197 контрольно-надзорных мероприятий. По результатам проведения 195 мероприятий выявлено отсутствие в поручении лицу, которому оператором доверяется обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности. По итогам выявленных нарушений при проведении контрольно-надзорных мероприятий территориальным органами Роскомнадзора выдано 731 предписание об устранении установленных нарушений.

За отчетный период территориальными органами Роскомнадзора составлен и направлен на рассмотрение в суды 7721 протокол об административных правонарушениях, по результатам, рассмотрения которых наложено 10 454 600 рублей штрафов, из них взыскано 4 818 615 рублей.

Следует отметить, что из года в год растет количество обратившихся в Роскомнадзор за защитой своих прав как субъектов персональных данных граждан, прием которых ведется должностными лицами данной организацией с 2008 года. На рисунке 1.1 можно увидеть динамику такого обращения с 2008 по 2015 годы[54].

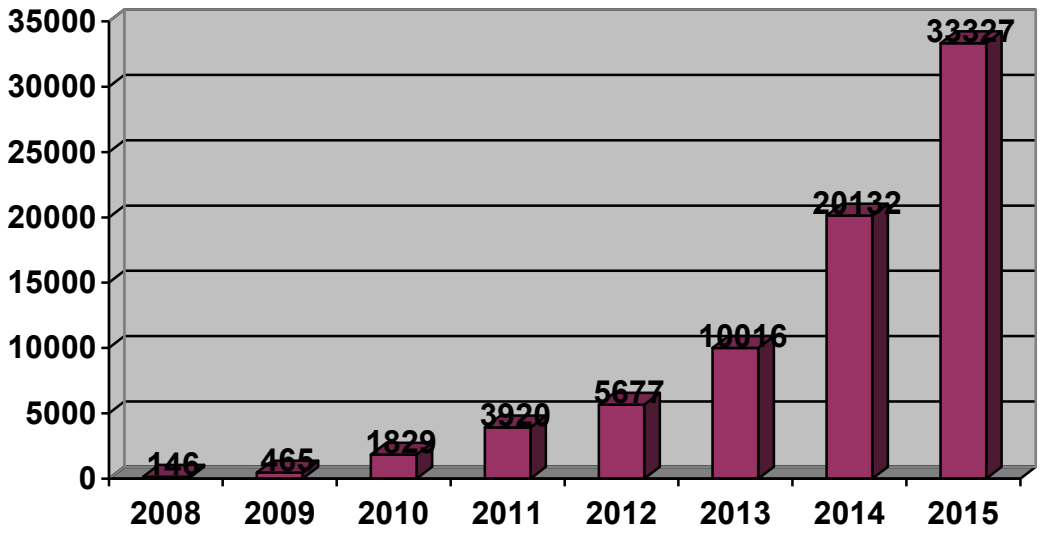

Рис. 1.1. Количество граждан, обратившихся в Роскомнадзор за защитой своих прав в 2008-2015гг.

[54] Сайт Роскомнадзора. - URL: - https://rkn.gov.ru/docs/Otchet ZPD 2016.pdf (дата обращения: 12.12.2018).

Наибольшее количество жалоб граждан поступило на действия кредитных учреждений (14710), владельцев интернет-сайтов (в том числе социальных сетей) (3574), организаций ЖКХ (1425). Более наглядно это можно увидеть на рисунке 1.2. На действия данных категорий операторов традиционно поступает множество жалоб, что в первую очередь связано с обработкой ими персональных данных значительного числа граждан.

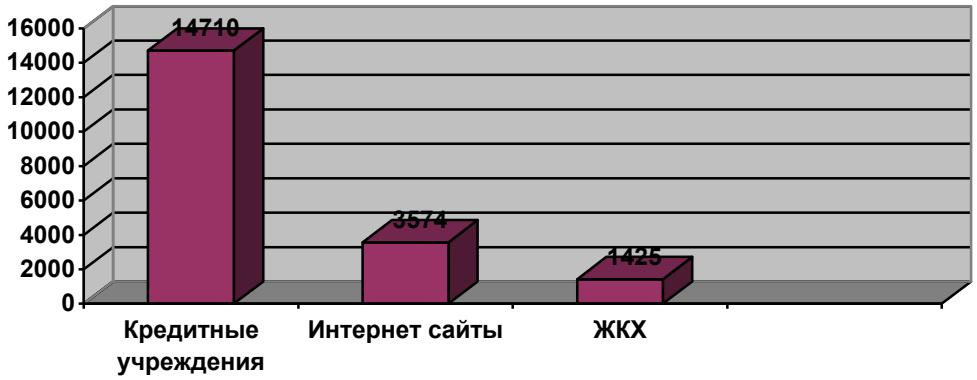

Рис.1.2. Количество жалоб граждан о нарушении законодательства о персональных данных учреждениями различных отраслей

Следует отметить, что в Роскомнадзор уже традиционно поступает наибольшее количество жалоб граждан на банковскую сферу в части нарушения прав субъектов персональных данных. Причем количество жалоб из года в год только увеличивается.

В отношении кредитных учреждений распространены жалобы на: действия, связанные с передачей персональных данных без согласия субъектов персональных данных; несоответствие ч. 4 ст. 9 Закона № 152-ФЗ в части, касающейся согласия на обработку персональных данных (избыточный объем обрабатываемых персональных данных по отношению к заявленным целям обработки); отказ от удаления обрабатываемых персональных данных по истечении срока договора; по достижении цели обработки персональных данных; неправомерные действия банка в части передачи персональных данных должников третьим лицам для истребования долга в случае непогашения кредита/неосуществления своевременных платежей, в случае отзыва согла-

сия на обработку персональных данных; неправомерную обработку персональных данных третьих лиц (поручителей); противоречие законодательству в области персональных данных (посмертная обработка персональных данных); неправомерную обработку персональных данных после расторжения кредитного договора в одностороннем порядке и передачу персональных данных третьим лицам.

Обращаясь за защитой своих нарушенных прав в сети Интернет, как правило, граждане жалуются на обработку интернет-ресурсами персональных данных в отсутствие их согласия либо иных правовых оснований, на отсутствие на сайте политики в отношении обработки персональных данных, на создание «фейковых» аккаунтов. При анализе указанных обращений Уполномоченный орган руководствуется принципом всесторонности и объективности их рассмотрения. Основанием для принятия мер, в частности направления требования администратору Интернет-ресурса об удалении неправомерно размещенных персональных данных, является отсутствие волеизъявления субъекта, иных правовых оснований для обработки персональных данных, а также отсутствие персональных данных в любых иных открытых источниках сети Интернет.

Большое количество жалоб поступает и на лиц, осуществляющих деятельность в сфере ЖКХ. При этом граждане зачастую жалуются, что их данные были переданы коллекторским организациям или иным третьим лицам, например, расчетным центрам для взыскания задолженностей по коммунальным платежам.

Как видим, как само российское законодательство о персональных данных, так и практика его применения далеки еще от своего идеала и нуждаются в совершенствовании.

На современном этапе значительные трудности в правоприменении вызывают, как определение содержания термина «персональные данные», так и применяемые для их классификации критерии. Обратимся к исследованию каждого из этих правовых явлений.

Так, содержание понятия «персональные данные» в общем виде раскрывается как в международных, так и в отечественных нормативных правовых актах.

В статье 2 Конвенции «О защите физических лиц при автоматизированной обработке персональных данных», заключенной в г. Страсбурге 28.01.1981 г[55]., персональные данные определяются, как: «любая информация об определенном или поддающемся определению физическом лице («субъект данных»). Согласно определению, содержащемуся в ст. 3 Федерального закона «О персональных данных» от 27 июля 2006 г., персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

По справедливому утверждению отдельных исследователей: «ключевым понятием в дефиниции, содержащейся в Законе о персональных данных, является «информация об определенном или определяемом лице», и по смыслу оно тождественно использованному в Конвенции понятию «информация о конкретном или могущем быть идентифицированным лице». Несомненно, в рассматриваемом контексте слово «идентифицирован» более уместно, так как точнее передает смысл формулировки. Именно слово «идентифицирован» использовалось в некоторых редакциях российского законопроекта, однако позднее законодатель отказался от него в пользу слова «определен»»[56].

Н.И. Петрыкина отмечает, что: «разработка определения такого сложного и несколько абстрактного понятия, как персональные данные, не могла не вызвать затруднений, однако закрепленное в Законе о персональных дан-

---

[55] Конвенция «О защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства РФ. - 2014. - №5. - Ст. 419.

[56] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.15.

ных определение, главным смысловым звеном которого является понятие «определение» (или «идентификация»), представляется все же вполне удачным. Именно свойство идентификации (определения) является тем признаком, который позволяет вычленить из общего массива сведений об индивиде те данные, с помощью которых он (индивид) может быть с точностью идентифицирован (определен). Например, личные беседы, которые ведет лицо с кем-либо, относятся к отношениям, охватываемым понятием «частная жизнь», однако не относятся к персональным данным, так как не позволяют идентифицировать субъекта»[57].

В то же время следует помнить, что информация, относящаяся к персональным данным, по своей сути неоднородна. Так, в их структуре можно выделить номинативную информацию и иную информацию.

Номинативной информацией является та информация, которая позволяет провести идентификацию конкретного лица[58]. К ней относятся фамилия, имя, отчество, пол, серия и номер паспорта, дата и место рождения и т.п. Для идентификации человека требуется наличие значительной части номинативной информации, так как отдельные ее элементы не всегда позволяют провести идентификацию личности. Так, правовым средством, индивидуализирующим человека как субъекта правоотношений, является его имя. Однако для идентификации лица этого явно недостаточно хотя бы потому, что носитель определенного имени не может запретить другому лицу носить такое же имя. По этому поводу Е.А. Флейшиц указывала на то, что использование распространенной фамилии само по себе уже не служит средством индивидуализации ее носителя[59]. Отдельные авторы указывают в качестве дополнительных

---

[57] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.15.

[58] Стрельников В. Персональным данным - особую защиту // ЭЖ-Юрист. - 2013. - №12. - С. 6.

[59] Флейшиц Е.А. Личные права в гражданском праве Союза ССР и капиталистических стран // Ученые труды Всесоюзного института юридических наук НКЮ СССР. - М., 1941. Вып. VI. - С. 234.

средств индивидуализации личности его место жительства[60].

В качестве «дополнительной» информации, по мнению отдельных ученых, могут также выступать: «биометрическая информация о лице; данные о супруге, детях, других членах семьи; индивидуальные средства коммуникации (номер телефона, адрес электронной почты, ICQ, персональный сайт или иной личный ресурс в Интернете, например блог или страница в социальной сети); сведения о событиях и обстоятельствах жизни лица, позволяющие его идентифицировать, в том числе аудио- и видеофайлы, и т.д. Перечень сведений, которые могут быть отнесены к персональным данным, является открытым»[61].

Достаточно интересным видится нам позиция российского правоприменителя в отношении индивидуальных средств коммуникации, например, номера сотового телефона. Очевидно, что по номеру сотового телефона можно идентифицировать его владельца, однако, российские суды по данному вопросу занимают противоположную позицию. Проиллюстрируем это примером из судебной практики. Так, «Судебная коллегия по гражданским делам Московского городского суда, рассматривая иск Кубаева А.Г. к АО «Альфа-Банк» о взыскании компенсации морального вреда причиненного незаконной обработкой персональных данных, установила, 17 мая 2014 года между Кубаевым М.Г. и АО «Альфа - Банк» был заключен кредитный договор. При заполнении Анкеты - Заявления Кубаев М.Г. в качестве дополнительного контактного телефона указал номер принадлежащий своему брату - Кубаеву А.Г., с согласия последнего.

Данное обстоятельство также было установлено вступившим в законную силу решением Мещанского районного суда г. Москвы от 07 декабря 2015 года по делу № * по иску Кубаева А.Г. к АО «Альфа-Банк» о взыскании компенсации морального вреда, что в силу ст. 61 ГПК РФ освобождает сто-

---

[60] Гражданское право: Учебник: В 3 т. / Отв. ред. А.П. Сергеев, Ю.К. Толстой. - М., 2006. - Т. 1. - С.345.

[61] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.16.

рону доказывать вновь данное обстоятельство, и не подлежат оспариванию при рассмотрении дела, в котором участвуют те же лица.

Согласно детализации услуг связи абонентского номера * за период с 24.04.2015 г. по 15.05.2015 г. поступило два SMS-сообщения от «Альфа-Банк», и телефонные звонки с разных номеров телефона.

Отказывая в удовлетворении исковых требований, суд первой инстанции исходил из того, что каких-либо объективных и бесспорных доказательств того, что сотрудники АО «Альфа-Банк» каким-либо способом обрабатывали (хранили, распространили либо разгласили, в том числе третьим лицам) персональные данные Кубаева А.Г., истцом представлено не было. Истец не обосновал нарушение установленными противоправными действиями ответчика его личных неимущественных прав либо посягательств на принадлежащие истцу другие нематериальные блага.

Судебная коллегия согласилась с выводами суда первой инстанции, поскольку они соответствовали установленным по делу обстоятельствам, и были сделаны при правильном применении норм материального права и его толковании, на основании представленных сторонами доказательств, которым судом дана надлежащая оценка в порядке ст. 67 ГПК Российской Федерации.

Довод жалобы о том, что телефонный номер абонента относится к персональным данным, суд посчитал несостоятельным, поскольку номер абонента не относится к персональным данным, т.к. не позволяет идентифицировать субъект персональных данных, а является лишь средством передачи данных и звонков. При этом, суд отметил, что в силу ст. 19 ГК РФ, к персональным данным лица следует относить, прежде всего его фамилию, имя, отчество, год, месяц и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, а также другую информацию, при которой возможно идентифицировать конкретное лицо.

Ссылка в жалобе на ст. 19 ФЗ РФ «О персональных данных», по мнению суда, также являлась несостоятельной, поскольку доказательств допуска

ответчиком утечки (передачи) персональных данных при осуществлении обработки персональных данных в отношении Кубаева А.Г. не имеется. При этом, судебная коллегия отмечала, что Кубаев А.Г. не состоял в договорных отношениях с АО «Альфа - Банк», и не являлся ни заемщиком, ни поручителем, в рамках кредитного договора заключенного АО «Альфа - Банк» с Кубаевым М.Г. Кроме того, из представленной стороной истца детализации звонков не следовало разглашение ответчиком персональных данных Кубаева А.Г. В этой связи, Судебная коллегия оставила без изменения Решение Мещанского районного суда г. Москвы от 30 марта 2017 года, а апелляционную жалобу Кубаева А.Г. - без удовлетворения»[62].

Такой подход отечественного правоприменителя видится нам не верным. Мы склонны полагать, что индивидуальные средства коммуникации, позволяют идентифицировать лицо, и в силу положений ст. 8 Федерального закона «О персональных данных» относиться к разряду общедоступных персональных данных.

Поскольку персональные данные исключительно разнообразны и разнородны, то возникает проблема, связанная с их систематизацией и классификацией. Как справедливо было подмечено в специальной литературе: «персональные данные можно по-разному классифицировать, объединять в различные группы в зависимости от избранного критерия и цели классификации, при этом любая такая классификация будет достаточно условной, поскольку некоторые сведения могут в равной степени относиться сразу к нескольким группам»[63].

Исходя из положений Федерального закона «О персональных данных» можно условно выделить три группы персональных данных:

- общедоступные персональные данные;

- специальные категории персональных данных;

---

[62] Апелляционное определение Судебной коллегии по гражданским делам Московского городского суда по делу № 33-28957 от 24 июля 2017 г. // СПС Консультант Плюс: Судебная практика.

[63] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.19.

- биометрические персональные данные.

Согласно ст. 8 Федерального закона №152-ФЗ, К общедоступным персональным данным могут быть отнесены: фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Специальные категории персональных данных касаются: расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (п. 1 ст. 10 Федерального закона «О персональных данных»). В эту же группу входит обработка персональных данных о судимости, которая 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 (п. 3 ст. 10 Федерального закона №152-ФЗ).

Биометрические персональные данные представляют собой сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (ст. 11 Федерального закона «О персональных данных»).

В специальной литературе можно встретить и еще одну классификацию персональных данных по признаку свободы оборота[64]. По данному критерию все персональные данные можно условно разделить на:

- свободно обращаемые;
- ограниченно обращаемые;
- обращаемые в специальных целях;
- запрещенные к обороту.

К свободно обращаемым персональным данным следует относить: имя, фамилия, отчество и пол лица. В некоторых случаях к ним можно добавить

[64] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.23.

возраст, образование, адрес места жительства, номер телефона, т.е. все те минимальные сведения, которые готов сообщить о себе субъект определенному кругу лиц и организаций, составляющих круг его каждодневного социального общения. Как правило, несанкционированное использование этих сведений не может причинить субъекту какого-либо существенного вреда, поэтому применение мер ответственности возможно только в том случае, если нарушен порядок сбора и обработки этой информации (в частности, должностным лицом).

Ограниченно обращаемые персональные данные представляют собой различные виды персональных данных, в том числе и данные регистрационных номеров документов, сообщаемые субъектом (с его согласия) различным организациям и органам с целью совершения каких-либо действий или получения каких-либо услуг. Например, для оформления потребительского кредита заемщик должен сообщить помимо прочих данные о месте работы, должности, размере заработной платы, наличии движимого и недвижимого имущества и т.п. Разглашение или иное несанкционированное использование полученных персональных данных есть грубое нарушение неприкосновенности частной жизни субъекта персональных данных, способное причинить ему моральный и материальный ущерб.

Обращаемые в специальных целях - это те персональные данные, в том числе биометрические, которые собираются государственными, муниципальными и иными уполномоченными органами в рамках их полномочий в соответствии с действующим российским законодательством.

Запрещенные к обороту - это наиболее чувствительная информация, т.е. специальные категории персональных данных. За нарушения положений законодательства о защите специальных категорий персональных данных, по мнению отдельных исследователей, должны устанавливаться наиболее жесткие меры ответственности, вплоть до уголовной ответственности[65].

---

[65] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М., 2011. - С.25.

Наряду с уже существующими классификациями персональных данных можно предложить и свою, авторскую, основанную на отраслевом критерии. По данному критерию можно условно выделить следующие виды персональных данных:

- предоставляемые в государственные и муниципальные органы (например, данные о наличии или отсутствии судимости; о доходах);

- предоставляемые в кредитные организации (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения);

- предоставляемые в медицинские организации (например, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью - в медико-профилактических целях; в целях установления медицинского диагноза и оказания медицинских услуг);

- предоставляемые в организации ЖКХ (например, данные о владении, пользовании и распоряжении недвижимым имуществом);

- предоставляемые в организации связи (например, адреса электронной почты; сведения об аккаунтах; IP-адрес);

- предоставляемые в образовательные учреждения (например, данные о составе семьи, об опеке (попечительстве), об отношение к группе риска, о поведенческом статусе).

Полагаем, что такая классификация в наибольшей мере отражает специфику работы с персональными данными, применительно к целям деятельности каждой конкретной организации.

Подводя итоги по первому параграфу первой главы выпускной квалификационной работы, отметим, что понятие «персональные данные» определяется как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). На современном этапе, такое определение представляет собой максимально широкое понимание данного термина. Такой подход отечественного законодателя следует считать правильным. Классификация персональных

данных возможна по различным критериям и признакам. Наиболее оптимальным, на наш взгляд, является отраслевой критерий, позволяющий систематизировать все персональные данные применительно к целям деятельности каждой конкретной организации.

1.2. Принципы и условия защиты персональных данных работников

Персональные данные представляют собой категорию, способную непосредственно влиять на жизнь, в том числе личную, общественную, трудовую и пр., конкретного индивида. Нарушение правил обработки персональных данных гражданина может сделать его частную жизнь достоянием гласности. Несомненно, что разные специальные категории персональных данных подлежат соответствующей специальной обработке. Однако в целях обеспечения защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, статьей 5 ФЗ РФ №152-ФЗ устанавливаются основные начала обработки персональных данных (принципы).

Первый принцип гласит о том, что обработка персональных данных должна осуществляться на законной и справедливой основе. Учитывая важность функционирования справедливости и законности при обработке персональных данных, считаем чрезвычайно важным для формирования правильного понимания места и роли данных принципов в системе права, остановиться подробно на их рассмотрении.

Следует отметить, что в настоящее время признание верховенства права и закона придает проблеме законности особую актуальность[66]. Ведь законность - важнейшая правовая категория всей юридической науки и практи-

[66] Петрова И.Г. Принцип законности в арбитражном судопроизводстве // Юридический мир. - 2006. - №3. - С. 76.

ки, а ее уровень и состояние служат главными критериями оценки правовой жизни общества и граждан[67].

Что касается справедливости, то, как справедливо подмечено в научной литературе: «она является той базовой, исходной идеей, которая выступает непосредственной основой продуцирования огромного числа других принципов права. В частности, содержательно выводятся из идеи справедливости, конкретизируют, дополняют и выражают ее принципы гуманизма, единства прав и обязанностей, равенства перед законом, ограничения свободы человека правами других лиц, неотвратимости ответственности и наступления ее только за виновно совершенные деяния и многие другие»[68].

Следует отметить, что эти две правовые категории упоминаются законодателем в качестве единого принципа далеко не случайно. Так, еще В.В. Мальцев, справедливо указывает на то, что: «уяснение принципов равенства граждан перед законом (ст. 19 Конституции РФ) и гуманизма (ст. ст. 2, 7, 20, 21 и др. Конституции)... возможно лишь в тесной связи с анализом содержания принципа справедливости», что объясняется «огромным общесоциальным влиянием идеи справедливости на процесс формирования права в целом и тем, что равенство и гуманизм, по существу, являются выражением уравнивающей и распределяющей ее сторон (форм) справедливости»[69]. Рассуждая далее, ученый отмечает, что: «хотя на первый взгляд это кажется парадоксальным, в том числе и законность оказывается «без справедливости... лишена содержания, по сути, мертва» несмотря на то, что содержательно не может быть выведена из нее»[70].

---

[67] Пчелинцев С.С. Современное понимание принципа законности на государственной службе // Юридический мир. - 2010. - №4. - С. 33.

[68] Винницкий И.Е. Роль справедливости и законности в обеспечении целостности и устойчивости системы принципов права // История государства и права. - 2011. - №13. - С. 15.

[69] Мальцев В.В. Равенство и гуманизм как принципы уголовного законодательства // Правоведение. - 1995. - №2. - С. 98.

[70] Мальцев В.В. Принципы уголовного законодательства и общественно опасное поведение // Государство и право. - 1997. - №2. - С. 101.

По мнению А.К. Черненко: «Без справедливости законность, т.е. точное и неукоснительное исполнение законов и иных правовых актов, превращается в формальный акт, лишенный... перспективы»[71].

Содержательная связь всех других принципов права как базовых, основополагающих для него и пронизывающих все сферы его действия идей с принципом справедливости, предопределяет то, что справедливость зачастую рассматривают непосредственно в качестве свойства права[72]. Б.К. Мартыненко полагает, что справедливость придает всей системе устойчивость в условиях проблематичности выбора дальнейшего пути ее развития, которая возникает как вследствие разнообразия опосредующих ее действие внешних факторов, так и в силу множественности самих принципов и их полифункциональности[73].

В литературе также отмечается, что принцип справедливости выступает своеобразным «идейным ядром» системы принципов права, выполняет по отношению к ней функцию системообразования, интеграции входящих в нее структурных компонентов[74].

Принцип справедливости также играет важную роль в обеспечении целостности и устойчивости системы принципов права, дифференцируя последние от других возникающих в сфере действия права и в связи с его функционированием идей[75]. Справедливость выступает главным критерием, определяющим возможность воспроизводства и функционирования той или иной по своему содержательному наполнению идеи именно в качестве принципа права. Справедливое содержание идеи выступает условием ее общественного признания (то, что не является справедливым, объективно не мо-

---

[71] Черненко А.К. Теоретико-методологические проблемы формирования правовой системы общества. - Новосибирск, 2004. - С. 135.
[72] Нерсесянц В.С. Философия права. - М., 1997. - С. 28.
[73] Мартыненко Б.К. Право и справедливость // Философия права в России: теоретические принципы и нравственные основания: Мат-лы Межд. науч. конф. (15 - 17 ноября 2007 г., Санкт-Петербург). - СПб.: Изд-во Санкт-Петербургского ун-та, 2008. - С. 75.
[74] Деревесников А.В. Справедливость как принцип права (историко-теоретический аспект). - Кострома, 2007. - С. 28.
[75] Винницкий И.Е. Роль справедливости и законности в обеспечении целостности и устойчивости системы принципов права // История государства и права. - 2011. - №13. - С. 16.

жет получить общественного признания, и в этой связи можно согласиться с утверждением о том, что «в известной мере справедливость обосновывает другие принципы права»[76]). Оно же становится предпосылкой того, что идея приобретает значение фундаментальной и универсальной, пронизывающей своим действием всю сферу действия права - все то, что наиболее тесно связано с идеей справедливости, не просто позиционируется в качестве базового и общезначимого, но и в действительности становится таковым.

Принимая во внимание изложенные обстоятельства, тем не менее, полагаем, что действие принципа законности является наиболее значимым для обеспечения оборота персональных данных, нежели идеи справедливости не являющейся правовой по своему характеру.

Второй принцип гласит о том, что обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Статья 86 ТК РФ содержит закрытый перечень целей обработки персональных данных работника:

· обеспечение соблюдения законов и иных нормативных правовых актов;

· содействия работников в трудоустройстве;

· получение образования и продвижения по службе;

· обеспечение личной безопасности работников;

· контроль количества и качества выполняемой работы;

· обеспечение сохранности имущества.

Соответственно, обработка персональных данных, выходящая за рамки обозначенных целей, не допустима. Использование такого механизма в трудовых отношениях обеспечивает защиту персональных данных работника от произвольного сбора и обработки. Особая сложность рассматриваемой про-

[76] Вязов А.Л. Принцип справедливости в современном российском праве и правоприменении: теоретико-правовое исследование: Автореф. дис. ... канд. юрид. наук. - М., 2001. - С. 8.

блемы заключается в противостоянии внутри нее разнонаправленных интересов: с одной стороны - интереса работодателя, заинтересованного в поддержании эффективности трудового процесса, обеспечении сохранности своего имущества и безопасности внутрикорпоративной информации, а с другой - интересов работников, подвергаемых риску необоснованного вторжения в их частную жизнь[77]. Эти особенности предопределяют путь решения поставленной проблемы, заключающийся в поиске баланса двух групп интересов и легального закрепления границ вмешательства работодателя в частную жизнь своих сотрудников. Ввиду объективной невозможности детального регулирования всех возможных случаев подобного вмешательства правильным решением является выработка определенных принципов взаимодействия работодателя и работников при осуществлении производственного контроля за последними[78].

Следует отметить, что нецелевая обработка персональных данных является нарушением Закона о персональных данных и влечет за собой наступление юридической ответственности. Например, обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, если эти действия не содержат уголовно наказуемого деяния, - влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей, в соответствии со ст. 13.11 КоАП РФ. Помимо этого, административная ответственность предусмотрена за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, по-

---

[77] Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. - 2013. - №4. - С. 35.
[78] Овсянникова Е. Насколько эффективна защита персональных данных работников? // Трудовое право. - 2013. - №2. - С. 94.

лучившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ). За нецелевую обработку персональных данных может наступить и уголовная ответственность. Так, например, ст. 137 УК РФ предусматривает уголовную ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. В свою очередь, в ст. 272 УК РФ установлена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, в том числе баз персональных данных.

Содержание третьего принципа составляет запрет на объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Так, например, нарушение данного принципа послужило предметом для судебного разбирательства, в результате которого Центральный районный суд г. Челябинска пришел к выводу об обоснованности требований истца о признании действий ответчиков незаконными и необоснованными и взыскании компенсации морального вреда[79].

Четвертый принцип указывает на то, что обработке подлежат только персональные данные, которые отвечают целям их обработки. Например, при формировании электронной базы временных работников, оператора персональных данных - Общество не должны интересовать сведения о судимости, как самого работника, так и членов его семьи.

Пятый принцип гласит о том, что 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. Данный принцип предполагает,

[79] Решение Центрального районного суда г. Челябинска по делу № 2-105/2016 от 31 мая 2016 г. // СПС Консультант Плюс: Судебная практика.

что сбор и обработка должна быть ограничена лишь теми данными, которые минимально необходимы и достаточны для достижения заявленных целей обработки. Наглядным примером нарушения данного принципа может служить следующее дело, в котором «суд апелляционной инстанции сделал правильный вывод о том, что для идентификации личности при приеме на работу достаточно фамилии, имени и отчества, при условии предъявления лицом документа, удостоверяющего личность, в котором содержатся все необходимые сведения. Хранение копий паспорта, страниц военного билета, свидетельства о заключении брака, свидетельства о рождении ребенка, превышает объем обрабатываемых персональных данных работника, нарушает права и свободы гражданина, снижает уровень прав и гарантий работника, противоречит федеральному законодательству. При проведении проверки управление сделало правильный вывод о том, что банк производил обработку избыточных персональных данных, по сравнению с теми, которые определены к заявленным целям их обработки, что является нарушением части 5 статьи 5 Закона № 152-ФЗ»[80].

На наш взгляд, содержание данного принципа можно объединить с предыдущим, назвав его принципом минимизации данных.

Согласно шестому принципу, 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.

Требование точности персональных данных означает, что они должны соответствовать действительности. Употребление законодателем термина достаточность определяет полноту данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем шире

[80] Постановление Федерального арбитражного суда Северо-Кавказского округа по делу № А53-13327/2013 от 21 апреля 2014 г. // СПС Консультант Плюс: Судебная практика.

диапазон методов, которые можно использовать, тем проще подобрать метод, вносящий минимум погрешностей в ход информационного процесса. Актуальность персональных данных представляет собой свойство данных в указанный момент времени представлять интерес для Оператора. Нарушение данного принципа на практике приводит к наложению на виновное лицо административной ответственности. Проиллюстрируем это выдержкой из судебного решения. Так, «Четвертый арбитражный апелляционный суд рассмотрев апелляционную жалобу общества с ограниченной ответственностью «Константа» на решение Арбитражного суда Забайкальского края от 12 февраля 2018 года по делу №А78-19156/2017 по заявлению Управления Федеральной службы судебных приставов по Забайкальскому краю к обществу с ограниченной ответственностью «Константа» о привлечении к административной ответственности по части 2 статьи 14.57 Кодекса Российской Федерации об административных правонарушениях установил, что ООО «Константа», являясь оператором по обработке персональных данных, не приняло необходимых и достаточных мер по уточнению данных, представленных должником, в том числе не установило факт принадлежности номера телефона +79145026779 именно Астраханцеву О.П., что привело к нарушению прав третьего лица Запасных М.З. и положений Закона № 230-ФЗ при осуществлении деятельности по взысканию задолженности Астраханцева О.П. Учитывая вышеизложенные обстоятельства дела, Четвертый арбитражный апелляционный суд, посчитал, что суд первой инстанции, верно, пришёл к выводу о наличие в действиях общества события административного правонарушения, предусмотренного часть 2 статьи 14.57 КоАП РФ»[81].

Заключительный принцип гласит о том, что хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен

[81] Постановление Четвертого арбитражного апелляционного суда по делу № А78-19156/2017 от 4 мая 2018 г. // СПС Консультант Плюс: Судебная практика.

федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В соответствие со ст. 87 ТК РФ, работодатель обязан обеспечить такой порядок хранения персональных данных, который бы ограничивал несанкционированный доступ к ним. Все документы, содержащие персональные данные работников, прежде всего это личные дела, картотеки, учетные журналы необходимо хранить в рабочее и нерабочее время в специально оборудованных шкафах или сейфах, которые запираются и опечатываются. Трудовые книжки работников целесообразно хранить в сейфе отдельно от личных дел. В конце рабочего дня все личные дела должны сдаваться в отдел кадров.

Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети[82]. В таком случае доступ к персональным данным работников должен быть технически возможен только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы им для выполнения конкретных функций. Все документы по личному составу должны обязательно сдаваться в архив.

Исходя из положений Приказа Минкультуры РФ №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» от 25 августа 2010 г[83]., данные документы относятся к документам долговременного хранения и хранятся 75 лет или постоянно.

---

[82] Раудштейн А.В. Информационные отношения в сфере труда: понятие и характеристика // Российский юридический журнал. - 2010. - №6. - С. 154.

[83] Приказ Минкультуры РФ №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов,

В соответствии со ст. 89 ТК РФ в целях обеспечения защиты своих персональных данных, хранящихся у работодателя, работник обладает правом на:

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

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника;

- определение своих представителей для защиты своих персональных данных;

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

- требование об исключении или исправлении неверных или неполных персональных данных. При отказе работодателя исключить или исправить персональные данные работника последний имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

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

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

Соблюдение всех вышеизложенных требований должны обеспечивать совместными усилиями кадровая служба, юридическая служба, а в случае ведения автоматизированного учета кадров и специалисты по защите информации.

органов местного самоуправления и организаций, с указанием сроков хранения» от 25 августа 2010 г. (Зарегистрировано в Минюсте РФ 08.09.2010 №18380) // Бюллетень нормативных актов федеральных органов исполнительной власти. - 2011. - №38.

Условиям обработки персональных данных, посвящена ст. 6 Федерального закона №152-ФЗ. Так, обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) 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;

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

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

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом №210-ФЗ "Об организации предоставления государственных и муниципальных услуг" от 27 июля 2010 г[84]., включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

---

[84] Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 г. (ред. от 29.07.2018) // Собрание законодательства РФ. - 2010. - №31. - Ст. 4179.

5) 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;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях" от 3 июля 2016 г[85]., либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

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

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона №152-ФЗ, при условии обязательного обезличивания персональных данных;

---

[85] Федеральный закон №230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях» от 3 июля 2016 г. (ред. от 12.11.2018) // Собрание законодательства РФ. - 2016. - №27 (Часть I). - Ст. 4163.

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.1. Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом №57-ФЗ «О государственной охране» от 27 мая 1996 года[86].

Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются статьями 10, 11 Федерального закона «О защите персональных данных».

Определение состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, осуществляется на основе Постановления Правительства РФ №772 от 30 июня 2018 г[87]. Так, в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным био-

---

[86] Федеральный закон №57-ФЗ «О государственной охране» от 27 мая 1996 г. (ред. от 07.03.2018) // Собрание законодательства РФ. - 1996. - №22. - Ст. 2594.

[87] Постановление Правительства РФ №772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» от 30 июня 2018 г. // Собрание законодательства РФ. - 2018. - №28. - Ст. 4234.

метрическим персональным данным гражданина Российской Федерации, размещаются следующие сведения:

а) биометрические персональные данные физического лица - гражданина Российской Федерации следующих видов:

- данные изображения лица человека, полученные с помощью фото-видео устройств;

- данные голоса человека, полученные с помощью звукозаписывающих устройств;

б) идентификатор сведений в соответствующем регистре юридических лиц или регистре органов и организаций федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" государственного органа, банка, иной организации в случаях, определенных федеральными законами, разместивших в электронной форме в единой биометрической системе биометрические персональные данные гражданина Российской Федерации, - основной государственный регистрационный номер записи о создании юридического лица;

в) идентификатор сведений об уполномоченном сотруднике уполномоченной организации в регистре органов и организаций единой системы идентификации и аутентификации, разместившего в электронной форме в единой биометрической системе биометрические персональные данные гражданина Российской Федерации, - страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации;

г) идентификатор сведений о физическом лице в регистре физических лиц единой системы идентификации и аутентификации, биометрические персональные данные которого размещаются в единой биометрической системе, - идентификатор учетной записи в единой системе идентификации и аутен-

тификации.

В соответствие с п. 3 ст. 6 Федерального закона №152-ФЗ, оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом.

В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона о персональных данных.

Следует отметить, что лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных (п. 4 ст. 6 ФЗ РФ №152-ФЗ).

В случае, если оператор поручает обработку персональных данных другому лицу, то согласно п. 5 ст. 6 Федерального закона о персональных данных, ответственность перед субъектом персональных данных за действия указанного лица несет оператор, а лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность уже перед самим оператором.

Подводя итоги по данному параграфу выпускной квалификационной работы, мы вынуждены констатировать, наличие в действующем российском

законодательстве о персональных данных чрезмерно большого количества принципов, содержание и смысл которых дублируют друг друга или носят сугубо формальный характер. Так, например, в целях оптимизации можно объединить основополагающие начала о том, что обработке подлежат только персональные данные, которые отвечают целям их обработки, а содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, а также положение о том, что обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки, в один принцип, назвав его: «принципом минимизации персональных данных». Что касается условий обработки персональных данных, то они достаточно подробно расписаны в ст. 6 Федерального закона №152-ФЗ о персональных данных и достаточно эффективно реализуются на практике. Следует отметить, что при обработке персональных данных должно учитываться основное свойство таких данных не подлежать огласке (конфиденциальность) о чем и пойдет речь в следующем параграфе.

1.3. Конфиденциальность персональных данных и особенности их обработки

Конфиденциальность персональных данных из смысла диспозиции ст. 7 Федерального закона о персональных данных представляет собой обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Применительно к такой правовой категории, как персональные данные, проблема конфиденциальности приобретает совершенно особое значение. Не будет преувеличением сказать, что проблема обеспечения конфиденциальности персональных данных является одной из важнейших теоретических и практических проблем, подлежащих разрешению специалистами в области

права и информационной безопасности. Согласно данным, приведенным журналом «Управление персоналом», одним из наиболее востребованных видов инсайдерской информации в настоящее время являются персональные данные сотрудников компаний[88].

Комплексное решение правового обеспечения конфиденциальности персональных данных должно учитывать двоякую природу этого понятия. С одной стороны, персональные данные являются составной частью понятия «частная жизнь» индивида, а неприкосновенность частной жизни, как известно, охраняется законом. С другой стороны, персональные данные есть необходимый элемент социализации индивида. Они представляют собой его своеобразную «визитную карточку» в обществе и являются юридической основой для реализации его право- и дееспособности, поэтому не всегда могут и должны быть конфиденциальными[89].

В силу вышеназванных причин правовое регулирование обеспечения конфиденциальности персональных данных должно развиваться в четырех основных направлениях:

Первое направление, самое общее, связано с защитой конфиденциальности персональных данных в процессе социальной жизни индивида (взаимоотношения с государственными органами, профессиональная деятельность, брачно-семейные отношения, финансовая сфера, здравоохранение и медицина, получение нотариальных, адвокатских услуг и т.п.), т.е. с обработкой персональных данных операторами информационных систем персональных данных.

Второе направление связано с обеспечением конфиденциальности персональных данных личности в условиях свободы СМИ.

Третье направление - это правовые изъятия из общего режима конфиденциальности персональных данных, действующие во время избирательных

---

[88] Инсайдер - вариант с заклеиванием usb-порта не поможет: Интервью с Е. Преображенским // Управление персоналом. - 2009. - № 7. - С.27.

[89] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие. - М.: Статус, 2011. - С.15.

кампаний и в иных случаях.

Четвертое направление связано с обеспечением конфиденциальности персональных данных, при исполнении запросов социально-правового характера.

Рассмотрим подробнее каждое из этих направлений, пересекающееся с темой нашей выпускной квалификационной работы.

Каждый из нас постоянно использует свои персональные данные для реализации своих прав, исполнения обязанностей, получения гарантий и т.п. В данном случае персональные данные служат инструментом социализации, и раскрытие их конфиденциальности необходимо человеку для реализации его право- и дееспособности. Обеспечивать конфиденциальность персональных данных, добровольно и в собственных интересах раскрытых субъектом, обязаны операторы персональных данных. Согласно ст. 3 Закона о персональных оператором признается любой субъект, осуществляющий сбор и обработку персональных данных с определенной целью, но (как правило) не для личных или семейных нужд. Ситуации, связанные с предоставлением своих персональных данных разнообразны. Так, например, реализуя свое право на труд, гражданин предоставляет целый ряд документов, содержащих его персональные данные: сведения об образовании, квалификации, прошлой профессиональной деятельности и доходах, а также о месте жительства, семейном положении и т.д. Помимо этого лицо обязано представить оператору-работодателю данные о состоянии своего здоровья. Получая значительный объем различных сведений о потенциальном работнике, кадровая служба организации, являющаяся по смыслу закона оператором, обязана обеспечить их конфиденциальность.

Также, любой гражданин, взаимодействуя с различными государственными и общественными организациями, постоянно представляет им свои персональные данные. Соответственно, огромные массивы персональных данных накапливаются у многочисленных операторов. Нарушение оператором режима конфиденциальности может нанести субъекту персональных

данных моральный и материальный ущерб, поэтому эффективное обеспечение конфиденциальности персональных данных операторами - один из важнейших элементов механизма защиты персональных данных, имеющих огромное практическое значение. Ведь именно то, насколько хорошо будут защищены персональные данные граждан в процессе их обработки органами государственной власти, во многом определит общую степень защиты персональных данных в России. Но, несмотря на то что отечественное законодательство в области защиты персональных данных постоянно пополняется, практика показывает его абсолютную неэффективность при сложившейся системе общественных отношений в стране и в мире. Так, на черном рынке по прежнему продаются базы данных налогоплательщиков (с указанием доходов и объектов налогообложения), абонентов сотовых сетей (с указанием телефонных номеров), водительских удостоверений и т.д. Для исследования общественной опасности утечки персональных данных из автоматизированных информационных систем в сфере государственного управления рассмотрим два возможных последствия таких утечек. Первое из них - предложение баз данных на черном рынке - представляет собой достаточно известное и широко обсуждаемое явление. Общественная опасность обусловливается массовостью нарушений прав человека, поскольку пострадавшим является каждый, сведения о ком были преданы огласке. Но более серьезную опасность представляет, на наш взгляд, второй вариант преступного деяния, связанного с нарушением конфиденциальности персональных данных. Он связан с тенденцией интеграции государственных АИС и слияния государственных баз данных[90].

Следует отметить, что проблема обеспечения конфиденциальности персональных данных тесно связана с другой, весьма сложной проблемой так называемого рутинного (или вторичного) использования персональных данных. Так, термин «Рутинное использование», впервые появился в США, и

[90] Амелин Р.В. О правовых принципах разработки государственных АИС, обрабатывающих персональные данные // Информационное право. - 2009. - №2. - С.33.

трактовался как исключение из общих правил обеспечения режима конфиденциальности персональных данных, что создавало широкие возможности для обмена персональной информацией между различными государственными ведомствами. Эта оговорка разрешала ведомствам использовать персональные данные и раскрывать их для целей, совместимых (но не обязательно совпадающих) с той целью, для которой была собрана информация[91].

Следует сказать о технических мерах, используемых для защиты персональных данных в информационных системах. В ст. 19 Закона о персональных данных устанавливается обязанность операторов при обработке персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Следует отметить, что основным недостатком любой, даже самой технически совершенной информационной системы, является профессионализм и ответственность обслуживающего ее персонала. Как отмечается специалистами по информационной безопасности, человеческий фактор должен учитываться и являться основным элементом построения эффективной системы защиты автоматизированных информационных систем[92].

Общие требования относительно правил работы с персональными данными работников операторов - юридических лиц устанавливаются подзаконными актами, например, утвержденным Постановлением Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г[93].

---

[91] Петросян М.Е. Защита персональных данных. Американская модель // США - Канада. - 2000. - № 6. - С 93.

[92] Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. - М., 2001. - С. 42.

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

Для регламентации особенностей трудовой функции работников, в чью компетенцию входит работа с персональными данными, можно использовать трудовой договор (а также различные соглашения) с этими работниками и другие локальные нормативные акты организации. Принимая на работу работников, в чью компетенцию будет входить работа с персональными данными, необходимо вносить в их трудовые договоры пункты о порядке работы с персональными данными, о соблюдении требований конфиденциальности, о прохождении работником соответствующего обучения и т.д. Работники должны быть ознакомлены под роспись со всеми должностными инструкциями и правилами, касающимися работы с конфиденциальными данными. Работодатель обязан проводить обучение и регулярный инструктаж этих работников по работе с автоматизированной информационной системой. В правилах внутреннего трудового распорядка или ином локальном нормативном акте (лучше всего - в специальном положении о персональных данных) должен быть закреплен порядок доступа сотрудников к конфиденциальным сведениям, порядок работы с ними и режим охраны этих сведений.

Словом, в локальном нормативном регулировании, касающемся прав и обязанностей, как работника, так и работодателя, должен быть закреплен весь спектр мер, направленных на предупреждение возможности несанкционированного доступа, использования и разглашения персональных данных, а также дифференцированная система мер ответственности за нарушение конфиденциальности персональных данных.

Сбор и обработка персональных данных в СМИ имеют свои особенности, связанные как с обеспечением конфиденциальности, так и, напротив, с изъятиями из общих правил о соблюдении конфиденциальности. Следует также отметить, что в Законе о СМИ и в Законе о персональных данных имеются концептуальные различия в трактовке защиты информации личного характера. В частности, в Законе о СМИ есть нормы, регулирующие распространение материалов и сообщений, сделанных с использованием скрытой аудио-, видеозаписи, кино- и фотосъемки. На наш взгляд, такое распростра-

нение противоречит правилам о соблюдении конфиденциальности.

Несколько иначе обстоит дело с обеспечением конфиденциальности персональных данных во время проведения избирательных компаний. На это время установлены правовые изъятия из общего режима конфиденциальности персональных данных, действующие на все время избирательной кампании. Так, например, в процессе выдвижения кандидата в депутаты законодательных органов, такое лицо обязано сообщить о себе следующие сведения: фамилия, имя, отчество; дата и место рождения; адрес места жительства; серия, номер и дата выдачи паспорта или документа, заменяющего паспорт; гражданство; образование; основное место работы или службы; занимаемая должность. Такое лицо также вправе указать свою принадлежность к той или иной политической партии или иному общественному объединению. В случае наличия у кандидата иностранного гражданства указываются сведения о его приобретении. В случае наличия у кандидата неснятой и непогашенной судимости указываются сведения о судимости. Кроме того, в избирательную комиссию кандидат обязан представить сведения о размере и источниках доходов, о принадлежащем ему имуществе, в том числе денежных вкладах и ценных бумагах. Как видим, вся информация о кандидате, которая должна предоставляться во время выборов, обнародуется с целью оценки кандидата избирателями и обеспечения гласности и открытости избирательного процесса и не является нарушением конфиденциальности персональных данных.

Постоянный рост запросов социально-правового характера, поступающих в государственные архивы, обусловлен увеличением объема документов по личному составу, поступивших на хранение в государственные архивы от ликвидированных и реорганизованных организаций и предприятий, а также внесением в этот период многих изменений и дополнений в нормы действующего законодательства по вопросам социального обеспечения и возникшей необходимостью представления в органы социального обеспечения дополнительных справок, подтверждающих право гражданина на те или иные социальные льготы и компенсации. Тематика запросов социально-правового ха-

рактера, исполняемых государственными архивами, охватывает вопросы: о гражданском состоянии, подтверждении трудового стажа, размерах заработной платы, прохождении службы в Вооруженных силах, несчастных случаях на производстве, награждении государственными и ведомственными наградами, присвоении почетных званий, получении образования, опекунстве, патронировании, о подтверждении имущественных и других прав. К группе запросов социально-правового характера относятся исключительно те запросы по названной тематике, исполнение которых предусматривает подтверждение данных, необходимых для получения гражданином государственных социальных льгот. Информация, необходимая для исполнения запросов социально-правового характера, содержится в документах официального происхождения, образовавшихся в процессе документирования жизнедеятельности человека как гражданина общества. В их числе: акты гражданского состояния, дипломы и свидетельства об образовании, многочисленные виды документов, отражающие сведения о трудовой деятельности, состоянии здоровья, военной службе, местах проживания, официальных заслугах перед обществом и государством, другие факты биографии человека, которые определяют его право на соответствующее государственное социальное обеспечение.

Часть этой информации является конфиденциальной и относится к информации ограниченного доступа. Согласно ФЗ «Об архивном деле в Российской Федерации» «ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов». После окончания 75 лет дела и документы, содержащие такую информацию, становятся общедоступными, за исключением дел и документов личного происхождения, переданных в архив на особых условиях доступа к ним. Собственник имеет право установить свои сроки ограничения и условия доступа.

Правом получить конфиденциальные персональные данные обладает

субъект персональных данных (человек, информация о котором содержится в документе), если это не противоречит законодательству Российской Федерации (например, законам «, «Об оперативно-розыскной деятельности», «Об органах Федеральной службы безопасности в Российской Федерации» и т.п.), после смерти субъекта персональных данных - его наследники (при наличии свидетельства о смерти субъекта информации); доверенные лица субъекта персональных данных, его наследников (при наличии нотариально заверенных доверенностей).

Правом получить конфиденциальные персональные данные в качестве ответа на официальный мотивированный письменный запрос, в котором указываются цель получения информации и форма ее использования (например, «информация будет использована для подготовки справочно-информационного издания в обезличенном виде» или «в связи с заведением уголовного дела»), обладают также сотрудники организаций-фондообразователей и их правопреемников; органов государственной власти, государственных органов и организаций, органов местного самоуправления; судов, органов прокуратуры, органов предварительного следствия, органов дознания (по делам, находящимся в их производстве) в пределах исполнения ими своих служебных обязанностей.

Подводя итоги по первой главе выпускной квалификационной работы, отметим, что в действующем российском законодательстве термин «персональные данные» определяется как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Такое содержание позволяет достаточно широко трактовать исследуемое понятие.

В отечественной науке систематизация и классификация всех персональных данных возможна по различным признакам и критериям. На наш взгляд, наиболее оптимальным, является применение отраслевого критерия для классификации всех персональных данных, обрабатываемых в соответствие с целями деятельности той или иной конкретной организации.

Обработка персональных данных осуществляется на основе многочисленных основополагающих принципов, содержание и смысл которых дублируют друг друга или носят сугубо формальный характер. Условий обработки персональных данных, нашли свое законодательное закрепление в ст. 6 Федерального закона №152-ФЗ о персональных данных и достаточно эффективно реализуются на практике.

Конфиденциальность персональных данных представляет собой обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания. Оператору персональных данных следует обеспечить конфиденциальность информации не только своей организации, но и те персональные данные, которые доверили организации клиенты, посредники, представители и партнёры.

ГЛАВА 2.
ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ООО «ТИТОВСКИЙ КИРПИЧНЫЙ ЗАВОД»

2.1. Меры по обеспечению безопасности персональных данных при их обработке в обществе

В соответствии с пп. 13-15 Постановления Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г[94]., к мерам по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации, относятся:

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

- необходимость обеспечения раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

---

[94] Постановление Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. // Собрание законодательства РФ. - 2008. - №38. - Ст. 4320.

- необходимость соблюдения при хранении материальных носителей условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Являясь оператором, ООО «Титовский кирпичный завод» вправе осуществлять - без уведомления уполномоченного органа по защите прав субъектов персональных данных - обработку персональных данных, обрабатываемых в соответствии с трудовым законодательством (ст. 22 Федерального закона «О персональных данных»).

Следует отметить, что в коллективном договоре, правилах внутреннего трудового распорядка ООО «Титовский кирпичный завод» закрепляются и дополнительные меры защиты персональных данных работников, вырабатываемые совместно работодателем, работниками и их представителем. К ним относятся:

1) меры защиты, применяемые работодателем и выборным органом первичной профсоюзной организации, когда работодатель решает вопрос с учетом мотивированного мнения этого органа;

2) меры защиты, используемые комиссией по трудовым спорам при рассмотрении индивидуального трудового спора работника;

3) запрет хранения определенной информации о работниках на компьютерах, к которым имеется свободный доступ.

Методы и способы защиты информации в информационных системах персональных данных ООО «Титовский кирпичный завод» осуществляются на основании положений Приказа ФСТЭК России №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г[95].

[95] Приказ ФСТЭК России №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке

Меры по обеспечению безопасности персональных данных, реализуемые ООО «Титовский кирпичный завод» в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации № 1119 от 1 ноября 2012 г[96]., и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

в информационных системах персональных данных» от 18 февраля 2013 г. (Зарегистрировано в Минюсте России 14.05.2013 №28375) (ред. от 23.03.2017) // Российская газета. - 2013. - 22 мая.

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

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

По результатам анализа исходных данных и модели определения угроз исходящих от НДВ в ПО ИСПДн, ИСПДн «Сотрудники» в ООО «Титовский кирпичный завод» присвоен 4 уровень защищенности, который нашел свое отражение в Акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных (Приложение 1).

Рассмотрим нормативные требования для всех уровней защищенности. Так, необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных дан-

ных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе. В ООО «Титовский кирпичный завод» такие полномочия возложены на начальника отдела кадров.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах ООО «Титовский кирпичный завод» доступ к содержанию электронного журнала сообщений возможен только начальнику отдела кадров общества.

В целях обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах ООО «Титовский кирпичный завод» выполняются следующие требования: автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника общества по доступу к персональным данным, содержащимся в информационной системе; назначен ответственный за обеспечение безопасности персональных данных в информационной системе.

Контроль за выполнением настоящих требований в ООО «Титовский кирпичный завод» организуется и проводится руководителем общества самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль в Обществе проводится не реже 1 раза в 3 года в сроки, определяемые руководителем Общества.

Примечателен тот факт, что определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится

руководителем Общества с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных». Оперируя термином вред, законодатель, к сожалению, не указывает его вид, что, на наш взгляд, является явным упущением, позволяющим трактовать данное понятие достаточно широко. Не секрет, что в современной научной доктрине термин «вред» имеет самое разнообразное определение. Так, например, С.А. Степанов считает, что: «Под вредом понимаются неблагоприятные для потерпевшего имущественные и неимущественные последствия»[97]. П.В. Крашенинников предлагает рассматривать вред как всякое умаление охраняемого законом материального или нематериального блага, любые неблагоприятные изменения в охраняемом законом благе, которое может быть как имущественным, так и неимущественным (нематериальным).

Действительно, в науке уже на протяжении длительного времени господствует точка зрения, что вред - это «родовое понятие отрицательных имущественных последствий правонарушения»[98]. В специальной литературе выделяют следующие виды вреда: материальный, моральный и вред здоровью[99]. Очевидно, что в данном случае идет речь исключительно об одном виде вреда - моральном. Об этом свидетельствует и сложившаяся судебная практика.

Так, например, по одному из судебных дел Переславский районный суд Ярославской области указал, что сам факт нарушения законных прав субъекта персональных данных компенсируется денежной компенсацией и с учетом

---

[97] Алексеев С.С., Васильев А.С., Голофаев В.В., Гонгало Б.М. и др. Комментарий к Гражданскому кодексу РФ (учебно-практический). Части первая, вторая, третья, четвертая. 2-е изд., перераб. и доп. / Под ред. С.А. Степанова. - М.: Проспект 2009. - С. 943.

[98] Смирнов В.Т., Собчак А.А. Общее учение о деликтных обязательствах в советском гражданском праве. - Л.: Изд-во Ленинградского государственного университета, 1983. - С. 59.

[99] Малиновский А.А. Вред как юридическая категория // Юрист. - 2006. - №2. - С. 222.

принципа разумности справедливости, определил размер денежной компенсации морального вреда, подлежащий взысканию в пользу истца[100]. Возмещение морального вреда за нарушение законодательства о персональных данных являлось предметом судебных разбирательств и по многим другим делам[101].

Однако, в соответствие с ст. 1101 ГК РФ[102], размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда и ни как уж не может оцениваться оператором персональных данных. В этой связи, считаем целесообразным, внести соответствующие изменения и дополнения как в подп. 5 п. 1 ст. 18.1 Закона о защите персональных данных, так и в п. 7 Постановления Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г., заменив в них термин «оценка» понятием «предупреждение» и дополнив указанием на конкретный вид причиненного вреда, изложив их в следующей редакции:

«Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными право-

---

[100] Решение Переславского районного суда Ярославской области по делу № 2-668/2017 от 11 мая 2017 г. // СПС Консультант Плюс: Судебная практика.

[101] Решение Химкинского городского суда Московской областипо делу № 2-6262/2017 от 9 февраля 2018 г. // СПС Консультант Плюс: Судебная практика; Решение Бугульминского городского суда Республики Татарстан по делу № 2-1654/2017 от 10 октября 2017 г. // СПС Консультант Плюс: Судебная практика; Решение Калининского районного суда г. Уфа Республики Башкортостан по делу № 2-3678/2017 от 5 сентября 2017 г. // СПС Консультант Плюс: Судебная практика; Решение Калининского районного суда города Санкт-Петербургапо делу № 2-3317/2017 от 24 августа 2017 г. // СПС Консультант Плюс: Судебная практика; и др.

[102] Гражданский кодекс Российской Федерации (часть вторая) (в ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 01.09.2018) // Собрание Законодательства Российской Федерации. - 1996. - № 5. - Ст. 410.

выми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

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

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

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

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) предупреждение морального вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к

защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных».

«7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом предупреждения возможного морального вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

Внесение таких изменений, на наш взгляд, будет способствовать наиболее эффективной регламентации мер, направленных на обеспечение выполнения оператором обязанностей, по защите персональных данных в информационных системах.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

- регистрация событий безопасности;

- антивирусная защита;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание конкретных мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, в ООО «Титовский кирпичный завод» приведены в Приложении 2.

Конкретные меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

В свою очередь, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры, направленные на защиту машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных ООО «Титовский кирпичный завод», включает:

- определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

- уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

- дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими

выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных ООО «Титовский кирпичный завод». В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

Подводя итоги по данному параграфу выпускной квалификационной работы, отметим, что в ООО «Титовский кирпичный завод» используются основные и дополнительные меры по обеспечению безопасности персональных данных, причем их применение напрямую зависит от того, осуществляется ли такая обработка с использованием или без использования средств автоматизации.

2.2. Документирование процедуры защиты персональных данных работников общества

Для обеспечения конфиденциальности сведений в организации ООО «Титовский кирпичный завод» имеются локальные документы, регламентирующие защиту персональных данных работников общества.

Всю документацию Общества, которая относится к защите персональных данных, условно можно разделить на 3 группы: организационную, технологическую и методическую.

Организационная документация определяет задачи, функции и объем ответственности сотрудников, которые проверяют и отвечают за сбор, обра-

ботку и сохранность конфиденциальных сведений работников в Обществе. К данной группе можно отнести: инструкции; положение; уведомления, приказы (о допуске сотрудников к работе с ПД).

Положения технологической документации определяют порядок и способы реализации обеспечения защиты персональных данных в Обществе. Сюда можно отнести различного рода перечни.

Методическая документация детализирует процессы обработки, порядок и правила работы с персональными данными в Обществе.

Охарактеризуем все имеющиеся в ООО «Титовский кирпичный завод» документы, посвященные защите персональных данных работников Общества. Так, все персональные данные подлежащие защите в информационных системах Общества в соответствие с требованиями установленными ФЗ № 152 «О персональных данных» от 27.06.2006 г., отражены в Перечне персональных данных, подлежащих защите в информационных системах ООО «Титовский кирпичный завод» (Приложение 3).

В данном обществе на основании Приказа о назначении ответственных сотрудников за организацию обработки персональных данных и перечне мер по их защите (Приложение 4) назначено лицо, осуществляющее возложенные на него обязанности по хранению и защите персональных работников. Исполнение таких обязанностей возложено на Начальника отдела кадров Общества.

В соответствие с ФЗ «О персональных данных» и Указом Президента РФ № 188 от 6 марта 1997 г., в ООО «Титовский кирпичный завод» разработан список конфиденциальных сведений.

В данный список входят:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Приказом №56 Директора «О выделении помещений для обработки персональных данных» установлен список помещений ООО «Титовский кирпичный завод», где проводится обработка персональных данных (Приложение 5).

Для обеспечения доступа работников в помещения предусматривается комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности Общества. Указанные меры организуются лицом, ответственным за организацию обработки персональных данных.

Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где ведется обработка персональных данных с использованием средств автоматизации или без использования таковых. Для помещений, в которых обрабатываются персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носите-

лей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Доступ работников Общества в помещения осуществляется в соответствии со списком работников, имеющих право самостоятельного доступа в помещения, в которых ведется обработка персональных данных (далее - Список). Список готовится и уточняется лицом, ответственным за организацию обработки персональных данных, и утверждается директором Общества. Доступ в помещения иных лиц осуществляется работниками Общества, указанными в Списке. Пребывание посторонних лиц в помещениях допускается только в присутствии вышеуказанных работников Общества на время, ограниченное необходимостью решения вопросов, связанных с осуществлением полномочий в рамках договоров, заключенных с Обществом, обслуживания компьютерной техники и оргтехники. Внутренний контроль за соблюдением порядка доступа в помещения проводится лицом, ответственным за организацию обработки персональных данных или комиссией, список которой утверждается приказом директора Общества.

В целях обеспечения защиты персональных данных, обрабатываемых в информационной системе персональных данных ООО «Титовский кирпичный завод» Приказом «Об утверждении мест хранения персональных данных», в Обществе определены места для хранения материальных носителей персональных данных (Приложение 6).

Каждый сотрудник Общества, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, несёт персональную ответственность за свои действия при работе с информационными ресурсами, содержащими персональные данные. Обязанности пользователя информационной системы персональных данных прописаны в Инструкции пользователей системы персональных данных.

В ООО «Титовский кирпичный завод» инструкция пользователя информационной системы персональных данных (ИСПДн) определяет долж-

ностные обязанности всех пользователей. Пользователь информационной системы персональных данных осуществляет обработку персональных данных в ИСПДн. Пользователем является каждый сотрудник Общества, участвующий в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Документ состоит из разделов: общие положения, должностные обязанности и организация парольной защиты, правила работы в сетях общего доступа и (или) международного обмена (при необходимости).

Основные должностные обязанности пользователя ИСПДн следующие:

Знать и выполнять требования действующих нормативных документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него в положении о разграничении прав доступа к обрабатываемым персональным данным.

Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

Соблюдать требования парольной политики.

Соблюдать правила при работе в сетях общего доступа и (или) международного обмена (Интернет и т.п.).

Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

Обо всех выявленных нарушениях, связанных с информационной безопасностью оператора, а также для получений консультаций по вопросам информационной безопасности, обращаться к лицу, ответственному за обеспечение информационной безопасности ИСПДн.

Для получения консультаций по вопросам работы и настройке элементов ИСПДн обращаться к администратору ИСПДн.

Пользователям Общества запрещается: разглашать защищаемую информацию третьим лицам, копировать защищаемую информацию на внешние носители без разрешения своего руководителя, самостоятельно устанавливать программное обеспечение.

В инструкции пользователя информационной системы персональных данных указано, что:

- личные пароли доступа к элементам ИСПДн выдаются пользователям администратором информационной безопасности, администратором ИСПДн или создаются самостоятельно;

- полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца;

- при формировании пароля, его ввода и хранения необходимо придерживаться утвержденных правил;

- лица, использующие паролирование, обязаны четко знать и строго выполнять требования инструкции и других руководящих документов по паролированию, а также своевременно сообщать администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Персональные данные хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению. Для этого существует следующий порядок действий:

Носители, в которых содержится персональная информация, подлежат уничтожению, согласно утверждённому приказу руководителя организации. Занимается уничтожением специальная комиссия.

Распространители, содержащие ПД, удаляются в срок, который не превышает 30 дней с момента достижения цели обработки личных данных или утраты необходимости в их достижении.

Комиссия выполняет отбор машинопечатных и бумажных носителей ПД, которые подлежат удалению.

На отобранные к уничтожению распространители составляется акт. В акте исправления не допускаются.

Комиссия выполняет проверку всех носителей, занесенных в акт.

По окончании сверки в акт подписывают всех членом комиссии, а затем его утверждает руководитель организации.

Распространители ПД, подлежащие удалению и включённые акт, после сверки комиссией складывают в нужное место и опечатывают.

Персональные данные могут быть уничтожены любым способом, который не позволит провести их дальнейшую обработку.

В ООО «Титовский кирпичный завод» удаление носителей, содержащих личные данные, происходит под контролем специальной Комиссии. Она создаётся приказом руководителя организации (Приложение 7). Во время манипуляции составляется акт об уничтожении ПД. После составления акта в течение 3-х дней направляются на утверждение руководителю организации.

Факт удаления носителя с персональными данными заносится в «Журнал регистрации носителей информации, содержащих ПД и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения» вносятся соответствующие данные. Этот журнал является конфиденциальной документацией и вместе с актами уничтожения его хранят в сейфе.

Когда срок хранения документации подошёл к концу, то удаление происходит методом измельчения на мелкие части или же другим способом, исключающим возможность дальнейшего восстановления информации. Бумажные носители могут сжигаться.

По завершении указанных сроков хранения машинные носители ПД, подлежащие уничтожению, физически удаляются с целью невозможности восстановления и последующего использования. Достичь это можно путем деформирования, нарушения единой целостности носителя и его сжигания. Файлы, подлежащие уничтожению и находящиеся на жёстком диске компь-

ютера, удаляют средствами операционной системы с дальнейшим очищением корзины.

В организации определяется узкий круг лиц, которые имеют право работать с конфиденциальной информацией для выполнения своих служебных обязанностей. Они назначаются специальным приказом (Приложение 8).

Приказ представляет собой правовой акт, который относится ко всему предприятию, определяет его деятельность и решает его основные задачи. Он издается единолично руководителем фирмы.

В перечень таких лиц могут войти руководитель, его заместители, работники отдела кадров, сотрудники бухгалтерии, служба безопасности, секретарь и иные работники, которым эти сведения нужны для выполнения трудовых обязанностей.

Доступ может быть и к информации, предоставленной клиентами организации или другими лицами. Все это требует отдельного уточнения при составлении документа.

Если допуск понадобится лицам, не обозначенным в приказе, для них издается отдельный документ. Допуск регистрируется в журнале.

Каждое лицо, осуществляющее свою трудовую деятельность в Обществе или вступающее с ним в гражданско-правовые или иные отношения принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе (ст. 9 ФЗ РФ «О персональных данных»). Такое согласие должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Согласие субъекта является комплексной категорией, при оценке которой необходимо учитывать: наличие свободы принятия субъектом решения; наличие собственной воли субъекта, т.е. отсутствие какого-либо давления на него со стороны; наличие интереса субъекта в связи передачей для возмож-

ной обработки собственных персональных данных. Комментируя данную норму, российские авторы, как правило, акцентируют внимание на гражданско-правовом принципе автономии воли. Последний подразумевает свободное и самостоятельное принятие решения, основанного исключительно на внутреннем убеждении субъекта, определяющего характер и содержание собственных действий. Одним из основных международных документов в данной области, который позволяет сравнить подходы при определении наличия/отсутствия согласия, является Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц в отношении обработки персональных данных и свободного обращения таких данных. Анализ положений, закрепленных в Директиве 95/46/ЕС, позволяет выявить несколько критериев для оценки свободы принятия решения субъектом. В соответствии со ст. 2 Директивы 95/46/ЕС "согласие субъекта данных означает любое свободно данное конкретное и сознательное указание на его желания, которым субъект данных выражает свое согласие на обработку относящихся к нему персональных данных". В соответствии со ст. 7 Директивы 95/46/ЕС согласие квалифицируется как однозначно данное согласие. В соответствии со ст. 8 Директивы 95/46/ЕС имеет место определение согласия как явно выраженное согласие на обработку. В соответствии со ст. 26 Директивы 95/46/ЕС передача персональных данных в третью страну может совершаться при условии, что субъект данных однозначно дал свое согласие на предполагаемую передачу данных.

Современные представления о защите персональных данных в Европе необходимо соотносить с последними из принятых документов. Одним из таких является Резолюция Европейского парламента от 06.07.2011 о комплексном подходе к защите персональных данных в Европейском союзе (2011/2025 (INI)). В ней отражаются основные тенденции, которые могут повлиять на отношения по поводу персональных данных в России. Документом провозглашается преемственность основных принципов Директивы 95/46/ЕС. Наличие разных подходов в государствах - членах ЕС не снимает

обязанности ЕС обеспечить неприкосновенность частной жизни в отношении любой обработки персональных данных физических лиц в пределах и за пределами ЕС при любых обстоятельствах в современных условиях, вызванных глобализацией, в целях решения многочисленных задач. Особенно подчеркивается необходимость защиты данных в связи с расширением деятельности в Интернете.

В документе подчеркнуто, что право на свободу выражения мнения и информации и принцип прозрачности должны быть полностью учтены при обеспечении фундаментального права на защиту персональных данных. Далее отмечается необходимость комплексного подхода по защите персональных данных во всех областях, в которых обрабатываются персональные данные, в том числе в области полицейского и судебного сотрудничества по уголовным делам, области общей внешней политики и политики безопасности без ущерба для конкретных правил. Европейский парламент призывает Европейскую комиссию убедиться в том, что текущий пересмотр законодательства ЕС о защите данных будет предусматривать: полное согласование на самом высоком уровне предоставления правовой определенности и единого высокого стандарта уровня защиты людей в любых обстоятельствах; оценку воздействия и тщательный учет затрат; укрепление существующих принципов и элементов, таких как прозрачность данных, минимизация и цели ограничения, наличие предварительного и явного согласия, данные о нарушениях прав и уведомление субъектов, особенно в отношении глобальной онлайновой среды; подчеркивается, что согласие должно считаться действительным только тогда, когда имеется однозначное сообщение, свободное, конкретное и четкое; когда имеется адекватный реализованный механизм для фиксации согласия или отзыва согласия пользователя[103].

Следует отметить, что универсального бланка такого документа не существует. Поэтому каждый оператор может самостоятельно его разработать

[103] Personal data protection in the European Union. European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025 (INI)) // Official Journal C 033 E, 05.02.2013. - P. 0101 - 0110.

или использовать предложенные образцы, подготовленные специалистами Консультант Плюс.

В соответствие с п. 4 ст. 9 Закона «О персональных данных», согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

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

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

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

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

В ООО «Титовский кирпичный завод» разработана типовая форма Согласия на обработку персональных данных. Данное Согласие дает право Обществу хранить и обрабатывать следующие персональные данные:

- фамилия, имя, отчество;

- год, месяц, дата и место рождения;

- свидетельство о гражданстве;

- реквизиты документа, удостоверяющего личность;

- идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты свидетельства постановки на учет в налоговом органе;

- номер свидетельства обязательного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования;

- номер полиса обязательного медицинского страхования;

- адрес фактического места проживания и регистрации по месту жительства и (или) по месту пребывания;

- почтовый и электронный адреса;

- номера телефонов;

- фотографии;

- сведения об образовании, профессии, специальности и квалификации, реквизиты документов об образовании;

- сведения о семейном положении и составе семьи;

- сведения об имущественном положении, доходах, задолженности;

- сведения о занимаемых ранее должностях и стаже работы, воинской обязанности, воинском учете.

В делопроизводстве Общества предусмотрен вариант предоставления согласия субъектом персональных данных на обработку его персональных в форме электронного документа. Данная процедура предусмотрена Федеральным законом №210-ФЗ «Об организации предоставления государственных и

муниципальных услуг» от 27 июля 2010 г[104]. Во исполнение ст. 21.2 данного Федерального закона Правительством Российской Федерации утверждены Правила использования простых электронных подписей при оказании государственных и муниципальных услуг. В соответствии с Постановлением Правительства РФ №33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» от 25 января 2013 г[105]. субъект персональных данных должен указать фамилию, имя и отчество (если имеется), страховой номер индивидуального лицевого счета, а также дать согласие заявителя на обработку его персональных данных. Оператор, выдавая ключ, обязан установить личность заявителя. Таким образом, согласие в форме электронного документа предусматривает наличие простой электронной подписи и минимального количества персональных данных, необходимых для идентификации субъекта.

В случае если на работу в ООО «Титовский кирпичный завод» принимается лицо, не достигшее возраста 18-лет согласие на обработку его персональных данных дает законный представитель субъекта персональных данных. Для лиц, ограничено дееспособных по медицинским показаниям, представителями могут выступать также должностные лица медицинского учреждения. В иных случаях представитель субъекта персональных данных может осуществлять свою деятельность только при наличии доверенности. Требования к форме и содержанию доверенности наиболее полно разработаны в действующем российском гражданском законодательстве (гл. 10 ГК РФ). Доверенность, выданная представителю, должна содержать:

- конкретное указание о том, кому она предоставлена в каких целях и на какой срок;

---

[104] Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 г. (ред. от 29.07.2018) // Собрание законодательства РФ. - 2010. - №31. - Ст. 4179.

[105] Постановление Правительства РФ №33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (вместе с «Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг») от 25 января 2013 г. (ред. от 20.11.2018) // Собрание законодательства РФ. - 2013. - № 5. - Ст. 377.

- указание оператора, для каких целей дается согласие на обработку персональных данных;

- указание на то, что данное действие не противоречит интересам субъекта персональных данных;

- указание на то, что согласие на обработку персональных данных дается по воле субъекта персональных данных;

- а также, что представляется важным, причину, по которой выдана доверенность, т.е. почему субъект персональных данных дает согласие на обработку персональных данных через представителя, а не лично.

Вопрос о том, каким образом проверяются полномочия представителя субъекта персональных данных, решаются оператором в каждом конкретном случае самостоятельно. Оператор для данного случая должен иметь соответствующие положения, закрепленные в документе, который входит в систему документов, именуемую в целом "политика обработки персональных данных". Считаем, что для данного случая должна быть разработана специальная инструкция либо специальный раздел в инструкции, регулирующий данную группу общественных отношений. Разработке такой инструкции будет посвящен параграф следующей главы выпускной квалификационной работы.

На практике очень часто возникают вопросы о том можно ли дать Согласие на обработку персональных данных посредством направления СМС-сообщений. На сайте Роскомнадзора указывается, что: «получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений действующим законодательством Российской Федерации не установлено»[106]. Такое разъяснение в СМИ считаем не совсем верным. С одной стороны - да, получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений не предусмотрено действующим российским законодательством, но, с другой стороны прямо и не запрещено в нем. Даже, наоборот, п. 1 ст. 9 гласит о том, что: «согласие на обработку пер-

[106] Сайт Роскомнадзора - URL: https://rkn.gov.ru/treatments/p459/p468/ (Дата обращения: 19.10.2018).

сональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом». Анализируя работу в Обществе по получению такого Согласия от отдельных субъектов персональных данных (иногородних работников, контрагентов находящихся в других районах или областях), полагаем, что получение такого согласия посредством СМС-сообщений упростило бы такой порядок. Считаем, что назрела необходимость внесения соответствующих изменений в Федеральный закон «О персональных данных». В этой связи предлагается следующая формулировка п. 1 ст. 9 Федерального закона №152-ФЗ:

«1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом, в том числе посредством направления оператору СМС-сообщений. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором».

Следует отметить, что разрешительный порядок уведомления посредством направления СМС-сообщений довольно эффективно используется для извещения участников судопроизводства. В данной сфере разработан и применяется Регламент организации извещения участников судопроизводства посредством СМС-сообщений (утв. приказом Судебного департамента при Верховном Суде РФ №257 от 25 декабря 2013 г.). Полагаем, что аналогичный подход можно применить и к делопроизводству ООО «Титовский кирпичный завод» разработав Регламент «О получении согласия на обработ-

ку персональных данных посредством СМС-сообщений». Данный документ предположительно мог бы включать в себя следующие разделы:

1. Общие положения.

В данном разделе, устанавливались общие правила и порядок дачи согласия на обработку своих персональных данных посредством направления Оператору СМС-сообщений; определялись термины и понятия, используемые в данном Регламенте.

2. Обязательные условия Согласия, направляемого посредством СМС-сообщений.

В данном разделе указываются: перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональными данными, на совершение которых дается согласие.

3. Порядок подготовки, отправки, учета и хранения СМС-сообщений.

В данном разделе должны быть расписаны процедуры подготовки, отправки, учета и хранения СМС-сообщений, содержащих Согласие субъектов на обработку их персональных данных.

4. Заключительные положения.

Данный раздел посвящен сфере действия данного Регламента. Порядок вступления его в силу, механизм внесения в него изменений и дополнений.

Считаем, что разработка такого Регламента позволит значительно упростить работу Оператора при получении Согласия от субъектов персональных данных посредством СМС-сообщений.

Подводя итоги по второй главе выпускной квалификационной работы, мы пришли к выводу о том, что применение в ООО «Титовский кирпичный завод» той или иной меры по обеспечению безопасности персональных данных при их обработке зависит от того, осуществляется ли такая обработка с использованием или без использования средств автоматизации. Наряду с основными мерами, в Обществе закрепляются также дополнительные меры защиты персональных данных работников, вырабатываемые совместно работо-

дателем, работниками и их представителем. В частности, к таковым относятся: меры защиты, применяемые работодателем и выборным органом первичной профсоюзной организации, когда работодатель решает вопрос с учетом мотивированного мнения этого органа; меры защиты, используемые комиссией по трудовым спорам при рассмотрении индивидуального трудового спора работника; запрет хранения определенной информации о работниках на компьютерах, к которым имеется свободный доступ и др.

Для обеспечения конфиденциальности сведений в ООО «Титовский кирпичный завод» разработаны локальные документы, определяющие порядок защиты персональных данных работников Общества, перечень которых, можно условно разделить на три группы: организационные, технологические и методические. Следует отметить, что разработка каждого из документов, обеспечивающих защиту персональных данных в ООО «Титовский кирпичный завод» осуществляется в строгом соответствии с положениями Федерального закона РФ «О персональных данных». Несмотря на наличие в Обществе огромного массива документов, направленных на эффективную защиту персональных данных, многие из них нуждаются в совершенствовании, в связи с изменением действующего российского законодательства, регулирующего исследуемую область общественных отношений. Отдельные документы, такие как: Положение о защите персональных данных, Инструкции о порядке обработки персональных данных требуют их нормативной разработки. Именно о разработке данных документов и пойдет речь в следующей главе выпускной квалификационной работы.

ГЛАВА 3.
СОВЕРШЕНСТВОВАНИЕ РАБОТЫ С ДОКУМЕНТАМИ, РЕГЛАМЕНТИРУЮЩИМИ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «ТИТОВСКИЙ КИРПИЧНЫЙ ЗАВОД»

3.1. Разработка положения о защите персональных данных ООО «Титовский кирпичный завод»

В результате анализа всех локальных документов ООО «Титовский кирпичный завод», регламентирующих охрану персональных, было выявлено, что в данном Обществе отсутствует Положение о защите персональных данных. Считаем необходимым, восполнить этот пробел разработав такое Положение. Данный локальный акт должно иметь следующие реквизиты:

- наименование организации;
- наименование вида документа;
- дата и регистрационный номер документа;
- заголовок к тексту;
- гриф утверждения;
- текст;
- подпись;
- визы ознакомления.

Положение о защите персональных данных ООО «Титовский кирпичный завод» разрабатывается в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом № 149-ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г.; Федеральным законом № 152-ФЗ "О персональных данных" от 27 июля 2006 г., иными нормативными правовыми актами, действующими на территории Российской Федерации и определяет порядок сбора, обработки, хране-

ния, уничтожения, передачи и любого другого использования персональных данных в данной коммерческой организации.

Разработанное нами Положение о защите персональных данных ООО «Титовский кирпичный завод» (Приложение 9) имеет следующую структуру:

1. Общие положения;

2. Понятие и состав персональных данных;

3. Получение персональных данных;

4. Обработка и передача персональных данных;

5. Хранение персональных данных;

6. Уничтожение персональных данных;

7. Права работника по обеспечению защиты своих персональных данных;

8. Обязанности и ответственность работодателя за нарушение норм, регулирующих обработку и защиту персональных данных;

9. Заключительные положения.

Раздел «Общие положения» содержит информацию о назначении Положения и перечне нормативных правовых актов, в соответствии с которыми оно разработано.

Раздел «Понятие и состав персональных данных» включает в себя основные понятия, связанные с защитой персональных данных, объекты, относящиеся к персональным данным, а также перечень документов, содержащих информацию персонального характера работника.

Раздел «Получение персональных данных» регламентирует права и обязанности работника и работодателя, связанные с получением персональных данных.

Раздел «Обработка и передача персональных данных» включает в себя указание на цели, в которых производится обработка и передача персональных данных, условия допуска отдельных категорий лиц, которым персональные данные необходимы для выполнения конкретных трудовых функций, а также перечень требований, которые должен соблюдать работодатель при

передаче персональных данных работника. В качестве приложения к данному разделу приводятся: Список лиц, имеющих право доступа к персональным данным работников; Форма согласия на обработку персональных данных работника.

В разделе «Хранение персональных данных», определяется круг субъектов и помещения, в которых организуется хранение и использование персональных данных работников. Указываются требования к помещениям, в которых хранятся носители с персональными данными работников.

Раздел «Уничтожение персональных данных» регламентирует порядок уничтожения таких данных.

В разделе «Права работника по обеспечению защиты своих персональных данных» включены основные права работников по обеспечению защиты своих персональных данных, такие как: право на полную информацию о своих персональных данных и обработке этих данных; свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом; определение своих представителей для защиты своих персональных данных; доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору; требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства РФ; требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях; обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Раздел «Обязанности и ответственность работодателя за нарушение норм, регулирующих обработку и защиту персональных данных» содержит информацию о последствиях за нарушение законодательства о персональных данных (лица, виновные в нарушении норм, регулирующих получение, обра-

ботку и защиту персональных данных работника, несут различные виды ответственности в соответствии с российским законодательством).

Раздел «Заключительные положения», указывает круг лиц, на которых распространяется данное Положение, а также порядок ознакомления с ним. В качестве приложения к данному разделу приводится Форма обязательства о конфиденциальности и неразглашении персональных данных.

Работодатель утверждает положение самостоятельно, соблюдая процедуру согласования, установленную локальным нормативным актом организации. Как правило, принимаемый локальный акт согласовывается с начальником отдела кадров, главным бухгалтером, юристом или другими работниками. Положение вводится в действие приказом работодателя (Приложение 10).

Считаем, что разработанное нами Положение позволит более полно регламентировать порядок обеспечения защиты персональных данных в ООО «Титовский кирпичный завод».

Основным организационным документом, регламентирующим служебные обязанности лиц, осуществляющих сбор, обработку, хранение и передачу персональных данных работников является должностная инструкция пользователя по работе с персональными данными, именно о разработке такого документа и пойдет речь в следующем параграфе выпускной квалификационной работы.

. 3.2. Разработка инструкции пользователя по работе с персональными данными

С целью защиты интересов ООО « Титовский кирпичный завод» и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными, предлагаем разработать единую для всех пользователей Общества Инструкцию пользователя по работе с персональными данными.

Данный документ будет распространять свое действие, как на работу в автоматизированных системах, так без применения таковых. Данная Инструкция, как и Положение о защите персональных данных разрабатываются в соответствие с требованиями ГОСТ Р 7.0.97-2016.

Обязательными реквизитами такой инструкции являются:

- наименование организации;
- вид документа;
- дата;
- номер документа (при непосредственном утверждении руководителем);
- место составления;
- заголовок к тексту
- визы согласования документа;
- подпись;
- гриф утверждения.

Разработанная нами Инструкция (Приложение 11) имеет следующие разделы:

I. Общие положения;
II. Термины и определения;
III. Порядок работы со сведениями, содержащими персональные данные;
IV. Порядок доступа лиц в помещения;
V. Требования по техническому укреплению;
VI. Ответственность за разглашение персональных данных;
VII. Заключительные положения.

Текст Инструкции начинается с раздела «Общие положения», в котором излагаются цели и предназначение данного документа, нормативные правовые акты в соответствии с которыми разработан данный документ, порядок ознакомления с настоящей Инструкцией.

Второй раздел Инструкции «Термины и определения» содержит перечень основных терминов и понятий, используемых в тексте данного локального акта (автоматизированное рабочее место, документированная информация, доступ к информации, информационная система персональных данных, информация, несанкционированный доступ, носитель информации, обработка персональных данных, персональные данные, посторонние лица, распространение персональных данных, средство защиты информации от несанкционированного доступа, уничтожение персональных данных).

В третьем раздел данного документа «Порядок работы со сведениями, содержащими персональные данные» устанавливается обязанность сотрудников Общества при обработке персональных данных на бумажных документах, съёмных носителях (дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, следить за сохранностью, как самих бумажных документов, съёмных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, и не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с такими данными. В данном разделе также прописывается перечень действий, которые запрещены при обработке, хранении и передаче персональных данных. В качестве приложения к данному разделу прилагается Форма Журнала учета машинных носителей информации.

Четвертый раздел Инструкции «Порядок доступа лиц в помещения» предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка доступа лиц в помещения ООО «Титовский кирпичный завод». В соответствии с этим разделом Инструкции, контроль за порядком обеспечения доступа лиц в помещения Общества возлагается на начальника отдела кадров. В помещения ИСПДн Общества беспрепятственно пропускаются директор Общества и сотрудники, имеющие допуск к работе с персональными данными и только с целью выполнения своих должностных обязанностей. При наличии служебного удостоверения, с разрешения директора Общества и в сопровождении ответственного за ор-

ганизацию обработки персональных данных пропускаются: сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции. Ограниченный режим пропуска установлен для сотрудников, не имеющих допуска к работе с персональными данными или не имеющих функциональных обязанностей в помещениях, где обрабатываются или хранятся такие данные, а также сотрудники сторонних организаций и учреждений для выполнения договорных отношений. В качестве приложения к данному разделу прилагается Форма Журнала учета ключей от сейфов и помещений.

Пятый раздел разработанного нами документа «Требования по техническому укреплению» закрепляет обязанность руководителя Общества обеспечивать обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности помещений, в которых осуществляется сбор, обработка, хранение и передача персональных данных.

В шестом разделе Инструкции «Ответственность за разглашение персональных данных» указывается, что работники Общества, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации. В свою очередь, руководитель Общества за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого лица.

В заключительном седьмом разделе Инструкции «Заключительные положения», указывается круг лиц, на которых распространяется данный документ, а также определяется порядок ознакомления с ним.

Разработанная Инструкция утверждается директором Общества с соблюдением процедуры согласования. По общему правилу принимаемый в ООО «Титовский кирпичный завод» локальный акт согласовывается с начальником отдела кадров, главным бухгалтером и юристом. Инструкция вводится в действие приказом работодателя (Приложение 12).

Подводя итоги по третьей главе выпускной квалификационной работы, отметим, что Положение о защите персональных данных и Инструкция пользователя по работе с персональными данными являются основополагающими документами, регламентирующими охрану персональных данных в ООО «Титовский кирпичный завод». От полноты содержания данных локальных актов зависит весь механизм обеспечения документационной защиты персональных данных в данной коммерческой организации.

ЗАКЛЮЧЕНИЕ

В результате исследования теоретических и практических вопросов, связанных с документационным обеспечением защиты персональных данных, мы пришли к следующим выводам:

1. В настоящее время значительные трудности на практике вызывают, как само определение содержания понятия «персональные данные», так и применяемые для классификации таких данных критерии и признаки. В действующем российском законодательстве под «персональными данными» понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Такая трактовка данного термина позволяет достаточно широко применять его на практике. Сложившийся в судебной практике подход не признавать телефонный номер абонента, в качестве его персональных данных, считаем не верным, поскольку он противоречит положениям ст. 8 Федерального закона «О персональных данных», в которой индивидуальные средства коммуникации относятся к разряду общедоступных персональных данных.

В научной литературе можно встретить различные признаки и критерии для классификации персональных данных. На наш взгляд, наиболее оптимальным для классификации всех персональных данных, будет является отраслевой критерий, который позволит систематизировать всю необходимую персональную информацию применительно к целям деятельности каждой конкретной организации.

По данному авторскому критерию можно условно выделить следующие виды персональных данных:

- предоставляемые в государственные и муниципальные органы (например, данные о наличии или отсутствии судимости; о доходах);

- предоставляемые в кредитные организации (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения,

сумма, условия вклада и другие сведения);

- предоставляемые в медицинские организации (например, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью - в медико-профилактических целях; в целях установления медицинского диагноза и оказания медицинских услуг);

- предоставляемые в организации ЖКХ (например, данные о владении, пользовании и распоряжении недвижимым имуществом);

- предоставляемые в организации связи (например, адреса электронной почты; сведения об аккаунтах; IP-адрес);

- предоставляемые в образовательные учреждения (например, данные о составе семьи, об опеке (попечительстве), об отношение к группе риска, о поведенческом статусе).

2. Сбор, обработка, передача и хранение персональных данных осуществляется на основании основополагающих принципов, закрепленных в ст. 5 Федерального закона №152-ФЗ. Анализ положений данных принципов позволил нам прийти к выводу о том, что содержание и смысл некоторых из них дублируют друг друга или носят сугубо формальный характер. Так, например, в целях оптимизации можно было бы объединить основополагающее начало о том, что обработке подлежат только персональные данные, которые отвечают целям их обработки, а содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки с положением о том, что обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки, в один принцип, назвав его: «принципом минимизации персональных данных».

Условия обработки персональных данных достаточно подробно урегулированы ст. 6 Федерального закона №152-ФЗ о персональных данных и достаточно эффективно реализуются на практике.

3. Конфиденциальность персональных данных представляет собой обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без

согласия субъекта персональных данных или наличия иного законного основания. Для обеспечения тайны персональных данных на том или ином коммерческом предприятии должен быть разработан пакет локальных нормативных актов, устанавливающих обязанность оператора-работодателя при обработке персональных данных принимать все необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования или распространения персональных данных, а также от иных неправомерных действий и предусматривающих меры ответственности за нарушение конфиденциальности таких данных.

4. В деятельности ООО «Титовский кирпичный завод» используются основные и дополнительные меры по обеспечению безопасности персональных данных, причем их применение напрямую зависит от того, осуществляется ли такая обработка с использованием или без использования средств автоматизации. Основные меры регламентируются федеральным законодательством, дополнительные - локальными актами данной организации.

Обработка персональных данных Общества, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было: определить места хранения персональных данных (материальных носителей); установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ; обеспечить раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях; соблюсти при хранении материальных носителей условия, обеспечивающие сохранность персональных данных и исключающих несанкционированный к ним доступ. Меры по обеспечению безопасности персональных данных, реализуемые ООО «Титовский кирпичный завод» в рамках системы защиты персональных данных, при их обработке в информационных системах персональных данных, должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных. Под такими

угрозами понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится руководителем Общества с учетом оценки возможного вреда (ст. 18.1 Федерального закона №152-ФЗ; п. 7 Постановления Правительства РФ №1119). Примечателен тот факт, что, оперируя термином вред, законодатель, к сожалению, не указывает его вид, что, на наш взгляд, является явным упущением, позволяющим трактовать данное понятие на практике достаточно широко. Не секрет, что в данном случае речь идет только об одном виде вреда - моральном, размер которого, согласно ст. 1101 ГК РФ определяется исключительно судом, ну ни как не руководителем организации. В этой связи, считаем целесообразным, внести соответствующие изменения и дополнения как в подп. 5 п. 1 ст. 18.1 Закона о защите персональных данных, так и в п. 7 Постановления Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г., заменив в них термин «оценка» понятием «предупреждение» и дополнив указанием на конкретный вид причиненного вреда.

5. Всю документацию ООО «Титовский кирпичный завод» регламентирующую защиту персональных данных, можно условно разделить на 3 группы: организационную, технологическую и методическую. Рассматривая различные документы Общества в сфере оборота персональных данных, мы акцентировали свое внимание на Согласии на обработку персональных данных и задались вопросом, можно ли получить его посредством направления СМС-сообщений? Поскольку Роскомнадзор на своем официальном сайте указал, что: «получение согласия на обработку персональных данных

по телефону, посредством СМС-сообщений действующим законодательством Российской Федерации не установлено», мы посчитали такое разъяснение не совсем верным. С одной стороны - да, получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений не предусмотрено действующим российским законодательством, но, с другой стороны прямо и не запрещено им. Анализируя деятельность сотрудников Общества по получению такого Согласия от отдельных субъектов персональных данных (иногородних работников, контрагентов находящихся в других районах или областях), полагаем, что получение такого согласия посредством СМС-сообщений значительно упростило бы им работу. В этой связи считаем внести соответствующие изменения в п. 1 ст. 9 Федерального закона №152-ФЗ «О персональных данных» и изложить его в следующей редакции:

«1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом, в том числе посредством направления оператору СМС-сообщений. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором».

Для более детальной регламентации процедуры получения согласия посредством направления Оператору СМС-сообщений, считаем необходимым, разработать в ООО «Титовский кирпичный завод» Регламент «О получении согласия на обработку персональных данных посредством СМС-сообщений», который предположительно мог бы включать в себя следующие разделы:

1.Общие положения.

В данном разделе, устанавливались общие правила и порядок дачи согласия на обработку своих персональных данных посредством направления Оператору СМС-сообщений; определялись термины и понятия, используемые в данном Регламенте.

2. Обязательные условия Согласия, направляемого посредством СМС-сообщений.

В данном разделе указываются: перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональными данными, на совершение которых дается согласие.

3. Порядок подготовки, отправки, учета и хранения СМС-сообщений.

В данном разделе должны быть расписаны процедуры подготовки, отправки, учета и хранения СМС-сообщений, содержащих Согласие субъектов на обработку их персональных данных.

4. Заключительные положения.

Данный раздел посвящен сфере действия данного Регламента. Порядок вступления его в силу, механизм внесения в него изменений и дополнений.

Полагаем, что разработка и внедрение такого Регламента в документооборот Общества позволит в значительной мере упростить работу Оператора при получении такого Согласия от некоторых категорий субъектов персональных данных.

6. В целях совершенствование работы с документами, регламентирующими защиту персональных данных, нами были разработаны и внедрены в делопроизводство ООО «Титовский кирпичный завод» следующие документы: Положение о защите персональных данных ООО «Титовский кирпичный завод»; Инструкция пользователя по работе с персональными данными. Данные локальные нормативные акты были оформлены с учетом требований ГОСТ Р 7.0.97-2016.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I. Источники

Нормативные правовые акты

1. Конвенция «О защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства РФ. - 2014. - №5. - Ст. 419.

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 2014. - №31. - Ст. 4398.

3. Гражданский кодекс Российской Федерации (часть вторая) (в ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 01.09.2018) // Собрание Законодательства Российской Федерации. - 1996. - № 5. - Ст. 410.

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Собрание законодательства РФ. - 2002. - № 1 (ч. 1). - Ст. 1.

5. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (ред. от 27.12.2018) // Собрание законодательства РФ. - 2002. - № 1 (ч. 1). - Ст. 3.

6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Собрание законодательства РФ. -1996. - № 25. - Ст. 2954.

7. Федеральный закон от 3 июля 2016 г. №230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях» (ред. от 12.11.2018) // Собрание законодательства РФ. - 2016. - №27 (Часть I). - Ст. 4163.

8. Федеральный закон от 27 июля 2010 г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (ред. от 29.07.2018) // Собрание законодательства РФ. - 2010. - №31. - Ст. 4179.

9. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 31.12.2017) // Собрание законодательства РФ. - 2006. - № 31 (1 ч.). - Ст. 3451.

10. Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.12.2018) // Собрание законодательства РФ. - 2006. - № 31 (1 ч.). - Ст. 3448.

11. Федеральный закон РФ от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» (ред. от 28.12.2017) // Собрание законодательства РФ. - 2004. - № 43. - Ст. 4169.

12. Федеральный закон РФ от 27 мая 1996 г. №57-ФЗ «О государственной охране» (ред. от 07.03.2018) // Собрание законодательства РФ. - 1996. - №22. - Ст. 2594.

13. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13.07.2015) // Собрание законодательства РФ. -1997. - № 10. - Ст. 1127.

14. Постановление Правительства РФ от 30 июня 2018 г. №772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и

хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства РФ. - 2018. - №28. - Ст. 4234.

15. Постановление Правительства РФ от 25 января 2013 г. №33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (вместе с «Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг») (ред. от 20.11.2018) // Собрание законодательства РФ. - 2013. - № 5. - Ст. 377.

16. 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.

17. Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Собрание законодательства РФ. - 2008. - №38. - Ст. 4320.

18. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375) (ред. от 23.03.2017) // Российская газета. - 2013. - 22 мая.

19. Приказ Минкультуры РФ от 25 августа 2010 г. №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» (Зарегистрировано в Минюсте РФ 08.09.2010 №18380) // Бюллетень нормативных актов федеральных органов исполнительной власти. - 2011. - №38.

20. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. приказом Росстандарта от 08.12.2016 № 2004-ст) (ред. от 14.05.2018). - М., 2017. - 18 с.

21. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. приказом Росстандарта от 17.10.2013 № 1185-ст). - М., 2014. - 26 с.

22. ГОСТ Р ИСО 15489-1-2007. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования (утв. приказом Ростехрегулирования от 12.03.2007 № 28-ст). - М., 2007. - 19 с.

Материалы судебной практики

23. Апелляционное определение Судебной коллегии по гражданским делам Московского городского суда по делу № 33-28957 от 24 июля 2017 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

24. Постановление Четвертого арбитражного апелляционного суда по делу № А78-19156/2017 от 4 мая 2018 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

25. Постановление Федерального арбитражного суда Северо-Кавказского округа по делу № А53-13327/2013 от 21 апреля 2014 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

26. Решение Химкинского городского суда Московской области по делу № 2-6262/2017 от 9 февраля 2018 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

27. Решение Бугульминского городского суда Республики Татарстан по делу № 2-1654/2017 от 10 октября 2017 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

28. Решение Калининского районного суда г. Уфа Республики Башкортостан по делу № 2-3678/2017 от 5 сентября 2017 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

29. Решение Калининского районного суда города Санкт-Петербурга по делу № 2-3317/2017 от 24 августа 2017 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

30. Решение Переславского районного суда Ярославской области по делу № 2-668/2017 от 11 мая 2017 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

31. Решение Центрального районного суда г. Челябинска по делу № 2-105/2016 от 31 мая 2016 г. - Доступ из справ.-правовой системы «КонсультантПлюс»: Судебная практика.

II. Литература

Литература на русском языке

32. Абаев, Ф.А. Понятие, правовая природа персональных данных / Ф.А. Абаев // Право и государство: теория и практика. - 2014. - № 3 (111). - С. 126-131.

33. Алексеев, С.С., Васильев, А.С., Голофаев, В.В., Гонгало, Б.М. и др. Комментарий к Гражданскому кодексу РФ (учебно-практический). Части первая, вторая, третья, четвертая / Под ред. С.А. Степанова. - М.: Проспект 2009. - 943 с.

34. Амелин, Р.В. О правовых принципах разработки государственных АИС, обрабатывающих персональные данные / Р.В. Амелин, // Информационное право. - 2009. - №2. - С.33-35.

35. Ануфриева, Н.С. Правовые проблемы обработки персональных данных в трудовых отношениях / Н.С. Ануфриева // Актуальные проблемы современной юридической науки: Сборник научных трудов. - Сургут: ИЦ СурГУ, 2012. - С. 114-119.

36. Астахова, Л.В., Рублёв, Е.Л. Проблемы защиты персональных данных в период смены нормативной базы и пути их решения / Л.В. Астахова, Е.Л. Рублёв // Вестник УрФО. Безопасность в информационной сфере. -2013. - № 1 (7). - С. 32-41.

37. Барышников, А. Безопасность корпоративных центров обработки персональных данных / А. Барышников // Защита информации. Инсайд. - 2013. - № 6 (54). - С. 40-41.

38. Басаков, М.И. Документационное обеспечение управления (Делопроизводство): Учебник / М.И. Басаков. - Рн/Д.: Феникс, 2013. - 350 с.

39. Бегларян М.Е., Пичкуренко Е.А. Безопасность персональных данных в современной России / М.Е. Бегларян, Е.А. Пичкуренко // Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов материалы 4-ой Международной научно-практической конференции. - Краснодар: КСЭИ, 2015. - С. 24-28.

40. Бобров И.В., Комарецев Ю.В. Проблема защиты персональных данных работника // Проблемы российского законодательства и международного права Сборник статей Международной научно-практической конференции. Отв.ред. А.А. Сукиасян. - Уфа: АЭТЕРНА, 2015. - С. 26-28.

41. Богатыренко, З.С. Новейшие тенденции защиты персональных данных работника в российском трудовом праве / З.С. Богатыренко // Трудовое право. - 2006. - № 10. - С. 29-51.

42. Бойкова, О.Ф. Обрабатываем персональные данные работников / О.Ф. Бойкова // Независимый библиотечный адвокат. - 2012. - № 2. - С. 21-32.

43. Болотин, В.С., Маслёха, М.А. Механизм защиты права на неприкосновенность частной жизни при обработке персональных данных в информационных системах / В.С. Болотин, М.А. Маслёха // Вестник государственного и муниципального управления. - 2012. - № 3. - С. 99-103.

44. Бондарь, А.О. Организация работы по обеспечению защиты государственных информационных систем персональных данных / А.О. Бондарь, В.П. Железняк, В.А. Мещеряков // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции. - Воронеж: ИПЦ «Научная книга», 2013. - С. 174-175.

45. Борисова, С.А. Общие требования при обработке персональных данных работника и гарантии их защиты / С.А. Борисова // Трудовое право. - 2005. - № 11. - С. 30-36.

46. Быкова, Т.А. Делопроизводство: Учебник / Под ред. Т.В. Кузнецова. - М., 2013. - 364 с.

47. Важорова, М.А. Соотношение понятий «информация о частной жизни» и «персональные данные» / М.А. Важорова // Вестник Саратовской государственной юридической академии. - 2012. - № 4 (86). - С. 55-59.

48. Васильева, К.В. Правила работы с персональными данными сотрудников / К.В. Васильева // Делопроизводство и документооборот на предприятии. - 2008. - № 9. - С. 32-52.

49. Винницкий, И.Е. Роль справедливости и законности в обеспечении целостности и устойчивости системы принципов права / И.Е. Винницкий // История государства и права. - 2011. - №13. - С. 14-17.

50. Войниканис, Е.А. Развитие правового регулирования персональных данных в условиях глобализации: теоретические аспекты / Е.А. Войниканис // Труды по интеллектуальной собственности. - 2014. - Т. 19. - № 4. - С. 131-141.

51. Войниканис, Е.А. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведе-

ний о частной жизни и персональных данных: проблемы совершенствования законодательства / Е.А. Войниканис, Е.О. Машукова, В.Г. Степанов-Егиянц // Законодательство. - 2014. - № 12. - С. 74-80.

52. Волков, Ю.В. Защищенность субъекта при автоматизированной обработке его персональных данных / Ю.В. Волков // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 3-4. - С. 49-53.

53. Волокитина, Р.Н. К вопросу о защите персональных данных работника / Р.Н. Волокитина, Д.В. Дюмина // Сборник научных работ студенческого научного общества «LEX». - Курск: КГУ, 2013. - Вып. 3. - С. 85-87.

54. Воробьева, Ю.А. Проблема определения понятия «персональные данные работника» / Ю.А. Воробьева // Право в условиях глобализации: сборник материалов II Всероссийской научной конференции студентов и аспирантов, 27-28 марта 2014 года. - Архангельск: КИРА, 2014. - С. 151-154.

55. Вышеславова, Т.Ф. Дифференциация персональных данных работников / Т.Ф. Вышеславова // НаукаПарк. - 2015. - № 9 (39). - С. 69-73.

56. Вышеславова, Т.Ф. Правовое регулирование защиты персональных данных работников в современных трудовых правоотношениях / Т.Ф. Вышеславова // Правовая политика: приоритеты и формы реализации. Материалы Второй Международной научно-практической конференции. - М.: Изд-во МГСУ, 2015. - С. 325-327.

57. Вязов, А.Л. Принцип справедливости в современном российском праве и правоприменении: теоретико-правовое исследование: Автореф. дис. ... канд. юрид. Наук / А.Л. Вязов. - М., 2001. - С. 8.

58. Гильмуллина, Д.А., Чикенёва И.В. О защите персональных данных в системе трудовых правоотношений / Д.А. Гильмуллина, И.В. Чикенёва // Известия Оренбургского государственного аграрного университета. - 2014. - № 3. - С. 231-234.

59. Гражданское право: Учебник: В 3 т. / Отв. ред. А.П. Сергеев, Ю.К. Толстой. - М.: ТК Велби, Изд-во Проспект, 2006. - Т. 1. - 345 с.

60. Губарева, А.В. Угрозы безопасности персональных данных: проблемы современности / А.В. Губарева, А.Н. Гулемин // Политика и общество. - 2015. - № 2. - С. 151-158.

61. Гугуева, Т.А. Конфиденциальное делопроизводство: Учебное пособие / Т.А. Гугуева. - М., 2012. - 192 с.

62. Деревесников, А.В. Справедливость как принцип права (историко-теоретический аспект) / А.В. Деревесников. - Кострома, 2007. - 125 с.

63. Джавахян Р.М., Ястребова А.И. Конституционно-правовые аспекты защиты права на неприкосновенность частной жизни работника в Российской Федерации / Р.М. Джавахян, А.И. Ястребова // Теория и практика общественного развития. - 2015. - № 11. - С. 106-111.

64. Егошина, Г.Г. Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции / Г.Г. Егошина // Теория и практика общественного развития. - 2014. - № 3. - С. 328-330.

65. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника / М.С. Журавлев // Информационное право. - 2013. - № 4. - С. 35-38.

66. Иличенков А. Обработка персональных данных работников без их согласия / А. Иличенков // Кадровик. - 2013. - № 5. - С. 159-166.

67. Инсайдер - вариант с заклеиванием usb-порта не поможет: Интервью с Е. Преображенским // Управление персоналом. - 2009. - № 7. - С.27-28.

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

69. Катунцева, М.О. Конституционное право на информацию и проблема защиты персональных данных в социальных сетях / М.О. Катунцева // Конституционные права и свободы человека и гражданина в РФ: проблемы

реализации и защиты Материалы межвузовского студенческого круглого стола. (г. Иркутск, 27 ноября 2015 г.) - Иркутск, 2016. - С. 31-37.

70. Кафтанникова, В.М. Правовое регулирование информационных систем персональных данных / В.М. Кафтанникова // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 2 (4). - С. 14-19.

71. Кафтанникова, В.М. Проблемы правового регулирования персональных данных в государственных информационных системах / В.М. Кафтанникова // Проблемы права. - 2013. - № 2 (40). - С. 104-108.

72. Корняков, В.И. Нормативные предпосылки для закрепления норм о защите персональных данных работника в Трудовом кодексе РФ / В.И. Корняков // Трудовой кодекс Российской Федерации: проблемы теории и практики: материалы региональной научно-практической конференции (г. Пермь, Перм. гос. нац. иссл. ун-т, 11 мая 2012 г.). - Пермь: Перм. гос. нац. иссл. ун-т, 2012. - С. 86-88.

73. Корякина Ю.С. Разрабатываем положение о защите персональных данных / Ю. С. Корякина // Справочник по управлению персоналом. - 2007. - № 7. - С. 90-92.

74. Костомаров К.В., Качанова Е.А. Банк России в сфере защиты персональных данных клиентов коммерческих банков: экономический и юридический аспекты. Монография / К.В. Костомаров, Е.А. Качанова. - Екатеринбург: Уральский институт управления РАНХиГС, 2015. - 139 с.

75. Крапивин О.М. Трудовой договор. Заключение. Изменение. Прекращение. Защита персональных данных работников / О.М. Крапивин. - М.: Ось 89, 2006. - 223 с.

76. Кротов А.В. Опыт обработки персональных данных работника в компании / А.В. Кротов // Информ. право. - 2007. - № 2. - С. 21-24.

77. Крылатова, Н.В. Государственно-правовое регулирование защиты персональных данных работника / Н.В. Крылатова // Правовая система России: история и современность: материалы VI межвузовской (международной) научно-практической конференции. - М.: Изд-во МГОУ, 2013.- С. 94-99.

78. Кузнецов, Д.Л. Кадровое делопроизводство (правовые основы): Практическое пособие / Д.Л. Кузнецов. - М.: Инфра-М, 2013. - 239 с.

79. Кузнецов, И.Н. Документационное обеспечение управления. Документооборот и делопроизводство: учебник и практикум для прикладного бакалавриата / И.Н. Кузнецов. - 3-е изд., перераб. и доп. - М.: Издательство Юрайт, 2018. - 461 с.

80. Кузнецова, Т.В. Организация работы с персональными данными / Т.В. Кузнецова // Трудовое право. - 2011. - № 5. - С. 75-80.

81. Куняев, Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: Учебник / Н.Н. Куняев. - М.: Логос, 2011. - 452 с.

82. Кутенков, Ю.И. Защита субъективного права работника на доступ к своим персональным данным, как проявление защитной функции трудового права / Ю.И. Кутенков // Научные новации трудового права и права социального обеспечения: сборник материалов участников секции трудового права и права социального обеспечения. - М.: Изд-во Моск. гуманит. ун-та, 2014. - С. 259-266.

83. Кутенков, Ю.И. Понятие персональных данных работника в российском трудовом праве / Ю.И. Кутенков // Азиатско-тихоокеанский регион: Экономика, политика, право. - 2015. - № 4 (37). - С. 116-133.

84. Кутенкович, Ю.И. Проблемы правового регулирования оборота персональных данных работников в трудовом законодательстве Российской Федерации / Ю.И. Кутенкович // Экономико-правовые аспекты развития современного общества: научно-практическая конференция, Владивосток, 25 ноября 2013 г. - Владивосток: Изд-во Дальневост. федер. ун-та, 2013. - С. 65-69.

85. Лушников, А.М. Неприкосновенность частной жизни и персональные данные в сфере трудовых отношений: стратегия правотворчества в контексте мирового опыта / А.М. Лушников // Юридическая техника. - 2015. - № 9. - С. 410-417.

86. Лушников, А.М. Персональные данные в сфере трудовых отношений и их правовая защита: сравнительно-правовой аспект // Международные трудовые стандарты и российское трудовое право: перспективы координации / Э.Н. Бондаренко, Е.С. Герасимова, С.Ю. Головина, А.М. Куренной, А.М. Лушников, М.В. Лушникова, Н.Л. Лютов, Е.Е. Мачульская, Э.А. Мжаванадзе, П.Е. Морозов, Ю.П. Орловский, Е.Р. Радевич, Д.В. Черняева, О.А. Шевченко. - М.: Норма : ИНФРА М, 2016. - С. 170-182.

87. Мазина, Г.П. Персональные данные и их защита в трудовых и служебных правоотношениях / Г.П. Мазина // Общественная безопасность, законность и правопорядок в III тысячелетии. - 2015. - № 1-2. - С. 180-185.

88. Малеина, М.Н. Право на тайну и неприкосновенность персональных данных / М.Н. Малеина // Журнал российского права. - 2010. - № 11. - С. 19-24.

89. Малиновский, А.А. Вред как юридическая категория / А.А. Малиновский // Юрист. - 2006. - №2. - С. 222.

91. Мальцев В.В. Принципы уголовного законодательства и общественно опасное поведение / В.В. Мальцев // Государство и право. - 1997. - №2. - С. 99-102.

92. Мальцев В.В. Равенство и гуманизм как принципы уголовного законодательства / В.В. Мальцев // Правоведение. - 1995. - №2. - С.97-103.

93. Маркевич, А.С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях: дис. ... канд. юрид. наук / А.С. Маркевич. - Воронеж, 2006. - 170 с.

94. Маркевич А.С. Персональные данные работника как объект правоотношения: категориально-правовая характеристика / А.С. Маркевич // Вестник Санкт-Петербургской юридической академии. - 2015. - Т. 27. - № 2. - С. 40-45.

95. Маркевич, А.С. Теоретико-правовой анализ зарубежного законодательства о защите персональных данных в сфере трудовых отношений / А.С. Маркевич // Вопросы безопасности. - 2016. - № 3. - С. 89-98.

96. Меликов, У.А. Гражданско-правовая защита персональных данных / У.А. Меликов // Вестник УрФО. Безопасность в информационной сфере. - 2015. - № 4 (18). - С. 49-53.

97. Меньшикова, А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения / А.В. Меньшикова // Экономика и менеджмент инновационных технологий. - 2014. - № 11 (38). - С. 156-159.

98. Минаева, И.В. Электронная база данных по оценке деловых и личностных качеств работника / И.В. Минаева // Газовая промышленность. - 2007. - № 3. - С. 78-80.

99. Мищенко, Е.Ю., Соколов А.Н. Количественные критерии идентификации физического лица при обезличивании персональных данных / Е.Ю. Мищенко, А.Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. - 2014. - № 1 (11). - С. 27-33.

100. Нерсесянц, В.С. Философия права / В.С. Нерсесянц. - М., 1997. - С. 28.

101. Никольская, К. Значение персональных данных в век информационных технологий / К. Никольская // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 2 (4). - С. 45-47.

102. Овсянникова, Е. Насколько эффективна защита персональных данных работников? / Е. Овсянникова // Трудовое право. - 2013. - №2. - С.91-102.

103. Панасенко, Ю.А. Делопроизводство: документационное обеспечение управления: Учебное пособие / Ю.А. Панасенко. - М., 2013. - 112 с.

104. Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, Ю.А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. - 2015. - № 110. - С. 866-894.

105. Петров, А.Я. О персональных данных работника: современное состояние правового регулирования / А.Я. Петров // Трудовое право. - 2008. -№ 4. - С. 90-96.

106. Петрова И.Г. Принцип законности в арбитражном судопроизводстве / И.Г. Петрова // Юридический мир. - 2006. - №3. - С. 76.

107. Петросян, М.Е. Защита персональных данных. Американская модель / М.Е. Петросян // США-Канада. - 2000. - № 6. - С 93.

108. Петрыкина, Н.И. Правовое регулирование оборота персональных данных. Теория и практика. Учебное пособие / Н.И. Петрыкина. - М., 2011. - 112с.

109. Писаренко А.В., Миронова И.И. Нормативно-правовое обеспечение института защиты персональных данных / А.В. Писаренко, И.И. Миронова // Научные исследования: от теории к практике. - 2015. - Т. 2. - № 4 (5). - С. 261-269.

110. Прохорова, Т.Ю. К вопросу о нормативно-правовом регулировании защиты персональных данных / Т.Ю. Прохорова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. - 2016. - № 1 (33). - С. 318-325.

111. Пузикова Л.Н. Защита персональных данных работника / Л.Н. Пузикова // Российское правоведение: Трибуна молодого ученого: Сборник статей. - Томск: Изд-во Том. ун-та, 2014. - Вып. 14. - С. 132-133.

112. Пчелинцев С.С. Современное понимание принципа законности на государственной службе / С.С. Пчелинцев // Юридический мир. - 2010. - №4. - С.32-34.

113. Раудштейн, А.В. Информационные отношения в сфере труда: понятие и характеристика / А.В. Раудштейн // Российский юридический журнал. - 2010. - №6. - С.152-159.

114. Рахимкулова, Л.С. К вопросу о защите персональных данных работника / Л.С. Рахимкулова, Ю.И. Уметбаева // Фундаментальные и прикладные исследования в современном мире. - 2016. - № 15. - С. 204-206.

115. Румянцева, С.А. Конфиденциальная информация. Правовые основы конфиденциальности / С.А. Румянцева // Справочник секретаря и офис-менеджера. - 2008. - №8. - С. 16-20.

116. Саранчук Ю.М. Административная ответственность в области обработки персональных данных: опыт государств СНГ / Ю.М. Саранчук // Закон и право. - 2014. - № 9. - С. 143-146.

117. Сафонов В. Использование персональных данных работника / В. Сафонов // Кадровик. - 2015. - № 8. - С. 28-34.

118. Симоненко, О.С. Нормативное регулирование защиты персональных данных в информационных системах / О.С. Симоненко // Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования Сборник научных статей международной конференции. - 2015. - С. 1015-1018.

119. Смирнов В.Т., Собчак А.А. Общее учение о деликтных обязательствах в советском гражданском праве / В.Т. Смирнов, А.А. Собчак. - Л.: Изд-во Ленинградского государственного университета, 1983. - С. 59.

120. Сологуб, О.П. Делопроизводство: составление, редактирование и обработка документов: Учебное пособие / О.П. Сологуб. - М., 2013. - 207 с.

121. Станскова, У.М. Состав персональных данных в трудовых отношениях: что подлежит защите / У.М. Станскова // Кадровик. - 2014. - № 1. - С. 16-23.

122. Станскова, У.М. Защита персональных данных в трудовых отношениях: некоторые проблемы / У.М. Станскова // Вопросы управления. - 2013. - № 1 (3). - С. 228-231.

123. Станскова, У.М. Проблемы защиты персональных данных в трудовых отношениях / У.М. Станскова // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 3-4. - С. 37-45.

124. Стенюков, М.В. Делопроизводство. Организация документационного обеспечения предприятия / М.В. Стенюков. - М., 2007. - 176 с.

125. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. Пособие / Е.А. Степанов, И.К. Корнеев. - М., 2001. - С. 42.

126. Стрельников, В. Персональным данным - особую защиту / В. Стрельников // ЭЖ-Юрист. - 2013. - №12. - С. 6.

127. Тифенцев, Е.В. Некоторые проблемы защиты персональных данных работников / Е.В. Тифенцев // Защита трудовых прав: проблемы теории и практики: сборник научных статей. - Новосибирск: Экор-книга, 2014. - С. 85-100.

128. Туркиашвили А.М. Правовое регулирование персональных данных как элемента конституционного права на неприкосновенность частной жизни / А.М. Туркиашвили // Образование и право. - 2015. - № 5 (69). - С. 76-92.

129. Федюнин А.Е., Бочкарёв М.В. Роль и место конституционных прав личности в защите персональных данных работника / А.Е. Федюнин, М.В. Бочкарёв // Правовая культура. - 2013. - № 1 (14). - С. 171-175.

130. Флейшиц Е.А. Личные права в гражданском праве Союза ССР и капиталистических стран / Е.А. Флейшиц // Ученые труды Всесоюзного института юридических наук НКЮ СССР. - М., 1941. - Вып. VI. - С. 234.

131. Хачатурова С.С. Персональные данные под защиту! // Международный журнал прикладных и фундаментальных исследований / С.С. Хачатурова. - 2016. - № 5-4. - С. 666-668.

132. Хачатурян Ю. А. Право работника на защиту персональных данных: проблемы применения законодательства / Ю. Хачатурян // Кадровик. - 2015. - № 9. - С. 23-29.

133. Циулина, Н.Е. Формирование и развитие правовой категории «персональные данные» / Н.Е. Циулина // Вестник УрФО. Безопасность в информационной сфере. - 2013. - № 1 (7). - С. 47-52.

134. Чизганов, А.А. Обработка персональных данных работника / А.А. Чизганов // Российское правоведение: Трибуна молодого ученого: Сборник статей. - Томск: Изд-во Том. ун-та, 2014. - Вып. 14. - С. 121-122.

135. Щербович, А.А. Локализация персональных данных граждан России: проблемы правоприменения / А.А. Щербович // Копирайт. Вестник Российской академии интеллектуальной собственности. - 2015. - № 4. - С. 66-77.

Литература на иностранных языках

136. Personal data protection in the European Union. European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025 (INI)) // Official Journal C 033 E, 05.02.2013. - P. 0101-0110.

III. Электронные ресурсы

137. Защита персональных данных в Евросоюзе и США. - URL: http://www.tadviser.ru/index.php/ (дата обращения: 05.01.2019).

138. Регламент Евросоюза о персональных данных. - URL: http://www.tadviser.ru/index.php/ (дата обращения: 05.01.2019).

139. Сайт Роскомнадзора. - URL: https://rkn.gov.ru/treatments/p459/p468/ (дата обращения: 19.10.2018).