Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал федерального государственного автономного образовательного учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»
(ЛФ ПНИПУ)

Факультет профессионального образования
Направление 44.03.04Профессиональное обучение (по отраслям)
Кафедра «Общенаучных дисциплин»

Зав.кафедрой ОНД
_____М.Е. Жалко
«___» _____ 2025г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

На тему: «Регулирование и защита персональных данных работника (на примере судебной практики по спорам о защите персональных данных)»

Студент Ю.Ю. Ширяева

Состав выпускной квалификационной работы:
1. Пояснительная записка на 61 стр.
2. Графическая часть на __ листах.

Руководитель выпускной квалификационной работы
кандидат педагогических наук, доцент кафедры ОНД А.Н. Попцов

Лысьва, 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
1. Общая характеристика персональных данных 6
1.1 Создание и развитие защиты персональных данных 6
1.2 Понятие персональных данных работника 11
1.1.1 Сущность понятия "персональные данные работника" 12
1.1.2 Признаки персональных данных работника 14
1.2 Нормативно-правовое регулирование обработки персональных данных 16
2. Общие требования при работе с персональными данными работника 19
2.1 Получение, хранение и использование персональных данных работника 19
2.2 Принципы и условия обработки персональных данных работника 22
3. Анализ судебной практики по спорам о защите персональных данных работника 41
3.1 Предложения по совершенствованию защиты персональных данных 46
3.2 Предложение по внедрению системы классификации персональных данных в производственном предприятии 49
ЗАКЛЮЧЕНИЕ 56
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 58
Приложение А 62

ВВЕДЕНИЕ

В современном цифровом обществе, где информация стала одним из ключевых ресурсов, а технологии проникают во все сферы жизни, вопросы защиты персональных данных приобретают особую актуальность. Трудовые отношения, несомненно, являются одной из тех сфер, где личные данные работника подвергаются интенсивной обработке, начиная с этапа трудоустройства и заканчивая прекращением трудового договора. В связи с этим, проблема правового регулирования и обеспечения защиты персональных данных работника становится все более значимой и требует глубокого и всестороннего изучения[1].

Многоаспектность исследуемой проблематики находит свое отражение в нескольких ключевых тенденциях современного общества. Прежде всего, это связано с революционными изменениями в сфере цифровизации, которые приводят к большому росту объема персональных данных, требующих надежной защиты. В условиях повсеместной автоматизации процессов сбора и обработки информации существенно возрастают риски компрометации данных, их неправомерного использования и возможных злоупотреблений со стороны третьих лиц.

Параллельно с технологическим прогрессом наблюдается правовая осознанность граждан. Современные работники демонстрируют высокий уровень осведомленности о своих правах в сфере защиты персональных данных, что выражается в готовности активно защищать свои интересы, в том числе путем обращения в судебные инстанции при выявлении любых нарушений.

Не менее значимым фактором выступает необходимость постоянного развития нормативно-правовой базы в данной области. Это предполагает не только совершенствование национального законодательства, но и его гармонизацию с международными стандартами защиты персональных данных, что требует комплексного подхода к формированию эффективной системы правоприменения на всех уровнях. [2].

Данная выпускная квалификационная работа посвящена исследованию вопросов регулирования и защиты персональных данных работника в Российской Федерации. Особое внимание уделяется анализу судебной практики по спорам о защите персональных данных, поскольку именно судебные решения являются важным источником толкования и применения законодательства, а также позволяют выявить проблемные аспекты и предложить пути их решения.

Целью выпускной квалификационной работы является комплексный анализ правового регулирования и судебной практики по вопросам защиты персональных данных работника, выявление проблемных аспектов и разработка практических рекомендаций по совершенствованию правового регулирования и правоприменительной практики в данной сфере.

Для достижения поставленной цели в работе решаются следующие задачи:

1. Изучение теоретических основ понятия и видов персональных данных, а также принципов их обработки в трудовых отношениях.

2. Анализ действующего законодательства Российской Федерации, регулирующего вопросы защиты персональных данных работника, в том числе трудового законодательства и законодательства о персональных данных.

3. Исследование судебной практики по спорам о защите персональных данных работника, выявление типичных нарушений и тенденций в рассмотрении данных споров.

4. Разработать предложения по совершенствованию защиты персональных данных работников

В качестве объекта исследования выступают общественные отношения, возникающие в связи с обработкой и защитой персональных данных работника. Предметом исследования являются правовые нормы, регулирующие данные отношения, а также судебная практика по спорам о защите персональных данных работника.

Методологическую основу работы составляют общенаучные и научные методы исследования, такие как анализ, синтез, сравнение, обобщение, системный подход, формально-юридический метод и другие.

Структура работы обусловлена поставленной целью и задачами и состоит из введения, основной части, заключения и списка использованных источников.

Данное исследование представляет практическую значимость для работников, работодателей, юристов и других специалистов, занимающихся вопросами трудового права и защиты персональных данных, а также может быть использовано в учебном процессе при изучении соответствующих дисциплин.

1. Общая характеристика персональных данных

1.1 Создание и развитие защиты персональных данных

Проблема защиты персональных данных имеет глубокие исторические корни, однако активное научное осмысление данного вопроса началось относительно недавно. В доцифровую эпоху вопросы конфиденциальности информации решались преимущественно на уровне ведомственных инструкций и профессиональной этики.

Формирование права на неприкосновенность частной жизни

Концептуальное оформление права на частную жизнь произошло в конце XIX века благодаря фундаментальной работе американских юристов Сэмюэля Д. Уоррена и Луи Д. Брендиса. В 1890 году в авторитетном юридическом журнале Harvard Law Review была опубликована их статья “The Right to Privacy”, где впервые было сформулировано понятие “право быть оставленным в одиночестве” (right to be let alone). Это определение легло в основу современного понимания права на неприкосновенность частной жизни.

Становление права на международном уровне

Сформулированные Уорреном и Брендисом идеи получили быстрое практическое воплощение. Уже в первой половине XX века право на частную жизнь начало активно применяться в судебной практике США. Впоследствии эта концепция получила международное признание:

В 1948 году право на частную жизнь было закреплено во Всеобщей декларации прав человека (статья 12). Это стало важным шагом в формировании универсальных стандартов защиты личных прав граждан.

Дальнейшее развитие право на частную жизнь получило в 1950 году с принятием Европейской Конвенции по Правам Человека (статья 8), где было сформулировано более конкретное определение: “Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции”.

Социально-исторический контекст

Особая актуальность прав человека в послевоенный период была обусловлена трагическими последствиями Второй мировой войны. В этот период приоритетным стало обеспечение наиболее значимых социальных прав, включая неприкосновенность личной и семейной жизни, а также тайну переписки. При этом проблема защиты персональных данных, логически вытекающая из права на частную жизнь, не получала широкого общественного и правового признания.

Развитие права в условиях технологического прогресса

Революционные преобразования в сфере защиты частной жизни начались во второй половине XX столетия, когда мир столкнулся с беспрецедентным развитием информационных технологий. Технологический прогресс не только радикально ускорил процессы обработки данных, но и сделал их доступными для массового пользователя, что создало качественно новую реальность в сфере информационной безопасности.

Масштабные изменения в области обработки данных не могли остаться незамеченными на международном уровне. Особую тревогу у европейских правозащитников вызвали потенциальные угрозы, которые новые технологии несли для фундаментального права человека на неприкосновенность частной жизни.

Исторической вехой в развитии законодательства о защите персональных данных стала публикация в 1968 году Рекомендации №509 Парламентской ассамблеи Совета Европы. В этом документе впервые на официальном уровне были обозначены риски, связанные с использованием современных технологий обработки информации, и выражена серьезная обеспокоенность возможными нарушениями права на частную жизнь. Именно этот документ положил начало формированию целостной системы правового регулирования в сфере защиты персональных данных на международном уровне.

Первые основополагающие законодательные инициативы

История правового регулирования персональных данных началась с новаторского решения в немецком регионе Гессен, где в 1970 году был принят первый в мире законодательный акт, регулирующий обращение с личной информацией граждан. Примечательно, что этот правовой эксперимент носил ограниченный характер, распространяясь исключительно на территорию одной федеральной земли, что, тем не менее, стало важным прецедентом в развитии международного законодательства о защите данных.

Качественно новый этап в формировании правовой базы защиты персональных данных ознаменовало принятие в 1974 году американского Privacy Act. Данный законодательный акт совершил концептуальный прорыв, установив прямую корреляцию между фундаментальным правом на неприкосновенность частной жизни и обработкой персональных данных. Впервые на законодательном уровне было закреплено понимание того, что любая деятельность государственных структур по сбору, обработке и распространению личной информации граждан потенциально может затрагивать их конституционное право на приватность.

Несмотря на то, что первые законодательные акты не являлись полноценными законами о защите персональных данных, они заложили фундамент для дальнейшего развития данного правового института. Постепенно право на защиту персональных данных начало приобретать самостоятельное значение, выходя из тени общего права на частную жизнь и формируясь как отдельный правовой институт, требующий специального регулирования.

Первые серьезные исследования в области защиты персональных данных появились в 1970-х годах, когда началось массовое внедрение компьютерных технологий в обработку информации. Ученые того периода фокусировались на технических аспектах защиты данных, уделяя особое внимание криптографическим методам и системам разграничения доступа.

Начало 1990-х годов ознаменовалось кардинальными изменениями в правовой системе России, что потребовало создания новых механизмов

защиты персональных данных. В этот период закладывались фундаментальные основы регулирования в данной сфере. Ключевым шагом стало включение в Конституцию РФ положений о защите частной жизни и персональных данных.

Исследователи того времени сосредоточились на адаптации международного опыта к российским реалиям. Особое внимание уделялось разработке базовых принципов защиты данных, формированию механизмов контроля за их обработкой и созданию правовых инструментов защиты прав субъектов персональных данных.

Следующий этап развития историографии защиты персональных данных в 2000-е годы характеризуется углублением исследований и их комплексным характером. Ученые начали рассматривать защиту данных как междисциплинарную проблему, требующую внимания специалистов в области права, информатики, социологии и этики.

В этот период активно изучались технические аспекты защиты информации, разрабатывались правовые механизмы регулирования, исследовались этические вопросы обработки персональных данных. Особое внимание уделялось влиянию глобализации на защиту персональных данных и проблемам цифрового суверенитета.

В эпоху активного развития цифровых технологий научное сообщество столкнулось с необходимостью глубокого изучения методов защиты личной информации пользователей. С появлением инновационных способов обработки и передачи данных вопрос обеспечения конфиденциальности стал одним из приоритетных направлений исследовательской деятельности.

Поворотным моментом в изучении проблематики защиты персональных данных стали 2010-е годы. Этот период ознаменовался существенным расширением тематики исследований и формированием новых научных концепций. Специалисты сконцентрировали усилия на совершенствовании систем кибербезопасности, выявлении потенциальных

угроз информационной защищенности и изучении практического применения существующих норм.

Начало 2020-х годов ознаменовалось переходом к качественно новому уровню регулирования в сфере защиты персональных данных. Данный этап характеризуется глубокой интеграцией правовых норм в цифровую среду общества. Особое внимание уделяется адаптации законодательства к современным технологическим достижениям, включая развитие искусственного интеллекта, методов машинного обучения и технологий работы с массивами данных.

В условиях тотальной цифровизации научное сообщество активно ищет новые решения в области обеспечения конфиденциальности информации. Значительный интерес представляют современные методы биометрической аутентификации, блокчейн-технологии и квантовые методы шифрования, открывающие перспективные направления в защите персональных данных.

Особое значение в современных исследованиях приобретает этический аспект использования личной информации в различных областях человеческой деятельности. Ученые стремятся найти оптимальное соотношение между потребностью в обработке данных для технологического прогресса и необходимостью обеспечения права граждан на конфиденциальность.

Серьезное внимание уделяется международному аспекту защиты данных. Исследователи работают над созданием единых стандартов и протоколов обмена информацией между странами, при этом уделяя особое внимание вопросам цифрового суверенитета государств в условиях доминирования глобальных цифровых платформ и облачных технологий.

Особое направление научных исследований составляет анализ влияния новых технологий на права человека в цифровой среде. Ученым предстоит найти ответы на вызовы, связанные с автоматизированной обработкой

персональных данных, использованием алгоритмов принятия решений и обеспечением прозрачности таких систем.

В современных условиях активно развивается методология оценки рисков и эффективности систем защиты данных. Исследователи разрабатывают новые метрики и инструменты для измерения уровня защищенности персональных данных, а также методы прогнозирования потенциальных угроз в условиях постоянно меняющейся цифровой среды.

1.2 Понятие персональных данных работника

В условиях цифровизации экономики и активного использования информационных технологий в сфере трудовых отношений, вопросы, связанные с обработкой персональных данных работников, приобретают особую актуальность. Защита информации о частной жизни, личной и семейной тайне является конституционным правом каждого гражданина, в том числе и работника. Данная подглава посвящена рассмотрению сущности и признаков понятия "персональные данные работника", а также анализу основных нормативных правовых актов, регулирующих порядок их обработки.

Персональные данные работника – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (работнику), которая необходима работодателю в связи с трудовыми отношениями и включает в себя сведения о фактах, событиях и обстоятельствах жизни работника, в том числе его анкетные данные, профессиональную квалификацию, деловые и профессиональные качества, а также иные сведения, необходимые для соблюдения законодательства, содействия в трудоустройстве, получении образования, продвижении по службе, обеспечения личной безопасности, контроля за количеством и качеством выполняемой работы, обеспечения сохранности имущества участников совместного труда. [4].

Данное понятие является универсальным и может применяться как в теоретическом анализе, так и в практической деятельности по защите персональных данных работников.

1.1.1 Сущность понятия "персональные данные работника"

Не существует единого, исчерпывающего перечня персональных данных работника, поскольку объем необходимой информации может варьироваться в зависимости от специфики трудовой функции, организационной структуры и кадровой политики организации. Однако, к типичным примерам персональных данных работника можно отнести:

— Идентификационные данные, например: фамилия, имя, отчество, дата и место рождения, паспортные данные, данные свидетельства о рождении, ИНН, СНИЛС;

Эти сведения, в совокупности, формирующие личную идентификационную картину гражданина, являются краеугольным камнем множества юридических и социальных процессов. От простейших бытовых операций, таких как покупка билета или оформление посылки, до сложных финансовых транзакций и участия в выборах, идентификационные данные играют роль ключа, открывающего доступ к правам и возможностям. Точность и актуальность этих сведений крайне важны для обеспечения бесперебойного функционирования государственных и коммерческих сервисов.

Фамилия, имя и отчество, являясь устоявшимися элементами идентификации, позволяют отличить одного человека от другого, особенно в условиях больших городов и высокой плотности населения. Дата и место рождения служат подтверждением возраста и места появления на свет, что важно для определения правоспособности и территориальной привязки. Паспортные данные, как основной документ, удостоверяющий личность, содержат в себе наиболее полную информацию о гражданине и используются практически во всех сферах жизни;

— Контактные данные. Адрес регистрации, адрес фактического проживания, номер телефона (рабочий, личный), адрес электронной почты.

Контактные данные, а именно адрес регистрации, адрес фактического проживания, номер телефона (рабочий, личный), адрес электронной почты, несомненно, относятся к персональным данным работника. Это связано с тем, что данная информация позволяет идентифицировать конкретное физическое лицо и установить с ним связь, что напрямую подпадает под определение персональных данных в соответствии с законодательством о защите персональных данных.

Указание адреса регистрации и фактического проживания необходимо для соблюдения требований миграционного законодательства, трудового законодательства и в целом для обеспечения возможности направления работнику юридически значимых уведомлений и документов.

Номера телефонов (рабочий и личный) и адрес электронной почты являются средствами оперативной связи с работником. Личный номер телефона может использоваться для экстренной связи с работником в случае необходимости;

— Сведения об образовании, квалификации и профессиональной подготовке;

— Сведения о трудовой деятельности и данные трудовой книжки. Информация о воинской обязанности, так же являются персональными данными работника;

— Данные о семейном положении и составе семьи: сведения о браке, детях, других членах семьи;

— Сведения о состоянии здоровья работника, включающие результаты медицинских осмотров (как предварительных, так и периодических), данные об установлении инвалидности (в случае ее наличия), а также информация о перенесенных или имеющихся заболеваниях, которые могут оказывать влияние на его трудоспособность, относятся к категории специальных персональных данных, требующих особого внимания и защиты;

— Финансовая информация: данные о заработной плате, банковских счетах, наличии задолженностей;

— Иные данные (фотографии, видеозаписи, данные о членстве в профсоюзах, политических взглядах)[17].

1.1.2 Признаки персональных данных работника

Персональные данные работника представляют собой особую категорию информации, которая характеризуется рядом существенных признаков, определяющих их правовой статус и особенности обработки. Основным признаком является возможность идентификации физического лица, как напрямую, так и косвенно через совокупность представленных сведений.

Идентификационный характер персональных данных проявляется в том, что любая информация, позволяющая установить конкретное лицо, приобретает статус персональных данных. Это может быть как прямая идентификация через фамилию, имя, отчество, так и косвенная – через совокупность других сведений, в том числе профессиональных или социальных характеристик работника.

Целевой характер использования персональных данных неразрывно связан с трудовыми отношениями. Информация приобретает статус персональных данных работника только в том случае, если она необходима работодателю для осуществления трудовых правоотношений.

Конфиденциальность информации является неотъемлемым признаком персональных данных работника. Такая информация требует особой защиты от несанкционированного доступа и распространения. Работодатель обязан обеспечить соответствующие меры безопасности, предотвращающие случайную или несанкционированную передачу данных третьим лицам.

Документальное оформление также выступает важным признаком персональных данных работника. Вся информация должна быть зафиксирована в установленном порядке, что позволяет осуществлять

контроль за её обработкой и хранением. Это касается как бумажных носителей, так и электронных баз данных.

Динамический характер персональных данных проявляется в том, что информация может меняться со временем, требуя актуализации и обновления. Работник обязан информировать работодателя об изменении персональных данных, а работодатель, в свою очередь, должен своевременно вносить корректировки в имеющиеся записи.

Системность персональных данных проявляется в том, что они образуют целостную информационную систему, включающую различные категории сведений о работнике. При этом каждая категория данных может иметь свои особенности обработки и хранения, требующие индивидуального подхода к защите.

Субъектный характер персональных данных определяется наличием конкретного субъекта – работника, чьи права и интересы подлежат защите. Работник обладает комплексом прав по отношению к своим персональным данным, включая право на доступ, исправление и удаление информации.

Взаимодействие с персональными данными работника регулируется законодательством о защите персональных данных. Работодатель обязан получить согласие работника на обработку его персональных данных, за исключением случаев, прямо предусмотренных законом.

Работник имеет право на получение информации о своих персональных данных, обрабатываемых работодателем, а также на требование об их уточнении, блокировании или уничтожении в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не соответствуют заявленным целям обработки. Работодатель обязан предоставить работнику доступ к его персональным данным, в течение установленного законом срока и принять меры по удовлетворению его требований.

1.2 Нормативно-правовое регулирование обработки персональных данных

Первоочередной целью принятия законов о защите данных стало обеспечение фундаментального права человека на неприкосновенность частной жизни в условиях цифровизации. По мере того как технологии обработки информации становились все более совершенными и доступными, возрастала и опасность несанкционированного доступа к личной информации граждан.

В процессе формирования правовой базы в сфере защиты персональных данных законодатели ставили перед собой задачу – создать эффективную систему контроля над обращением личной информации граждан. Основной упор делался на предотвращение различных форм незаконного использования данных, включая их несанкционированное распространение, неправомерный сбор и обработку, а также защиту от утечек.

Особое внимание уделялось регламентации деятельности организаций, оперирующих персональными данными. Разработчики законов детально проработали систему требований к компаниям-операторам, включая технические аспекты защиты информации и конкретные процедуры её обработки. Благодаря этому удалось сформировать понятную и прозрачную структуру взаимодействия всех участников процесса, где чётко определены права и обязанности каждой стороны.

При создании правовой базы законодатели стремились найти разумный компромисс между различными интересами. С одной стороны, требовалось обеспечить надёжную защиту частной информации граждан и их право на конфиденциальность. С другой стороны, необходимо было предусмотреть механизмы законного использования персональных данных в общественно значимых целях, включая государственные интересы и потребности общества в целом.

Такой подход позволил создать сбалансированную систему регулирования, учитывающую как права отдельных граждан, так и потребности различных институтов общества в работе с персональными данными. При этом основной акцент делался на обеспечение безопасности информации при одновременном сохранении возможности её легального использования в рамках установленных законом правил.

Основным нормативным правовым актом, регулирующим отношения в сфере защиты персональных данных в Российской Федерации, является Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Помимо данного закона, обработка персональных данных работников регулируется[8]:

- Трудовым кодексом Российской Федерации (ТК РФ) глава 14: статья 86 ТК РФ устанавливает общие требования к защите персональных данных работника и гарантии их защиты.
- Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"[10].
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (149-ФЗ) - устанавливает общие принципы защиты информации, включая персональные данные, в информационных системах[11].
- Иными федеральными законами и подзаконными актами, регулирующими отдельные аспекты обработки персональных данных (например, законы о медицинском страховании, пенсионном обеспечении и т.д.).

Принципы обработки персональных данных, закрепленные в Федеральном законе № 152-ФЗ, являются основополагающими для любой организации, осуществляющей такую обработку. К ним относятся законность, справедливость, ограничение обработки конкретными, заранее определенными и законными целями, соответствие целей обработки объему

и характеру обрабатываемых персональных данных, а также точность и актуальность персональных данных.

Обработка персональных данных работников, в частности, должна осуществляться с соблюдением требований, установленных Трудовым кодексом РФ. Статья 86 ТК РФ определяет общие требования к защите персональных данных работника, включая необходимость получения согласия работника на обработку его персональных данных, за исключением случаев, предусмотренных законом. Работодатель обязан ознакомить работника под роспись с документами организации, устанавливающими порядок обработки персональных данных работников, а также с его правами и обязанностями в этой области[3].

Особое внимание следует уделять обработке специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Такая обработка допускается только в случаях, прямо предусмотренных законом, и с соблюдением строгих ограничений. Например, обработка данных о состоянии здоровья работника может осуществляться в случаях, когда это необходимо для проведения обязательных медицинских осмотров или для обеспечения безопасных условий труда.

Работники, имеющие доступ к персональным данным, обязаны сохранять их конфиденциальность и не раскрывать третьим лицам, за исключением случаев, предусмотренных трудовым договором или законом.

Вывод по первой главе:

Первая глава посвящена исследованию понятия персональных данных работника, их сущности, признаков и нормативно-правового регулирования обработки.

В ходе исследования установлено, что персональные данные работника – это любая информация, относящаяся к прямо или косвенно определенному физическому лицу (работнику), которая позволяет идентифицировать его.

Сущность понятия "персональные данные работника" заключается в том, что это информация, связанная с трудовой деятельностью, квалификацией, образованием, а также личной жизнью работника, имеющая значение для трудовых отношений.

Признаки персональных данных работника:

— Относятся к конкретному работнику.

— Позволяют идентифицировать работника прямо или косвенно.

— Имеют значение для установления, изменения или прекращения трудовых отношений.

В главе подробно рассмотрено нормативно-правовое регулирование обработки персональных данных, включающее в себя Конституцию Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон "О персональных данных" и другие нормативные акты. Анализ нормативных актов показывает, что обработка персональных данных работника требует соблюдения ряда принципов и условий, включая законность, справедливость, конфиденциальность и обеспечение безопасности персональных данных.

Таким образом, первая глава формирует теоретическую базу для дальнейшего исследования проблематики защиты персональных данных работника, определяя ключевые понятия и нормативные рамки в данной области.

2. Общие требования при работе с персональными данными работника

2.1 Получение, хранение и использование персональных данных работника

Получение, хранение и использование персональных данных работника – это деликатная область, требующая строгого соблюдения законодательства и уважения к частной жизни сотрудника. Работодатель вправе собирать только необходимые для работы персональные данные. Избыточный сбор

информации является нарушением прав работника и влечет юридическую ответственность.

При получении персональных данных работника необходимо уведомить его о целях, способах обработки, круге лиц, имеющих доступ к этим данным, а также о его правах в отношении своих персональных данных. Получение согласия работника на обработку его персональных данных является обязательным условием, за исключением случаев, прямо предусмотренных законом[6].

При получении персональных данных, требуется:

— Получить согласие работника за исключением случаев, прямо предусмотренных законом (например, при заключении трудового договора). Согласие должно быть конкретным, информированным и сознательным. Рекомендуется получать согласие в письменной форме;

— Следовать принципу минимизации данных, то есть собрать только те данные, которые необходимы для достижения конкретных, заранее определенных целей, например при трудоустройстве на работу;

— Ограничить источники получения, получать данные непосредственно от работника. Запрос данных у третьих лиц возможен только с письменного согласия работника;

— Предоставить работнику информацию о целях обработки персональных данных, категориях обрабатываемых данных, сроках обработки, порядке осуществления прав субъекта персональных данных. Рекомендуется разработать и предоставить работнику "Уведомление об обработке персональных данных".

Хранение персональных данных работника должно осуществляться в условиях, обеспечивающих их конфиденциальность и защиту от несанкционированного доступа, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий. Работодатель обязан принимать необходимые меры для защиты персональных данных, включая использование средств защиты информации, ограничение доступа к

персональным данным только для уполномоченных лиц, и регулярное обновление систем безопасности.

Для хранения персональных данных требуется обеспечить следующее:

—Принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий;

—Определить места хранения персональных данных (электронные базы данных, бумажные архивы) и обеспечить их защиту;

—Ограничение доступа к персональным данным только теми сотрудниками, которым это необходимо для выполнения их трудовых обязанностей;

—Следить за актуальностью персональных данных и своевременно вносить изменения;

—По истечении срока хранения или при достижении целей обработки персональные данные должны быть уничтожены;

Использование персональных данных работника должно осуществляться строго в соответствии с заявленными целями и только в пределах, необходимых для достижения этих целей. Передача персональных данных третьим лицам допускается только с согласия работника, за исключением случаев, предусмотренных законодательством. Работодатель не имеет права использовать персональные данные работника в целях, не связанных с трудовыми отношениями, например, для продвижения товаров или услуг.

Так же требуется уточнить, что работник имеет право на доступ к своим персональным данным, право на их уточнение, блокирование или уничтожение в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Работник имеет право на информацию об обработке его персональных данных, отзыв согласия и защиту своих прав в случае нарушений, обратившись в уполномоченный орган или суд. Работодатель обязан предоставлять информацию и содействовать работнику.

2.2 Принципы и условия обработки персональных данных работника

Нормативная основа обработки персональных данных работников формируется на пересечении двух ключевых нормативно-правовых актов: Федерального закона №152-ФЗ «О персональных данных» и главы 14 Трудового кодекса Российской Федерации. Процедурная регламентация предваряется обязательным уведомлением Роскомнадзора, нарушение которого влечет за собой административно-правовую ответственность.

Принцип законности в контексте обработки персональных данных это легальная парадигма обработки персональных данных базируется на фундаментальном принципе законности. Правовой конструкт предусматривает осуществление всех операций с персональными данными исключительно в рамках установленных законодательством целей и на основе принципов справедливости. Категориальный императив не допускает обработку данных, противоречащую целям их первоначального сбора.

Целевая направленность обработки персональных данных строго регламентирована. Допустимыми целями являются: обеспечение соблюдения законодательства, содействие в трудоустройстве и профессиональном развитии, обеспечение личной безопасности работников, контроль качества работы и сохранность имущества. Обработка данных в иных целях категорически запрещена.

Принцип необходимости и достаточности это аксиологический подход к обработке персональных данных реализуется через принцип необходимости, предполагающий обработку исключительно релевантной информации, необходимой для достижения заявленных целей. Количественно-качественная характеристика обрабатываемых данных

должна соответствовать заявленным целям и исключать избыточность информации.

Точность и актуальность данных обеспечивается за счет регулярного обновления информации и поддержания её в состоянии, соответствующем действительности. Хранение данных осуществляется в форме, позволяющей определить субъекта данных, и только в течение необходимого для целей обработки срока.

Субъектно-правовое регулирование обработки персональных данных базируется на обязательном получении согласия работника, за исключением случаев, прямо предусмотренных законодательством. Формально-юридический аспект требует письменной формы согласия при обработке специальных категорий данных, биометрической информации и при принятии решений на основе автоматизированной обработки.

Ограничение доступа к персональным данным обеспечивается путем предоставления доступа только уполномоченным лицам и только в необходимом для выполнения должностных обязанностей объеме. В современных условиях передача личной информации сотрудников третьим лицам допускается только при наличии документально оформленного согласия самого работника. Исключением из этого правила являются ситуации, когда передача данных необходима для предотвращения непосредственной угрозы жизни или здоровью работника.

Комплексный подход к обеспечению безопасности персональных данных предполагает реализацию ряда обязательных мероприятий. Прежде всего, работодатель должен определить конкретное лицо, ответственное за организацию процесса обработки данных. Кроме того, требуется разработка полного пакета необходимой документации, внедрение как организационных, так и технических средств защиты информации, регулярная оценка возможных рисков и осуществление систематического внутреннего контроля.

В рамках документационного обеспечения работодатель обязан подготовить ряд ключевых документов: политику обработки персональных данных, положение о защите информации, приказ о перечне сотрудников, имеющих доступ к данным, а также соглашение о конфиденциальности. Эти документы формируют правовую основу для организации эффективной системы защиты информации.

Нарушение установленных правил работы с персональными данными влечет за собой наступление ответственности как для организации в целом, так и для конкретных должностных лиц. Преобладающей формой ответственности является административная, которая может выражаться в виде штрафных санкций различной величины. Размер и характер наказания определяются в зависимости от тяжести совершенного нарушения и его последствий.

Таким образом, принципы и условия обработки персональных данных работника формируют комплексную систему требований, направленную на обеспечение эффективной и безопасной работы с персональными данными в рамках трудовых отношений. Соблюдение этих принципов является обязательным для всех работодателей и служит основой для построения надежной системы защиты персональных данных работников.

2.3 Способы защиты персональных данных работника

В современных условиях цифровизации трудовых отношений обеспечение надежной защиты персональных данных сотрудников представляет собой критически важную задачу, требующую системного подхода к формированию многоуровневой системы информационной безопасности.

Реализация данного подхода предполагает внедрение комплекса взаимосвязанных организационно-технических мероприятий, направленных на предотвращение различных видов несанкционированного воздействия на конфиденциальную информацию: от неправомерного доступа и

несанкционированной модификации данных до их случайного или преднамеренного разглашения и безвозвратного уничтожения.

При этом особое внимание следует уделить не только технологическим аспектам защиты, но и формированию эффективной системы контроля доступа, а также разработке четких процедур реагирования на возможные инциденты информационной безопасности в сфере обработки персональных данных работников.

Комплексный характер защитных мероприятий должен обеспечивать непрерывность процесса защиты на всех этапах жизненного цикла персональных данных: при их сборе, хранении, передаче и последующем использовании в рамках трудовых правоотношений.

Только такой интегрированный подход к обеспечению информационной безопасности позволит создать надежную преграду для потенциальных угроз и минимизировать риски компрометации конфиденциальной информации о сотрудниках организации.

1. Организационные меры защиты:

1.1. Разработка и внедрение локальных нормативных актов:

—Разработка положения о защите персональных данных работников.

В положении о защите персональных данных работников необходимо четко определить, с какой целью собираются и обрабатываются персональные данные. Цель должна быть законной, конкретной и заранее определенной. Не допускается обработка персональных данных, несовместимая с целью сбора. Документ должен содержать перечень персональных данных, которые собираются и обрабатываются работодателем, а также источники их получения.

Положение должно детально регламентировать порядок доступа к персональным данным работников, включая порядок предоставления доступа сотрудникам организации, имеющим право доступа в силу своих должностных обязанностей, а также порядок предоставления доступа третьим лицам (например, государственным органам, страховым компаниям,

банкам) на основании законных оснований. Необходимо установить процедуры для обеспечения права работников на ознакомление со своими персональными данными, их изменение, блокирование или удаление в случаях, предусмотренных законодательством.

В положении о защите персональных данных необходимо указать ответственность за нарушения. Работодатель также несет ответственность за несоблюдение законодательства и нарушение прав работников.

Так же необходимо указать порядок утверждения, изменения и доведения положения до работников, а также обеспечить его регулярную актуализацию в соответствии с изменениями законодательства и процессов обработки персональных данных.

—Правила внутреннего трудового распорядка.

Необходимо включить пункты, касающиеся соблюдения режима конфиденциальности при работе с персональными данными. В частности, Правила должны регламентировать порядок доступа к персональным данным, определяя круг лиц, имеющих право работать с такой информацией, и устанавливая для них индивидуальные пароли и уровни доступа.

—Инструкции по работе с персональными данными.

Инструкции должны содержать подробные указания для каждого сотрудника, имеющего доступ к персональным данным, о правилах обработки информации и мерах безопасности.

Инструкция должна устанавливать строгие правила для обработки персональных данных. Для каждого этапа необходимо прописать конкретные действия, которые сотрудник должен совершать, и действия, которые категорически запрещены.

1.2. Определение ответственных за обработку персональных данных.

Работодатель обязан назначить ответственного сотрудника за организацию обработки персональных данных в организации:

1. Издать приказ о его назначении, может быть их несколько при наличии отдела кадров в организации;

2. Прописать обязанности в должностные инструкции (инструкции по профессии) или трудовом договоре.

В структуре организации функционирует расширенный круг уполномоченных специалистов, обладающих правом доступа к конфиденциальной информации сотрудников. Данная привилегия предоставляется исключительно тем работникам, чья профессиональная деятельность объективно требует оперирования персональными данными коллег в рамках исполнения должностных обязанностей.

К числу таких специалистов относятся:

—сотрудники кадровой службы;

—сотрудники бухгалтерии;

—специалисты налогового учета;

—работники, осуществляющие документооборот;

—сотрудники архивного отдела;

—технические специалисты, обеспечивающие функционирование информационных систем.

В соответствии с действующим законодательством (статья 88 Трудового кодекса РФ), работодатель обязан официально утвердить список лиц, уполномоченных на работу с персональными данными. Данный перечень может быть как включен непосредственно в текст распорядительного документа, так и оформлен в виде самостоятельного приложения к нему.

Дополнительно, согласно пункту 13 утвержденных постановлением Правительства РФ от 01.11.2012 №1119 Требований, необходимо сформировать и утвердить отдельный перечень сотрудников, получающих доступ к персональным данным через информационные системы организации. Это обусловлено необходимостью разграничения прав доступа и обеспечения дополнительного уровня защиты конфиденциальной информации в цифровой среде.

Таким образом, формирование и документальное закрепление круга лиц, допущенных к работе с персональными данными, представляет собой комплексный процесс, требующий учета как кадровых, так и технических аспектов информационной безопасности организации.

1.3. Ознакомление работников с локальными нормативными актами и обучение.

Эффективная система ознакомления и обучения включает в себя несколько этапов. Первоначально, при приеме на работу, каждому новому сотруднику предоставляется возможность изучить ключевые документы, регламентирующие обработку персональных данных. Подтверждением ознакомления служит подпись сотрудника в специальном журнале или листе ознакомления, где указывается дата и перечень изученных документов.

Формализация обучения сотрудников по защите персональных данных создает документальное подтверждение их осведомленности об обязанностях и ответственности, что делает журнал/лист ознакомления юридически значимым документом для разрешения споров.

1.4. Получение согласия на обработку персональных данных.

Работодатель обязан получить письменное согласие работника на обработку персональных данных, за исключением случаев, предусмотренных законом. Работник должен понимать, какие данные, как и в течение, какого срока, будут обрабатываться. Работодатель обязан предоставить полную информацию об обработке данных до получения согласия.

1.5. Ограничение доступа к персональным данным.

Необходимо предоставить доступ к персональным данным только тем сотрудникам, кому это требуется, дифференцируя права доступа по ролям и обязанностям. Для этого: проанализировать бизнес-процессы, определить потребности сотрудников в доступе и создать матрицу, учитывающую категории сотрудников, их функции и проекты.

2. Технические меры защиты:

2.1 Использование средств защиты информации:

—Антивирусное программное обеспечение. Обеспечивает защиту от вредоносных программ, которые могут быть использованы для кражи или повреждения персональных данных.

—Межсетевые экраны. Предотвращают несанкционированный доступ к внутренней сети организации.

—Системы обнаружения и предотвращения вторжений (IDS/IPS). Отслеживают сетевой трафик и выявляют подозрительную активность.

—Шифрование данных. Преобразует данные в нечитаемый формат, что делает их бесполезными для злоумышленников в случае утечки. Шифрование должно применяться как для данных, хранящихся на носителях информации, так и для данных, передаваемых по сети.

2.2 Контроль доступа к информационным системам:

—Использование паролей. Требования к паролям должны быть достаточно строгими (длина, сложность, регулярная смена).

—Двухфакторная аутентификация. Усиливает защиту учетных записей пользователей за счет использования двух факторов аутентификации (например, пароль и SMS-код, с последующим оповещением).

—Разграничение прав доступа. Каждому пользователю должны быть предоставлены только те права доступа, которые необходимы для выполнения его трудовых обязанностей.

—Регистрация и аудит действий пользователей. Необходимо вести журналы регистрации действий пользователей в информационных системах, что позволяет отслеживать несанкционированный доступ и выявлять инциденты безопасности.

—Защита каналов связи. При передаче персональных данных по сети необходимо использовать защищенные каналы связи (VPN, SSL/TLS).

—Резервное копирование данных. Регулярное создание резервных копий данных позволяет восстановить информацию в случае потери или

повреждения. Резервные копии должны храниться в безопасном месте, отдельно от основной базы данных.

3. Физическая защита:

—Контроль доступа в помещения, где хранятся персональные данные.

Ограничение доступа посторонних лиц в помещения, где хранятся серверы и другая аппаратура, содержащая персональные данные. Организация физической безопасности помещений, в которых обрабатываются персональные данные, является критически важным элементом защиты конфиденциальной информации. Доступ к серверным комнатам, архивам с бумажными документами и другим местам хранения персональных данных должен быть строго контролируемым и регламентированным. Неконтролируемый доступ повышает риск несанкционированного копирования, уничтожения, модификации или блокирования персональных данных, а также риск хищения носителей информации.

Для усиления контроля целесообразно применять современные СКУД (электронные карты, биометрия, кодовые панели). СКУД автоматизируют учет посещений, оперативно блокируют доступ при увольнении/изменении обязанностей и формируют отчеты о посещениях.

Помимо вышеперечисленных мер, важна и человеческая составляющая. Сотрудники, имеющие доступ к помещениям с персональными данными, должны быть проинструктированы о необходимости соблюдения правил безопасности, ответственности за их нарушение и порядке действий в случае возникновения внештатных ситуаций. Одним из ключевых аспектов обеспечения информационной безопасности является грамотное обучение сотрудников. Каждый работник должен обладать навыками выявления потенциально опасных ситуаций и уметь реагировать на нарушения установленных правил доступа к информации. Это включает в себя способность распознавать подозрительное

поведение коллег и своевременно информировать руководство о замеченных отклонениях от норм безопасности.

Особого внимания заслуживает вопрос контроля физического доступа к информационным ресурсам организации. Защита компьютерных систем и различных носителей данных от несанкционированного проникновения требует комплексного подхода и внедрения многоуровневых систем безопасности.

Особенно сложной задачей представляется организация контроля за перемещением информационных носителей за пределы организации. Для эффективного решения этой проблемы необходимо разработать и внедрить строгую систему учета, которая будет фиксировать все случаи выноса данных. Каждый такой случай должен сопровождаться документальным оформлением с указанием причины перемещения, ответственного сотрудника и сроков возврата носителя на территорию компании.

Формирование культуры информационной безопасности среди сотрудников – процесс непрерывный и требующий системного подхода. Работники должны не только владеть техническими навыками работы с данными, но и понимать существующие угрозы, уметь оценивать риски и принимать соответствующие меры предосторожности. Регулярные обучающие мероприятия и напоминания о правилах безопасности помогают минимизировать человеческий фактор как источник потенциальных уязвимостей.

Важно понимать, что даже самые современные технические средства защиты информации не могут гарантировать полную безопасность данных без активного участия персонала в поддержании установленных норм безопасности. Только сочетание технологических решений с высокой степенью осведомленности и дисциплины сотрудников способно создать действительно надежную систему защиты информации.

2.4 Ответственность за нарушения хранения и использований персональных данных работников

В настоящее время зафиксированы значительные штрафные санкции за нарушения законодательства в области обработки персональных данных, предусмотренные статьей 13.11 Кодекса об административных правонарушениях Российской Федерации (КоАП РФ). Ответственность распространяется как на юридические лица, так и на должностных лиц, ответственных за организацию работы с персональными данными. В случае отсутствия назначенного ответственного лица, ответственность, как правило, возлагается на руководителя организации.

В Таблице 1 представлены действующие размеры штрафов по ст. 13.11 КоАП РФ для юридических и должностных лиц (штрафы для физических лиц и индивидуальных предпринимателей в данной работе не рассматриваются).

Следует отметить, что в Государственной Думе РФ находится на рассмотрении законопроект, предусматривающий существенное увеличение размеров штрафных санкций (по состоянию на 23.01.2024 законопроект прошел первое чтение). Предполагается, что новое законодательство значительно увеличит финансовую ответственность за нарушения в сфере обработки персональных данных, что подчеркивает актуальность и серьезность данной проблемы.

Лицам, нарушившим требования Закона № 152-ФЗ, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная.

Статья 13.11 КоАП РФ устанавливает административную ответственность за нарушения в сфере обработки персональных данных. Штрафы варьируются в зависимости от типа нарушения и категории нарушителя (граждане, должностные лица, ИП, юридические лица). Наиболее распространенные нарушения, такие как обработка данных без

законных оснований или без согласия субъекта, влекут штрафы до 3 000 рублей для граждан и до 100 000 рублей для юридических лиц. Невыполнение обязанностей по предоставлению информации субъекту данных или по уточнению/блокировке/удалению данных также влечет штрафы, хотя и в меньшем размере.

Отдельно стоит статья 17.13 КоАП РФ, предусматривающая ответственность за незаконное распространение сведений о защищаемом лице. Важно учитывать, что размеры штрафов могут быть неактуальными, поэтому необходимо проверять информацию в актуальных редакциях КоАП РФ.

Таблица 1 - Ответственность за нарушение закона о персональных данных

Вид ответственности	Нарушение	Санкция	Норма
Административная ответственность	Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление таких сведений (информации) в неполном объеме или в искаженном виде	Предупреждение или административный штраф: для граждан в размере от 100 до 300 руб.; для должностных лиц – от 300 до 500 руб.; для юр. лиц – от 3 тыс. до 5 тыс. руб.	Статья 19.7 КоАП РФ
	Неправомерный отказ в предоставлении гражданину, в том числе адвокату в связи с поступившим от него адвокатским запросом, и (или) организации информации, предоставление которой предусмотрено законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	Административный штраф для должностных лиц в размере от 5 тыс. до 10 тыс. руб.	Статья 5.39 КоАП РФ
	Обработка персональных данных в случаях, не предусмотренных законодательством РФ, либо обработка персональных данных, несовместимая с целями сбора персональных данных	Административный штраф: для граждан – в размере от 2 тыс. до 6 тыс. руб.; для до лжностных лиц – от 10 тыс. до 20 тыс. руб.; для юрлиц - от 60 тыс. до 100 тыс. руб. За повторное совершение данного административного правонарушения, административный штраф: для граждан в размере от 4 тыс. до 12 тыс. руб.; для должностных лиц – от 20 тыс. до 50 тыс. руб.; для ИП – от 50 тыс. до 100 тыс. руб.; для юрлиц – от 100 тыс. до 300 тыс. руб.	Часть 1 и 1.1 ст. 13.11 КоАП РФ
	Обработка персональных данных без согласия в письменной форме субъекта персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ, либо обработка персональных данных	Административный штраф: для граждан в размере от 10 тыс. до 15 тыс. руб.; для должностных лиц – от 100 тыс. до 300 тыс. руб.; для юрлиц – от 300 тыс. до 700 тыс. руб.	Часть 2 и 2.1 ст. 13.11 КоАП РФ

	с нарушением установленных требований к составу сведений, включаемых в такое согласие	За повторное совершение данного административного правонарушения, административный штраф:	
		для граждан в размере от 15 тыс. до 30 тыс. руб.;	
		для должностных лиц – от 300 тыс. до 500 тыс. руб.;	
		для ИП – от 500 тыс. до 1 млн руб.;	
		для юрлиц – от 1 млн до 1,5 млн руб.	
	Невыполнение оператором предусмотренной законодательством РФ обязанности по опубликованию или обеспечению иным образом неограниченного до ступа к документу, определяющему политику оператора в от ношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных	Административный штраф:	Часть 3 ст. 13.11 КоАП РФ
		для граждан в размере от 1,5 тыс. до 3 тыс. руб.;	
		для до лжностных лиц – от 6 тыс. до 12 тыс. руб.;	
		для ИП – от 10 тыс. до 20 тыс. руб.;	
		для юрлиц – от 30 тыс. до 60 тыс. руб.	
	Невыполнение оператором предусмотренной законодательством РФ обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Административный штраф:	Часть 4 ст. 13.11 КоАП РФ
		для граждан – в размере от 2 тыс. до 4 тыс. руб.;	
		для должностных лиц – от 8 тыс. до 12 тыс. руб.;	
		для ИП – от 20 тыс. до 30 тыс. руб.;	
		для юрлиц – от 40 тыс. до 80 тыс. руб.	
	Невыполнение оператором в сроки, установленные законодательством РФ, требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	Административный штраф:	Часть 5 и 5.1 ст. 13.11 КоАП РФ
		для граждан в размере от 2 тыс. до 4 тыс. руб.;	
		для должностных лиц – от 8 тыс. до 20 тыс. руб.;	
		для ИП – от 20 тыс. до 40 тыс. руб.;	
		для юрлиц – от 50 тыс. до 90 тыс. руб.	
		За повторное совершение данного административного правонарушения, административный штраф:	
		для граждан в размере от 20 тыс. до 30 тыс. руб.;	

		для должностных лиц – от 30 тыс. до 50 тыс. руб.;	
		для ИП – от 50 тыс. до 100 тыс. руб.;	
		для юрлиц – от 300 тыс. до 500 тыс. руб.	
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним до ступ, если это повлекло неправомерный или случайный до ступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в от ношении персональных данных, при отсутствии признаков уголовно наказуемого деяния	Административный штраф:	Часть 6 ст. 13.11 КоАП РФ
		для граждан в размере от 1,5 тыс. до 4 тыс. руб.;	
		для должностных лиц – от 8 тыс. до 20 тыс. руб.;	
		для ИП – от 20 тыс. до 40 тыс. руб.;	
		для юрлиц – от 50 тыс. до 100 тыс. руб.	
	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных	Административный штраф для должностных лиц в размере от 6 тыс. до 12 тыс. руб.	Часть 7 ст. 13.11 КоАП РФ
	Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ	Административный штраф:	Часть 8 и 9 ст. 13.11 КоАП РФ
		для граждан в размере от 30 тыс. до 50 тыс. руб.;	
		для должностных лиц – от 100 тыс. до 200 тыс. руб.;	
		для юрлиц – от 1 млн до 6 млн руб.	
		За повторное совершение данного административного правонарушения, административный штраф:	
		для граждан в размере от 50 тыс. до 100 тыс. руб.;	
		для должностных лиц – от 500 тыс. до 800 тыс. руб.;	
		для юрлиц – от 6 млн до 18 млн руб.	
	Иные правонарушения:		
	Нарушение правил защиты информации (Статья 13.12 КоАП РФ);		
	Незаконная деятельность в области защиты информации (Статья 13.13 КоАП РФ);		
	Разглашение информации с ограниченным доступом (Статья 13.14 КоАП РФ).		

Уголовная ответственность	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	Штраф в размере до 200 тыс. руб. или в размере заработной платы или иного до хода осужденного за период до 18 месяцев, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо принудительными работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет	Статья 137 УК РФ
	Те же деяния, совершенные лицом с использованием своего служебного положения	Штраф в размере от 100 тыс. до 300 тыс. руб. или в размере заработной платы или иного до хода осужденного за период от 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо принудительными работами на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет	

Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего 16-летнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия	Штраф в размере от 150 тыс. до 350 тыс. руб. или в размере заработной платы или иного до хода осужденного за период от 18 месяцев до 3 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет	
Неправомерный отказ должностного лица в предоставлении собранных документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан	Штраф в размере до 200 тыс. руб. или в размере заработной платы или иного до хода осужденного за период до 18 месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет	Статья 140 УК РФ
Неправомерный до ступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	Штраф в размере до 200 тыс. руб. или в размере заработной платы или иного до хода осужденного за период до 18 месяцев, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок	Статья 272 УК РФ
То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности	Штраф в размере от 100 тыс. до 300 тыс. руб. или в размере заработной платы или иного до хода осужденного за период от одного 1 до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок	

	Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения	Штраф в размере до 500 тыс. руб. или в размере заработной платы или иного до хода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок	
	Те же деяния, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до 7 лет	
	Иные преступления:		
	Незаконное использование документов для образования (создания, реорганизации) юридического лица (Статья 173.2 УК РФ);		
	Разглашение тайны усыновления (удочерения) (Статья 155 УК РФ).		
Гражданско-правовая ответственность	Причинение лицу убытков в результате нарушения правил обработки его персональных данных	Возмещение убытков	Статья 15 ГК РФ
	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)	Статья 24 Закона № 152-ФЗ, ст. 151 ГК РФ
Дисциплинарная ответственность	Разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника	Увольнение	Подпункт "в" п. 6 ч. 1 ст. 81 ТК РФ
	Иные нарушения в области персональных данных при их обработке	Выговор, замечание, увольнение	Статья 90 и 191 ТК РФ

Вывод по второй главе:

Детально рассмотрены общие требования к работе с персональными данными работника в соответствии с действующим законодательством. Анализ получения, хранения и использования персональных данных подчеркнул необходимость строгих процедур для защиты конфиденциальности работников.

Было установлено, что получение персональных данных должно быть ограничено исключительно необходимой информацией, напрямую связанной с трудовыми отношениями.

Рассмотренные принципы и условия обработки персональных данных акцентировали важность законности, справедливости, соразмерности и ограниченности обработки целей, определенных работодателем.

3. Анализ судебной практики по спорам о защите персональных данных работника

Анализ судебных решений по спорам о защите персональных данных работника приобретает ключевое значение в контексте динамично меняющегося законодательства и технологических рисков. По данным Роскомнадзора, за 2023–2024 годы количество обращений граждан по вопросам нарушений в сфере персональных данных увеличилось на 65%, при этом 42% жалоб были связаны с трудовыми отношениями. Это свидетельствует о системных проблемах в правоприменении, включая:

—Недостаточную осведомленность работодателей о требованиях Закона № 152-ФЗ;

—Злоупотребление «законным интересом» при обработке данных без согласия работника;

—Использование избыточных данных (например, биометрии) без обоснования необходимости.

Рассмотрим судебную практику (Приложение А) Верховного Суда Российской Федерации комплексного трудового спора, в котором с одной стороны истец заявляет, о нарушении работодателя при обработке персональных данных, а также о незаконном приказе, о привлечении к дисциплинарной ответственности в последующем увольнением.

Общая характеристика дела

Судебный орган: Верховный Суд Российской Федерации

Категория дела: Трудовой спор

Участники процесса:

— Истец: ФИО2 (бывший работник)

— Ответчик: работодатель бывшего работника АО «Научно-производственное предприятие «Исток» им. А.И. Шокина»

Предмет спора

Истец обратился в суд с требованием:

— Признать незаконным приказ о привлечении к дисциплинарной ответственности;

— Признать незаконным приказ об увольнении;

— Восстановить на работе;

— Взыскать средний заработок за время вынужденного прогула;

— Взыскать компенсацию морального вреда;

— Признать неправомерными действия работодателя при обработке персональных данных.

Правовая основа:

В деле рассматриваются вопросы применения:

— статья 81 Трудового кодекса РФ ()

Данная статья определяет основания для увольнения работника по инициативе работодателя. В ней перечислены ситуации, при которых работодатель имеет право расторгнуть трудовой договор, например:

1. Неоднократное неисполнение работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание;
2. Прогул (отсутствие на рабочем месте без уважительных причин более четырёх часов подряд в течение рабочего дня);
3. Появление на работе в состоянии алкогольного, наркотического или иного токсического опьянения;
4. Совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя;
5. и другие основания.

— Законодательства о защите персональных данных

Федеральный закон № 152-ФЗ «О персональных данных» регулирует отношения, связанные с обработкой персональных данных в Российской Федерации. Закон направлен на защиту прав и свобод граждан при обработке их персональных данных, включая обеспечение конфиденциальности и

безопасности этих данных. В нём определены принципы и условия обработки персональных данных, права субъектов персональных данных, обязанности операторов, обрабатывающих персональные данные, а также меры по обеспечению безопасности персональных данных и ответственность за нарушения требований закона.

Фактические обстоятельства

История трудовых отношений:

— Принятие на работу: 23 октября 2017 г.;

— Перевод на должность заместителя начальника отдела режима: 9 апреля 2018 г.;

— Первое увольнение: 15 июля 2021 г. (по сокращению штата);

— Восстановление на работе: 30 ноября 2021 г.;

— Второе увольнение: 6 июня 2022 г. (за прогул).

Правовые позиции

Основания для обращения в суд:

— Нарушение процедуры увольнения;

— Дискриминационное преследование после восстановления на работе;

— Нарушение прав при обработке персональных данных;

— Необоснованное привлечение к дисциплинарной ответственности.

Результаты рассмотрения:

Решение суда первой инстанции:

— Приказ о привлечении к дисциплинарной ответственности признан незаконным

— Приказ об увольнении признан незаконным

— Истец восстановлен на работе

— Взыскана заработная плата за время вынужденного прогула (1 008 523,20 руб.)

— Взыскана компенсация морального вреда (30 000 руб.)

— Отказано в признании неправомерными действий по обработке персональных данных

Особенности дела

Ключевые моменты:

— Наличие предыдущего судебного спора о законности увольнения;

— Утверждение истца о дискриминационном характере действий работодателя;

— Нарушение процедуры привлечения к дисциплинарной ответственности;

— Распространение персональных данных работника.

Вывод по делу:

Данное судебное решение наглядно показывает, что соблюдение работодателем установленной процедуры увольнения является обязательным условием законности всех кадровых решений. Любое отклонение от установленного порядка может привести к признанию увольнения незаконным и последующему восстановлению работника на прежнем месте работы.

Особое внимание в деле уделяется необходимости тщательного выяснения причин отсутствия работника на рабочем месте. Работодатель обязан не только запросить письменное объяснение у сотрудника, но и предоставить ему необходимое время для его подготовки, а также проверить достоверность представленных работником сведений. Пренебрежение этими требованиями может стать основанием для признания увольнения незаконным.

Судебное решение также подтверждает недопустимость дискриминационного преследования работника со стороны работодателя. В случае с истцом прослеживается система ущемления его прав: от недоплаты пособия по временной нетрудоспособности до необоснованного отказа в предоставлении отпуска. Такие действия работодателя не только нарушают

трудовое законодательство, но и могут повлечь за собой дополнительную ответственность, включая взыскание компенсации морального вреда.

Важным аспектом дела является защита персональных данных работника. Распространение информации о дисциплинарном взыскании среди сотрудников без согласия работника признается нарушением закона. Это подчеркивает необходимость строгого соблюдения правил обработки и распространения персональных данных, установленных Федеральным законом «О персональных данных».

Анализ судебной практики наглядно демонстрирует, что исход трудового спора во многом зависит от качества собранной доказательственной базы. Когда сотрудник сталкивается с ущемлением своих законных интересов, критически важно подготовить основательный пакет подтверждающей документации. В качестве доказательств могут выступать официальные документы, письменные свидетельства коллег, электронная переписка и прочие материалы, способные объективно подтвердить факт неправомерных действий со стороны работодателя.

Судебная инстанция выполняет роль важнейшего института защиты трудовых прав граждан, обеспечивая восстановление нарушенных прав и законных интересов работников. В процессе рассмотрения дел суды не только принимают решения по конкретным ситуациям, но и формируют единую практику применения трудового законодательства, что способствует его более эффективному и единообразному применению на практике.

Рассмотренное судебное разбирательство представляет существенный интерес для всех участников трудовых правоотношений. Работодатели получают наглядный пример того, что пренебрежение нормами трудового законодательства, особенно в вопросах увольнения персонала или проявления дискриминации, может повлечь за собой серьезные последствия, включая восстановление работника в должности, компенсацию утраченного заработка и возмещение морального вреда.

Для работников данное судебное решение служит практическим руководством по защите своих прав в конфликтных ситуациях с работодателем. Оно убедительно демонстрирует, что даже в условиях очевидного дисбаланса сил между работником и работодателем, закон становится на сторону того, кто способен документально подтвердить факт нарушения своих прав. Это подчеркивает важность правовой грамотности работников и их способность грамотно отстаивать свои интересы в судебном порядке.

В заключение стоит отметить, что данное судебное решение демонстрирует комплексный подход к рассмотрению трудовых споров, включающих вопросы как собственно увольнения, так и защиты персональных данных работника. Особое внимание уделяется соблюдению процедурных требований при привлечении работника к дисциплинарной ответственности и его последующем увольнении.

3.1 Предложения по совершенствованию защиты персональных данных

Для совершенствования защиты персональных данных в организациях требуется комплексный подход, сочетающий правовые, технические и организационные меры. В первую очередь, необходимо усилить нормативно-правовую базу, адаптировав её к вызовам цифровой трансформации. Это предполагает разработку стандартов, регулирующих использование искусственного интеллекта и алгоритмов машинного обучения, которые всё чаще применяются для обработки данных. Важно законодательно закрепить требования к прозрачности автоматизированных систем, обеспечив возможность аудита их работы и контроля со стороны регуляторов. Такие меры позволят минимизировать риски дискриминации и ошибок, связанных с предвзятостью алгоритмов.

На техническом уровне критически важно внедрять современные средства защиты информации, такие как многофакторная аутентификация, сквозное шифрование и системы обнаружения аномалий. Организациям

следует регулярно проводить оценку рисков, выявляя уязвимости в информационных системах, и внедрять модели угроз, соответствующие специфике обрабатываемых данных. Особое внимание стоит уделить обезличиванию персональных данных, что позволит сохранить их аналитическую ценность при одновременном снижении рисков для конфиденциальности. Для этого целесообразно разработать методики деидентификации, сочетающие криптографические методы и дифференциальную приватность.

Организационные меры должны включать создание специализированных подразделений или назначение ответственных лиц, обладающих экспертизой в области информационной безопасности. Их задачи должны охватывать не только внедрение защитных технологий, но и разработку внутренних регламентов, обучение сотрудников и проведение регулярных аудитов. Формирование культуры конфиденциальности через тренинги и имитационные учения поможет снизить человеческий фактор, который остаётся одной из ключевых причин утечек. Внедрение «политики чистого стола» и строгого контроля доступа в помещения с носителями данных дополнительно минимизирует риски физического компрометирования информации.

Меры направлены на создание многоуровневой системы защиты, сочетающей правовую, техническую и организационную составляющие, что соответствует требованиям современных стандартов информационной безопасности:

1. **Формирование внутренней нормативной базы.** Для обеспечения правомерной обработки личных сведений организациям необходимо разработать комплекс внутренних регламентов, охватывающих все этапы работы с данными — от сбора до уничтожения. Ключевое значение имеет не только создание документов (таких как политика безопасности или порядок проведения аудитов), но и их адаптация к специфике деятельности компании.

Использование типовых шаблонов без учета отраслевых особенностей может привести к правовым рискам.

2. **Закрепление зон ответственности.** В зависимости от масштаба организации полномочия по контролю за обработкой данных могут быть делегированы отдельному специалисту (например, HR-менеджеру) или целому подразделению. Важно юридически оформить распределение обязанностей через приказы, дополнительные соглашения к трудовым договорам или должностные инструкции. Для повышения эффективности рекомендуется дифференцировать подходы к работе с различными категориями данных (персонал, клиенты, партнеры).

3. **Систематизация знаний персонала.** Сотрудники, имеющие доступ к личным сведениям, должны быть детально ознакомлены не только с положениями Федерального закона №152-ФЗ, но и с внутренними стандартами компании. Регулярное обновление базы нормативных документов и проведение инструктажей помогут минимизировать ошибки, вызванные неосведомленностью.

4. **Внедрение программ профессионального развития.** Назначение ответственного за защиту данных требует от сотрудника не только формального соответствия должности, но и наличия специализированных компетенций. Обязательным условием является прохождение профильного обучения (очно или в формате вебинаров), изучение судебной практики и участие в отраслевых семинарах для актуализации знаний.

5. **Регламентация взаимодействия с третьими сторонами.** Работа с контрагентами и субъектами данных должна строиться на основе письменных соглашений, четко определяющих условия обработки информации. Ключевыми элементами являются: оформление информированного согласия, включение в договоры разделов о конфиденциальности, а также разработка типовых форм поручений на обработку сведений.

6. **Создание системы превентивного контроля.** Для оперативного выявления нарушений необходимо внедрить механизмы внутреннего аудита, включая периодические проверки соблюдения регламентов и анализ инцидентов. Результаты таких проверок должны становиться основой для корректирующих действий, направленных на устранение уязвимостей.

7. **Обеспечение физической безопасности.** Помещения, где хранятся материальные носители данных (документы, серверы), требуют особого режима доступа. Целесообразно установить многоуровневую систему контроля (пропуски, журналы учета, видеонаблюдение), оборудовать сейфовые зоны и исключить несанкционированное присутствие посторонних лиц.

8. **Оптимизация технических средств защиты.** Анализ бизнес-процессов позволяет выявить критические точки, требующие усиления кибербезопасности. На основе оценки рисков внедряются решения: шифрование каналов связи, резервное копирование, антивирусная защита и сегментация сетей для ограничения несанкционированного доступа.

9. **Автоматизация управления учетными данными.** Парольная политика должна предусматривать регулярную ротацию сложных комбинаций, блокировку учетных записей при многократных ошибках ввода, а также внедрение двухфакторной аутентификации для сотрудников, работающих с особыми категориями данных.

3.2 Предложение по внедрению системы классификации персональных данных в производственном предприятии

Цель предложения - повышение уровня защиты персональных данных сотрудников за счет внедрения категоризации данных и дифференцированных мер безопасности, соответствующих уровню угроз.

Этапы реализации предложения на промышленном предприятии:

Этап 1. Классификация данных

1. Общедоступные персональные данные - ФИО, должность, рабочий телефон, корпоративная почта.

Использование общедоступными персональными данными может быть в корпоративных целях в телефонных справочниках с контактной информацией сотрудников, для какой-либо коммуникации между сотрудниками и руководством предприятия. При деловой переписке между сотрудниками могут использоваться общедоступные персональные данные для выполнения общей цели предприятия.

2. Специальные персональные данные - Медицинские заключения, сведения о судимостях, религиозные/политические взгляды (если собраны), информация о семейном положении.

Данные о группе здоровья, о противопоказаниях или информация о перенесенных заболеваниях могут использоваться для допуска сотрудника к работе во вредных условиях на производстве, для того чтобы обеспечить соответствие условий труда состоянию здоровья работника и предотвратить профессиональные заболевания. Это позволяет работодателю принимать обоснованные решения о распределении задач, предоставлении необходимых средств индивидуальной защиты и организации рабочего процесса, минимизируя риски для здоровья.

3. Биометрические персональные данные - отпечатки пальцев (для системы контроля и управления доступом), фотографии на пропусках, голосовые записи (системы идентификации).

Биометрические данные могут быть эффективно использованы в биометрических системах контроля доступа на промышленных предприятиях, позволяет значительно усилить безопасность критически важных зон и объектов. Традиционные методы, такие как пропускные карты или пароли, подвержены риску утери, кражи или передачи третьим лицам, что делает их менее надежными. Биометрические данные, будучи уникальными для каждого человека, исключают возможность несанкционированного проникновения и обеспечивают высокий уровень

безопасности. Это особенно важно в зонах с повышенным риском, таких как хранилища материалов, производственные цеха с опасным оборудованием или лаборатории.

Кроме того, биометрические системы контроля доступа значительно упрощают и повышают точность учета рабочего времени. Отсутствует необходимость в использовании табелей, карточек или других методов фиксации прихода и ухода сотрудников. Система автоматически регистрирует время начала и окончания работы каждого сотрудника на основе его биометрических данных, что исключает возможность манипуляций и ошибок, связанных с человеческим фактором. Это не только повышает точность расчета заработной платы, но и освобождает время сотрудников отдела кадров, которое можно направить на более важные задачи.

Методика классификации:

— Аудит существующих баз данных и документооборота.

— Присвоение меток категорий в информационных системах (например, «ОБЩ», «СПЕЦ», «БИО»).

Этап 2 Категоризация персональных данных

Таблица 2. Распределение категорий персональных данных по уровню угроз с мерами защиты

Категория данных	**Уровень угроз**	**Меры защиты**
Общедоступные	Низкий	—Шифрование при передаче по корпоративной сети. —Ограничение доступа по ролям (Для руководителей рассмотреть расширенный доступ к персональным данным) —Регулярное обновление паролей.
Специальные	Высокий	—Хранение в изолированной базе с двухфакторной аутентификацией. — Использование сертифицированных средств защиты информации (Система

Категория данных	Уровень угроз	Меры защиты
		сертифицированная во ФСТЭК России) — Ведение журнала аудита доступа.
Биометрические	Критический	—Авторизация пользователей для доступа к защищённым сетям, где находятся персональные данные. —Шифрование данных на уровне хранилищ. — Физическая защита серверов с хранением персональных данных сотрудников (сейфовые комнаты с видеонаблюдением).

Этап 3. Реализация предложения с помощью технических средств

Для общедоступных данных:

Внедрение системы предотвращение утечек информации для контроля передачи данных за пределы корпоративной сети.

Для специальных данных:

Установка межсетевых экранов и сегментация сети. Межсетевые экраны функционируют как барьер между внутренней сетью компании и внешним миром, тщательно фильтруя трафик и блокируя несанкционированный доступ. Грамотная настройка межсетевых экранов предполагает определение строгих правил для входящего и исходящего трафика, включая контроль протоколов, портов и IP-адресов. Это позволяет предотвратить проникновение вредоносного программного обеспечения, фишинговых атак и других угроз, направленных на компрометацию конфиденциальной информации.

Для биометрических данных:

Использование сертифицированных биометрических сканеров (соответствие Федеральной службой по техническому и экспортному контролю) и средств контроля защищенности персональных данных

сотрудников. Они становятся неотъемлемой частью стратегии информационной безопасности организаций, стремящихся к соблюдению требований законодательства РФ и минимизации рисков, связанных с утечкой конфиденциальной информации. Внедрение таких систем позволяет не только повысить уровень контроля доступа к критически важным ресурсам, но и обеспечивает соблюдение Федерального закона №152-ФЗ "О персональных данных".

Основное преимущество сертифицированных биометрических сканеров заключается в их соответствии требованиям ФСТЭК России, что гарантирует определенный уровень защиты обрабатываемых данных. Сертификация подтверждает, что устройства прошли необходимые испытания и соответствуют установленным стандартам безопасности, что позволяет организациям быть уверенными в надежности используемых технологий. Выбор сертифицированного оборудования минимизирует риски несанкционированного доступа, подмены данных и других угроз, направленных на компрометацию персональных данных сотрудников.

Этап 4. Внедрения предложения с соответствием нормам

— ст. 18.1 Федерального закона 152-ФЗ «О персональных данных».
— п. 12 Приказа ФСТЭК №2.

Ожидаемые результаты предложения

Внедрение системы классификации персональных данных на производственном предприятии позволит создать комплексную структуру управления информацией, обеспечивающую надежную защиту данных и их эффективное использование в корпоративной среде.

Результатом предложения станет формирование четкой иерархии доступа к различным категориям данных, где каждый сотрудник будет иметь только те права, которые необходимы для выполнения его должностных обязанностей. Система позволит разграничить общедоступные, и

специальные, биометрические персональные данные, что существенно снизит риски несанкционированного доступа и утечки информации.

На предприятии будет создана централизованная база данных с четкой категоризацией информации по уровням конфиденциальности, где каждый тип данных получит свой статус и правила обработки. Это обеспечит прозрачность в работе с информацией и позволит отслеживать все операции с персональными данными в режиме реального времени.

Предложение приведет к формированию единых стандартов обработки персональных данных во всех подразделениях предприятия. Сотрудники получат понятные инструкции по работе с информацией, а руководство – инструменты контроля соблюдения политики информационной безопасности.

Вывод под третьей главе:

Таким образом, анализ судебной практики по делам о защите персональных данных работников позволяет сделать следующие выводы.

Судебная система фиксирует растущую динамику обращений граждан по вопросам нарушений в сфере персональных данных, при этом значительная часть жалоб (42%) связана с трудовыми отношениями. Это свидетельствует о системных проблемах в правоприменении, включая недостаточную осведомленность работодателей о требованиях законодательства, злоупотребление “законным интересом” при обработке данных и использование избыточных данных без должного обоснования.

Судебная практика подтверждает недопустимость дискриминационного преследования работника со стороны работодателя, включая случаи ущемления прав в виде недоплаты пособий, необоснованного отказа в предоставлении отпуска и распространения персональных данных без согласия работника.

Таким образом, анализ судебной практики позволяет сформировать комплексное понимание проблем в сфере защиты персональных данных

работников и выработать эффективные механизмы их решения, что имеет важное практическое значение как для работодателей, так и для работников.

Разработано предложение, которое станет сформированной иерархией доступа к различным категориям данных, где каждый сотрудник будет иметь только те права, которые необходимы для выполнения его должностных обязанностей. Система позволит разграничить общедоступные, и специальные, биометрические персональные данные, что существенно снизит риски несанкционированного доступа и утечки информации.

ЗАКЛЮЧЕНИЕ

В рамках данной выпускной квалификационной работы было проведено всестороннее исследование вопросов, связанных с обработкой персональных данных работников в контексте трудовых отношений.

На основании осуществленного исследования были сформулированы основные заключения:

Персональные данные работника - сложный объект правового регулирования. Уточнена сущность понятия и выделены признаки, что позволило определить границы применения законодательства о персональных данных в трудовой сфере.

Подробно рассмотрено нормативно-правовое регулирование обработки персональных данных, включающее в себя Конституцию Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон "О персональных данных" и другие нормативные акты. Анализ нормативных актов показывает, что обработка персональных данных работника требует соблюдения ряда принципов и условий, включая законность, справедливость, конфиденциальность и обеспечение безопасности персональных данных.

Сформирована теоретическая база для дальнейшего исследования проблематики защиты персональных данных работника, определяя ключевые понятия и нормативные рамки в данной области.

В части, посвященной способам защиты персональных данных, особое внимание было уделено внедрению технических и организационных мер для предотвращения несанкционированного доступа, утечки, изменения или уничтожения информации. Подчеркнута важность регулярного аудита систем защиты и обучения персонала в области информационной безопасности.

В целом, глава 2 подчеркивает, что соблюдение общих требований к работе с персональными данными является ключевым условием обеспечения законности и защиты прав работников в сфере трудовых отношений.

Несоблюдение данных требований может повлечь за собой юридическую ответственность и репутационные риски для работодателя.

Анализ судебной практики выявил существенную проблему в сфере трудовых отношений – значительное количество конфликтов возникает вследствие некорректной работы с персональными данными сотрудников. Статистика показывает, что чаще всего встречаются три основных типа нарушений: несанкционированное использование личной информации работников, несоблюдение требований конфиденциальности и игнорирование установленных регламентов обработки данных.

Проведенное исследование убедительно демонстрирует необходимость модернизации существующей системы правового регулирования в области защиты персональных данных работников. Это обусловлено стремительным развитием информационных технологий и динамичными изменениями в правоприменительной практике. В связи с этим особую актуальность приобретает внедрение комплекса мер, направленных на усиление механизмов защиты личной информации сотрудников и обеспечение их законных прав в данной сфере.

Дальнейшее исследование проблематики может быть направлено на изучение новых технологических решений в области защиты персональных данных, анализ международного опыта регулирования данной сферы и разработку инновационных методов обеспечения информационной безопасности в трудовых отношениях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Проблема защиты персональных данных в условиях цифровизации экономики России / Н. А. Крутова, А. Н. Крутов, О. В. Иванчина, А. Р. Казыева // Вестник СамГУПС. – 2022. – № 4(58). – С. 76-88.

2. Гавриленко, В. А. Вопросы о праве на защиту персональных данных и способах их защиты / В. А. Гавриленко, А. С. Гончаров // Миссия права. Юридическая наука: традиции и инновации : Сборник материалов международной научно-практической конференции студентов, магистрантов, аспирантов и преподавателей, Великий Новгород, 16–17 апреля 2020 года. – Великий Новгород: Новгородский государственный университет имени Ярослава Мудрого, 2021. – С. 58-63.

3. Яковенко, Д. А. Федеральный закон от 27.07.2006 № 152-ФЗ "О защите персональных данных" и риски для бухгалтерии и кадровой службы / Д. А. Яковенко // Вестник профессионального бухгалтера. – 2017. – № 10-12(205-207). – С. 34-92.

4. Кандабарова, Т. С. Защита персональных данных / Т. С. Кандабарова // Трудовое право : Учебное пособие. В 2-х томах / Под общей редакцией Н.А. Соколова. Том 1. – Вологда : Вологодский институт права и экономики Федеральной службы исполнения наказаний, 2022. – С. 139-157.

5. Кузнецова, О. Кто и как отвечает в организации за работу с персональными данными? // Современное делопроизводство. – 2023. – № 10. – URL: (дата обращения: 30.04.2025г.).

6. Тишкович, К. С. Актуальные проблемы обработки персональных данных в трудовых правоотношениях / К. С. Тишкович // Вестник Омского университета. Серия: Право. – 2023. – Т. 20, № 1. – С. 66-74. – DOI 10.24147/1990-5173.2023.20(1).66-74.

7. Ответственность // ГАРАНТ.РУ : информационно-правовой портал. URL: https://www.garant.ru/actual/persona/otvetstvennost/ (дата обращения: 03.05.2025).

8. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3451.

9. Трудовой кодекс Российской Федерации: федер. закон Рос. Федерации от 30 дек. 2001 г. № 197-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 1, ст. 3.

10. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства Рос. Федерации от 15 сент. 2008 г. № 687 // Собр. законодательства Рос. Федерации. – 2008. – № 38, ст. 4323.

11. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3448.

12. Организационное и правовое обеспечение информационной безопасности / Сибирский федеральный университет, Институт космических и информационных технологий. – Красноярск : Сибирский федеральный университет, 2021. – 84 с.

13. Выбор средств защиты персональных данных на предприятии / А. А. Курдюков, Д. О. Морозов, С. В. Посохов, П. С. Шубин // Перспективы науки. – 2023. – № 5(164). – С. 35-39.

14. Летюшев, А. Д. Защита персональных данных / А. Д. Летюшев, Р. Н. Байгуллов // Парадигма. – 2024. – № 2. – С. 43-46.

15. Коршунов, И. Е. Актуальные вопросы защиты персональных данных работников / И. Е. Коршунов // Актуальные проблемы гражданского процесса, трудового права, природоресурсного права : сборник научных и научно-практических статей / под ред. И. В. Рехтиной. – Барнаул : Алтайский государственный университет, 2023. – С. 68-74.

16. Гавриленко, В. А. Вопросы о праве на защиту персональных данных и способах их защиты / В. А. Гавриленко, А. С. Гончаров // Миссия

права. Юридическая наука: традиции и инновации : Сборник материалов международной научно-практической конференции студентов, магистрантов, аспирантов и преподавателей, Великий Новгород, 16–17 апреля 2020 года. – Великий Новгород: Новгородский государственный университет имени Ярослава Мудрого, 2021. – С. 58-63.

17. Сапфирова, А. А. Классификация персональных данных работников и требования к их обработке работодателями / А. А. Сапфирова // Точки научного роста: на старте десятилетия науки и технологии : Материалы ежегодной научно-практической конференции преподавателей по итогам НИР за 2022 г., Краснодар, 12 мая 2023 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2023. – С. 955-957.

18. Защита персональных данных: ключевые аспекты законодательства и практические подходы. – URL: https://hanston.ru/press-centr/zaschita-personalnyh-dannyh-klyuchevye-aspekty-zakonodatelstva-i-prakticheskie-podhody (дата обращения: 20.04.2025г.).

19. Центр подготовки руководителей и специалистов проектного управления в сфере здравоохранения. Курс «Обеспечение безопасности персональных данных на предприятии» – URL: https://cprspb.ru/pages/2025/ppk4pd.html (дата обращения: 25.04.2025г.).

20. Защита персональных данных // PPT.ru. – URL: https://ppt.ru/art/personal-data/zashchita-personalnykh-dannykh (дата обращения: 15.05.2025г.).

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

22. Постановление Правительства РФ от 01.11.2012 № 1119 “Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных” // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6333.

23. Приказ Роскомнадзора от 05.09.2013 № 996 "Об утверждении административного регламента исполнения государственной функции по осуществлению контроля за соответствием обработки персональных данных требованиям федерального закона “О персональных данных” // Российская газета. – 2013. – № 218.

24. Приказ Минтруда России от 24.01.2014 № 33н “Об утверждении Перечня документов по личному составу, необходимых для хранения в целях обеспечения прав и законных интересов граждан” // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2014. – № 15.

Приложение А

УИД 50RS0042-01-2022-005393-37

ВЕРХОВНЫЙ СУД РОССИЙСКОЙ ФЕДЕРАЦИИ

№ 4-КГ23-92-К1

ОПРЕДЕЛЕНИЕ

г. Москва 4 марта 2024 г.

Судебная коллегия по гражданским делам Верховного Суда Российской Федерации в составе

председательствующего Пчелинцевой Л.М.,

судей Вавилычевой Т.Ю. и Киселева А.П.

рассмотрела в открытом судебном заседании 4 марта 2024 г. кассационную жалобу представителя акционерного общества «Научно-производственное предприятие «Исток» им. А.И. Шокина» по доверенности ФИО1 на решение Сергиево-Посадского городского суда Московской области от 23 ноября 2022 г., апелляционное определение судебной коллегии по гражданским делам Московского областного суда от 15 февраля 2023 г. и определение судебной коллегии по гражданским делам Первого кассационного суда общей юрисдикции от 7 августа 2023 г.

по делу № 2-4662/2022 Сергиево-Посадского городского суда Московской области по иску ФИО2 к акционерному обществу «Научно-производственное предприятие «Исток» им. А.И. Шокина» о признании незаконными приказа о привлечении к дисциплинарной ответственности и приказа об увольнении, восстановлении на работе, взыскании среднего заработка за время вынужденного прогула, компенсации морального вреда, о признании неправомерными действий работодателя при обработке персональных данных.

Заслушав доклад судьи Верховного Суда Российской Федерации Пчелинцевой Л.М., объяснения представителей акционерного общества

«Научно-производственное предприятие «Исток» им. А.И. Шокина» по доверенностям ФИО3 и ФИО1, поддержавших доводы кассационной жалобы, возражения на кассационную жалобу представителя ФИО2 по доверенности ФИО4, заключение прокурора Генеральной прокуратуры Российской Федерации Русакова И.В., полагавшего доводы кассационной жалобы обоснованными, обжалуемые судебные постановления подлежащими отмене с направлением дела на новое рассмотрение в суд первой инстанции,

Судебная коллегия по гражданским делам Верховного Суда Российской Федерации

установила:

ФИО2 7 июля 2022 г. обратился в суд с иском, уточненным в порядке статьи 39 Гражданского процессуального кодекса Российской Федерации, к акционерному обществу «Научно-производственное предприятие «Исток» им. А.И. Шокина» (далее также - АО «Исток»), в котором просил признать незаконным приказ от 6 июня 2022 г. № 07/3934 о привлечении его к дисциплинарной ответственности, признать незаконным его увольнение на основании приказа от 6 июня 2022 г. № 389, восстановить его в ранее занимаемой должности заместителя начальника отдела режима, взыскать с ответчика в его пользу средний заработок за время вынужденного прогула в связи с незаконным увольнением за период с 7 июня 2022 г. по день вынесения решения по делу, компенсацию морального вреда в размере 300 000 руб., признать неправомерными действия работодателя при обработке его персональных данных, нарушающие в том числе его честь и доброе имя, а также запрет на сбор и распространение сведений, касающихся его частной жизни и составляющих его личную и семейную тайну.

В обоснование заявленных требований ФИО2 указывал, что он 23 октября 2017 г. был принят на работу в АО «Исток» на должность специалиста и 9 апреля 2018 г. переведен на должность заместителя начальника отдела режима.

15 июля 2021 г. ФИО2 уволен работодателем на основании пункта 2 части первой статьи 81 Трудового кодекса Российской Федерации (сокращение численности или штата работников организации).

Вступившим в законную силу решением Сергиево-Посадского городского суда Московской области от 30 ноября 2021 г. увольнение ФИО2 признано незаконным, он восстановлен в ранее занимаемой должности.

После восстановления на работе, по мнению ФИО2, он подвергся i дискриминационному преследованию со стороны работодателя, которое, в частности, выражалось в недоплате ему пособия по временной нетрудоспособности, необоснованном непредоставлении отпуска и завершилось состоявшимся 6 июня 2022 г. незаконным увольнением за прогул, сопровождающимся нарушением установленной законом :

обязанности о произведении окончательного расчета при увольнении.

Приказом работодателя от 6 июня 2022 г. № 07/3934 ФИО2 привлечен к дисциплинарной ответственности в виде увольнения за прогул, оформленного приказом работодателя от 6 июня 2022 г. № 389.

ФИО2 считал приказ о его увольнении за прогул незаконным, ссылаясь на то, что работодателем не были выяснены причины его отсутствия на рабочем месте и вывод работодателя о неуважительности причин отсутствия ФИО2 на работе является необоснованным.

При этом приказ работодателя о привлечении ФИО2 к дисциплинарной ответственности (от 6 июня 2022 г. № 07/3934) был разослан работникам АО «Исток», что, по мнению ФИО2, привело к распространению его персональных данных.

Решением Сергиево-Посадского городского суда Московской области от 23 ноября 2022 г. исковые требования ФИО2 удовлетворены частично. Суд первой инстанции признал приказ от 6 июня 2022 г. № 07/3934 0 привлечении к дисциплинарной ответственности ФИО2 незаконным, признал приказ от 6 июня 2022 г. № 389 об увольнении ФИО2 с должности заместителя начальника отдела режима на основании подпункта «а» пункта 6

части первой статьи 81 Трудового кодекса Российской Федерации (однократное грубое нарушение работником трудовых обязанностей - прогул) незаконным, восстановил ФИО2 в должности заместителя начальника отдела режима АО «Исток» с 7 июня 2022 г., взыскал с ответчика в пользу ФИО2 заработную плату за время вынужденного прогула с 7 июня по 23 ноября 2022 г. в размере 1 008 523,20 руб. и компенсацию морального вреда в размере 30 000 руб.

В удовлетворении исковых требований ФИО2 о признании неправомерными действий работодателя при обработке персональных данных и взыскании компенсации морального вреда в большем размере отказано.