

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КАДРОВОМ ДЕЛОПРОИЗВОДСТВЕ

Пичугина Олеся Михайловна

ФГБОУ ВО «Уральский государственный университет путей сообщения»

e-mail: laakostaa@vk.com

Обеспечение конфиденциальности и защиты персональных данных является одной из ключевых проблем современного кадрового делопроизводства. Растущие объемы материалов о сотрудниках в организации требуют повышенного внимания к вопросам информационной безопасности, поскольку утечка конфиденциальных сведений может привести к серьезным юридическим последствиям, финансовым потерям и ущербу деловой репутации компаний.

Персональные данные относятся к частной жизни гражданина. В ст. 23 Конституции Российской Федерации сказано, что каждый имеет права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. В ст. 24 закреплено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются [3]. Из Указа Президента РФ от 06.03.1997 № 188, следует, что персональные данные носят конфиденциальный характер и не должны быть доступны общественности [5]. Таким образом, на законодательном уровне личная информация о человеке получила конфиденциальный характер и охраняется государством. И все субъекты, оперирующие такой информацией, обязаны соблюдать правила, установленные законом.

В нормативно-правовую базу в области работы с персональными данными работника помимо перечисленных выше законодательных и подзаконных актов РФ входят Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (глава 14 «Защита персональных данных работника»), Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон), Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

Актуальность настоящего исследования обусловлена необходимостью определения правил обработки (в частности, хранения) и эффективных механизмов защиты персональной информации сотрудников, позволяющих минимизировать риски нарушения прав работников и обеспечить соблюдение требований нормативных актов в области охраны персональных данных.

Итак, в соответствии с Законом персональные данные – любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным, в связи с этим, относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту персональных данных [4]. Операторами персональных данных являются организации-работодатели, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Работодатель обязан назначить ответственного за организацию обработки персональных данных путем издания соответствующего приказа и указания его обязанностей в должностной инструкции (инструкции по профессии) или трудовом договоре.

Работа с личными данными сотрудников организации ведется специалистами кадровой службы и делопроизводства, бухгалтерии, руководителями структурных подразделений, осуществляется сегодня как с использованием бумажных, так и электронных носителей.

Перечень лиц, доступ которых к персональным данным необходим для выполнения обязанностей, также должен быть утвержден работодателем (в силу ст. 88 ТК РФ) [6]. Кроме того, надо утвердить перечень работников, имеющих доступ к персональным данным в информационной системе (в силу подп. «в» п. 13 Требований, утв. постановлением Правительства РФ от 01.11.2012 № 1119). Оба перечня можно объединить в один приказ [2, с. 66].

К тому же, указанные выше специалисты при приеме на работу помимо традиционной процедуры знакомства с локальными нормативными актами (например, положением о структурном подразделении, должностной инструкцией и т.д.) подписывают и обязательство о неразглашении персональных данных.

Несмотря на все эти процедуры, в российских организациях не редки случаи нарушения работы с персональными данными, за которые ответственность сегодня только ужесточается.

В целях профилактики ошибок, прежде всего, выявим основные проблемы в области обработки и защиты персональных данных в системе кадрового делопроизводства. К ним мы отнесли:

1. Низкий уровень правовой грамотности ответственных за данное направление должностных лиц. Незнание и(или) несоблюдение Федерального закона № 152-ФЗ «О персональных данных» и других нормативно-правовых актов влечет за собой большие штрафы и иные санкции, в частности в отношении организации-работодателя.

2. Неправильное хранение бумажных документов. Часто возникают ситуации, когда документы с персональными данными хранятся ненадлежащим образом: специалисты оставляют открытыми кабинеты, шкафы, документацию кладут в местах общего пользования. Подобные проступки приводят к риску случайного попадания информации посторонним лицам.

3. Несформированность культуры информационной безопасности. Некоторые сотрудники не осознают важность соблюдения правил обращения с персональными данными. Передача информации коллегам или третьим лицам без согласия на это работников, недостаточная дисциплина в хранении паролей и использовании иных средств аутентификации заметно снижает общую защищенность компании.

4. Невысокий уровень технической оснащенности. Некоторые организации используют устаревшие системы защиты, не обновляют программное обеспечение и пренебрегают внедрением современных инструментов защиты.

Недостаточная защита локальных сетей и отсутствие контроля над передачей информации усиливают уязвимость.

5. Угрозы инсайдеров. Значительная доля нарушений связана с действиями недобросовестных сотрудников (так называемых внутренних нарушителей). Инсайдеры могут намеренно распространять конфиденциальную информацию, либо случайно допускать её разглашение вследствие небрежности или халатности.

6. Хакерские атаки и киберугрозы. Организации подвергаются постоянным попыткам взлома, фишинга и других видов кибератак. Без адекватных средств защиты высока вероятность компрометации данных и возникновения серьезных последствий для самих сотрудников и компании.

В целях повышения уровня зрелости работы с персональными данными на предприятиях должен быть реализован целый комплекс мероприятий в области обеспечения информационной безопасности и внедрения современных технологий, соблюдения законодательных требований и внутренних нормативных актов, а также проведен ряд организационных процедур. Рассмотрим данные меры более подробно.

К техническим мерам, обеспечивающим конфиденциальность и защиту персональных данных, относят:

- использование средств антивирусной защиты;
- резервное копирование информационных систем персональных данных и восстановление данных;
- передачу персональных данных по защищенным каналам связи с применением криптографической защиты;
- контроль отчуждаемых устройств (съёмных носителей информации);
- межсетевое экранирование;
- установку шлюзов безопасности электронной почты;
- внедрение современных систем аутентификации пользователей;
- регулярное изменение паролей на компьютерах и в информационных системах, которые используются для обработки персональных данных;
- своевременное обновление программного обеспечения для устранения уязвимостей;
- установление физических систем безопасности (видеонаблюдения);
- анализ событий безопасности;
- регистрацию инцидентов в информационных системах, обрабатывающих персональные данные и обращений по вопросам их обработки и хранения;
- проведение внутренних и внешних аудитов информационных систем и сервисов, по результатам которых разрабатываются планы устранения обнаруженных уязвимостей с указанием сроков и ответственных лиц и т.д.

Помимо технических мер, стоит уделить серьезное внимание и реализации правовых процедур. Это:

- соблюдение строгого соответствия процессов обработки и защиты персональных данных требованиям законодательства и ключевых регуляторов информационной безопасности (Роскомнадзор, ФСБ России, ФСТЭК России);

– разработка и утверждение локальных нормативных актов по обработке и защите персональных данных;

– своевременное ознакомление работников с законодательными актами, внутренними нормативными документами, организационно-распорядительными документами, определяющими правила работы с персональными данными;

– сбор согласий на обработку персональных данных работников, обязательств об их неразглашении;

– актуализация (обновление) нормативных документов согласно изменениям требований законодательства в сфере защиты персональных данных и т.д.

Среди организационных мер особо стоит отметить следующие действия:

– назначение в организации ответственного за организацию обработки персональных данных;

– создание и работу комиссии по защите персональных данных;

– строгую регламентацию и ограничение доступа к рабочим ресурсам, используемым для обработки данных, а также к помещениям с базами персональных данных (организация пропускного режима);

– оборудование помещений профильных структурных подразделений сейфами для хранения носителей персональных данных;

– разграничение доступа к данным, удаление доступа уволенных сотрудников;

– организацию обучения работников (кадровых служб, ИТ-подразделений и других категорий сотрудников, работающих с персональными данными) в области информационной безопасности и защиты персональных данных;

– проведение внутренних и внешних проверок соблюдения компанией требований законодательства в области защиты персональных данных и разработка рекомендаций по устранению выявленных недостатков (в том числе в структурных подразделениях) и т.д.

Таким образом, технические меры и средства позволяют обеспечить полноценную защиту персональных данных сотрудников. К таким мерам относят все программные решения, которые помогают бороться с угрозами, начиная от установки паролей до шифрования баз данных. При этом особое внимание необходимо уделить тем, что содержат персональные сведения сотрудников. Для их защиты создают резервные копии, регулярно обновляют программное обеспечение, что помогает минимизировать риск потерь или повреждения информации.

Меры правового характера формируют прочную основу для защиты персональных данных работников. Они устанавливают обязанности организации и лиц, работающих с такими данными, защищают права субъектов персональных данных и предусматривают ответственность за нарушения.

Важную роль в обеспечении конфиденциальности и сохранности персональных данных обеспечивают организационные мероприятия. Например, регулярное обучение персонала правилам обращения с персональными

данными повышает уровень осведомленности о возможных угрозах и способах их предотвращения, а внутренние инструкции в компании позволяют четко распределять обязанности среди работников кадровых служб и IT-подразделений. Также значимым элементом является контроль соблюдения установленных процедур, проводимый в формате регулярных проверок и аудитов.

Итак, персональные данные являются важнейшим активом любой современной организации и в то же время ее серьезной проблемой [1, с. 9]. Обеспечение конфиденциальности и целостности персональной информации в процессе кадрового делопроизводства – это комплексная задача, успешное разрешение которой требует оптимального сочетания современных технологий обеспечения информационной безопасности, правовых норм и организационно-управленческих процедур. Анализ текущего состояния проблемы свидетельствует о сохранении значительного числа факторов риска, обусловленных недостаточно строгим соблюдением сотрудниками требований корпоративной информационной культуры, незнанием правовой базы, регламентирующей обработку персональных данных, а также дефицитом высокотехнологичных решений, обеспечивающих надежную защиту конфиденциальной информации от несанкционированного доступа и ее утраты.

Список использованных источников

1. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Защита персональных данных в организации : монография. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 124 с.

2. Жижерина Ю. Кто и как отвечает в организации за работу с персональными данными // Делопроизводство и документооборот на предприятии. – 2024. – № 4. – С. 64-73.

3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=mlzd21pf8i937724297 (дата обращения: 24.02.2026).

4. О персональных данных : Федер. закон от 27.07.2006 № 152-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=mlzdd15g2n332134324 (дата обращения: 24.02.2026).

5. Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015). – URL: https://www.consultant.ru/document/cons_doc_LAW_13532/0179b6b5a612a4e6b17de579e3589aa0526bfe79/?ysclid=mlzd5f0bfz474568989 (дата обращения: 24.02.2026).

6. Трудовой кодекс от 30.12.2001 № 197-ФЗ (ред. от 28.12.2025, с изм. от 06.02.2026). – URL: https://www.consultant.ru/document/cons_doc_LAW_34683/?ysclid=mlzd7hvxj252739178 (дата обращения: 24.02.2026).