МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра государственного и муниципального управления

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
Заведующий кафедрой
канд. эконом. наук
_____ А.В. Любаненко
_____ 2023 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

бакалаврская работа

ПОРЯДОК ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНЫХ СЛУЖАЩИХ И МЕХАНИЗМЫ ЕГО СОВЕРШЕНСТВОВАНИЯ

38.03.04 Государственное и муниципальное управление

Профиль «Государственное и муниципальное управление»

Выполнил работу
студент 5 курса
заочной формы обучения — Орлова Янина Сергеевна

Руководитель
(указать ученую степень,
ученое звание) — Трухин Н.В.,
старший преподаватель кафедры
гражданско-правовых дисциплин

Тюмень
2023

Содержание

Введение.....3
Глава 1. Теоретико- методологические основы защиты персональных данных муниципальных служащих.....7
1.1.Понятие и принципы защиты персональных данных.....7
1.2. Правовые механизмы защиты персональных данных муниципальных служащих.....11
1.3. Зарубежная практика в области защиты персональных данных муниципальных служащих.....13
Глава 2. Исследование порядка защиты персональных данных муниципальных служащих Администрации города Муравленко.....28
2.1 Общая характеристика Администрации города Муравленко.....28
2.2. Современный опыт и технологии защиты персональных данных муниципальных служащих.....33
2.3. Оценка эффективности защиты персональных данных муниципальных служащих.....35
Глава 3. Проблемы и пути решения защиты персональных данных муниципальных служащих Администрации города Муравленко.....39
3.1 Проблемы обеспечения защиты персональных данных муниципальных служащих в Администрации города Муравленко.....39
3.2 Оптимизация и совершенствование порядка защиты персональных данных муниципальных служащих в Администрации города Муравленко 42
Заключение.....46
Библиографический список.....48

Введение

В последние годы все большее внимания уделяется вопросам обеспечения сохранности персональных данных граждан. Введённый в силу Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. от 14.07.2022) в 2011–2014 годах был в значительной мере детализирован сразу несколькими подзаконными документами всех основных регуляторов в данной области: Федеральной службы по контролю в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы по промышленному и экспортному контролю и Федеральной службы безопасности Российской Федерации [3].

Регулирование сбора, обработки, а также использования персональных данных является ключевой задачей по обеспечению безопасности личной жизни граждан. С развитием цифровизации и влияния интернета на жизнь людей, увеличилось повсеместное распространение персональных данных о гражданах. В поисковых системах Google или Яндекс, при малом количестве информации о человеке, например, фамилия, имя, примерное место проживание, на некоторых ресурсах можно обнаружить большой список персональных данных, которые добровольно не предоставлялись этим ресурсам. Это часто свидетельствует о том, что гражданин стал жертвой со стороны недобросовестного оператора по обработке персональных данных. Данные действия со стороны недобросовестного оператора по обработке персональных данных, приводят к возможным манипулятивным воздействиям на владельцев персональных данных.

Таким образом, большое количество людей сталкивается с мошенническими действиями, при которых используется личная информация в различных целях, в том числе для искажения существующей информации, тем самым очерняя личность человека. Кража и намеренное распространение персональных данных, становится наиболее острой проблемой не только в России, но и за рубежом. Мошенники, используя скоростное развитие

цифровизации, находят все больше новых способов для получения и продажи личной информации.

Такое нарушение закона имеет место в медицинских учреждениях, банковских сферах, в сфере развлекательных услуг, а так же в государственных и муниципальных органах. В рамках определения группы персональных данных действующим законодательством выделяются отдельные информационные группы, для которых устанавливаются специальные режимы обработки: отдельные категории персональных данных, отражающие национальность, политические взгляды, религиозные или философские убеждения, состояние здоровья и интимную жизнь заинтересованного лица; биометрические собственные данные, отражающие физиологические и биологические возможности человека, на основании которых может быть установлена его личность; публичные персональные данные, изображающие сведения о субъекте персональных данных из общественных источников. Согласно статье 7 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» общедоступной считается информация, доступ к которой не ограничен. К таким общедоступным источникам персональной информации относятся различные руководства, адресные книги, энциклопедии, изданные в печатном или электронном виде, опубликованные в сети Интернет или собранные в библиотеках, архивах, государственных учреждениях и органах местного самоуправления.

У каждого сотрудника есть ряд прав по защите его личных данных. Персональные данные сотрудника обрабатываются в соответствии со статьей 86 ТК РФ. Под подготовкой персональных данных понимается поиск, систематизация, накопление, хранение, уничтожение, использование, распространение, обезличивание, блокирование, уничтожение персональных данных в интересах сотрудника. Сбор, обработка, хранение персональных данных со стороны работодателя требуют письменного согласия со стороны сотрудника государственного или муниципального органа. Передача

персональных данных третьим лицам, если таковое условие не указано в письменном согласии по обработке персональных данных, – запрещена. Исключениями из правил, могут считаться мотивированные запросы на передачу данных из органов исполнительной власти, органов судебной власти и других. Они вправе запрашивать и обрабатывать персональные данные работников в рамках своей компетенции, без согласия субъектов персональных данных. В силу развития цифровизации органам государственной и муниципальной власти требуется размещать информацию о своей деятельности в сети интернет, таким образом, возникают новые аспекты в защите персональных данных работников. Например, принимая во внимание новые изменения в Федеральном Законе «О персональных данных» от 01.03.2021г., работодатель при размещении персональных данных сотрудника на сайте муниципального или государственного органа, должен заключить с работником новое согласие на распространение персональных данных. В ином случае размещение фотографий и имен сотрудников без дополнительного согласия работника может считаться нарушением закона.

Объектом исследования в работе выступает Администрация города Муравленко.

Предметом исследования в работе является порядок защиты персональных данных муниципальных служащих.

Целью данной работы является исследование порядка защиты персональных данных муниципальных служащих.

Задачи:

- изучить понятие и принципы защиты персональных данных;

- выделить правовые механизмы защиты персональных данных муниципальных служащих;

- рассмотреть зарубежную практику в области защиты персональных данных муниципальных служащих;

- проанализировать современный опыт и технологии защиты персональных данных муниципальных служащих;

- оценить эффективность защиты персональных данных муниципальных служащих;

- выявить проблемы обеспечения защиты персональных данных муниципальных служащих в Администрации города Муравленко;

- предложить пути оптимизации и совершенствование порядка защиты персональных данных муниципальных служащих в Администрации города Муравленко.

Теоретическую базу составляют нормативно-правовые акты органов государственной власти, органов местного самоуправления, международные правовые акты.

Методы исследования выпускной квалификационной работы складываются из общенаучных (диалектического, историко-правового методов, методов анализа, синтеза, индукции, дедукции) и специально-юридических (сравнительно-правового и системно-структурного) методов.

Структура выпускной квалификационной работы состоит из: введения, основной части, включающей 3 главы и подразделы, заключения, библиографического списка.

Глава 1. Теоретико-методологические основы защиты персональных данных муниципальных служащих

1.1.Понятие и принципы защиты персональных данных

Использование работодателями персональных данных работников и лиц, устраивающихся на работу обусловлено рядом причин. Во-первых, это предусмотрено законодательством, во-вторых, это необходимо для оказания помощи в отборе на работу, образовании и профессиональной карьере, а также для соблюдения безопасности работающих граждан. Новые способы сбора и обработки данных влекут некоторые риски для работников.

В действующем законодательстве данному аспекту посвящена глава 14 Трудового Кодекса РФ. Стоит отметить, что на сегодняшний день существуют различные национальные законы и международные стандарты устанавливающие обязательные процедуры обработки соответствующих данных, тем не менее, существует необходимость в разработке положений о защите информации, которая касается использования соответствующих данных [1].

Согласно п. 1 ст. 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 14.07.2022) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Понятие «персональные данные», включает в себя такую информацию, как фамилия, имя, отчество работника, его паспортные данные, пол и возраст, семейное положение, наличие детей и родственников [3].

Кроме того, к подобной информации может относиться профессия, социальное, имущественное положение, место жительства. На сегодняшний день достаточно распространены судебные споры об объеме персональных данных, которые вправе собирать и обрабатывать работодатель.

Суды основываются на том, что: «...при определении объема и содержания обрабатываемых персональных данных работника работодатель

должен руководствоваться Конституцией РФ, ТК и иными федеральными законами». То есть работодатель имеет право обрабатывать сведения о паспортных данных, месте проживания и т. д. именно потому, что для этого предусмотрено законное основание. Тем не менее, существует специальная категория персональной информации, которая не подлежат сбору и обработке работодателем. Данное возможно только с исключительного согласия самого работника. Еще одним необходимым условием для получения и обработки подобных данных является связь получаемой информации с трудовыми отношениями.

Соответственно, к таким данным относятся сведения о политических, религиозных и других убеждениях работника, его членстве в общественных объединениях, профсоюзной деятельности. Кроме того, к данной категории относятся сведения о национальности работников.

Так, Арбитражный суд Северо-Кавказского федерального округа признал неправомерным хранение и обработку банком сведений о национальности одного из сотрудников, мотивируя это тем, что для хранение такой информации отсутствует законное основание [9].

Оценка массива существующего законодательства в сфере информационного права, персональных данных, а также доступных материалов специальной литературы и сети Интернет показал, что материалы, относимые к категории персональных данных, могут быть условно разделены на основные группы и определены следующим образом:

1 - персональные данные: ФИО и сведения об их изменении, место, день, месяц и год рождения; фотографическое изображение человека, семейное положение, сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, контактный телефон);

2 - государственные удостоверения личности: паспортные данные; регистрация и фактический адрес проживания; гражданство; индивидуальный налоговый номер; страховой номер индивидуального

лицевого счета застрахованного лица; номер запасного свидетельства пенсионного страхования; данные полиса медицинского страхования; информация о государственных наградах и поощрениях; сведения о воинском учете (специальности воинского учета) [17, с. 87];

3 - данные трудовых взаимоотношений:

- сведения о месте работы (должность, структурное подразделение, категория квалификации, сведения об испытательном сроке работника, период работы, стаж, сведения об аттестации, табельный номер);

- информация о поощрениях и взысканиях;

- сведения о прошлых местах работы и особенностях рабочей деятельности;

- основание прекращения трудового договора (увольнения);

- сведения об отпуске и командировках;

- сведения о временной нетрудоспособности;

- профессиональные данные: образование (название учебного заведения, место и год окончания, наделенная квалификация);

- сведения о повышении квалификации и профессиональной переподготовке;

- сведения о профессиональной пригодности;

- сведения о наличии специальных знаний в определенных сферах;

- сведения о знании иностранных языков; сведения о существовании ученой категории и ученого звания [20, с. 74].

Государственные и муниципальные органы создают государственные или муниципальные информационные системы персональных данных в пределах своих полномочий, но при всем этом они должны руководствоваться требованиями в соотношении с федеральным законодательством. Учитывая, что персональные данные являются одним из видов конфиденциальной информации, совершенствование правовых механизмов, регулирующих и осуществляющих контроль за оборотом персональных данных, совершенствование средств и механизмов защиты

такой информации является актуальной задачей всего государственного аппарата Российской Федерации [15, с. 69].

Для защиты персональных данных используются различные варианты:

- Технические средства. Они являются частью программы мероприятий по защите программного обеспечения от несанкционированного доступа. Для защиты программного обеспечения необходимо привлекать ИТ-специалистов, моделировать угрозы, определять степень защиты персональных данных, обеспечивать надежность.

- Физические средства. Это сокращение доступа к персональным данным для посторонних лиц в виде разрешения работы с информацией только для определенных сотрудников; введение контроля доступа; организация мест хранения данных и др.

- Организационные и юридические меры. Они включает в себя разработку и внедрение руководства по обработке персональных данных компанией, положений о защите данных, издание указов о назначении ответственного лица и осуществление мер контроля [22, с. 205].

В случае правонарушений предусмотрен полный спектр ответственности:

- дисциплинарная – за неправомерную обработку данных сотрудником компании;

- гражданско-правовая – в виде возмещения убытков, возмещения морального вреда;

- административная – если это предусмотрено законом об административных правонарушениях;

- уголовная – за причинение вреда наиболее охраняемым общественным интересам.

Наиболее распространенным наказанием является наложение штрафа. Статья 13.11 Закона об административных преступлениях Российской Федерации устанавливает девять составов правонарушений, в том числе ответственность за обработку данных, если это не предусмотрено законом, в

случае отклонений от целей, поставленных компанией и иных неправомерных действий.

1.2. Правовые механизмы защиты персональных данных муниципальных служащих

Правовая база регулирования обращения с персональными данными муниципального служащего закладывается федеральным законодательством. Статья 29 Федерального закона «О муниципальной службе в Российской Федерации» от 02.03.2007 № 25-ФЗ определяет персональные данные муниципального служащего как информацию, необходимую представителю нанимателя (работодателю) в связи с исполнением муниципальным служащим обязанностей по замещаемой должности муниципальной службы и касающуюся конкретного муниципального служащего [2].

В отношении обработки таковых данных закон делает отсылку к главе 14 Трудового кодекса Российской Федерации (защита персональных данных работника), устанавливая правила ведения личного дела муниципального служащего, аналогичные правилам ведения личного дела государственного гражданского служащего [1].

Получение персональных сведений возможно исключительно от самого работника. Исключение составляет передача таких данных третьим лицом с письменного согласия работника, чьи данные передаются работодателю. Обязанностью работодателя является ознакомление работника с документацией, информирующей его о том, как будут обрабатываться полученные сведения и какими правами и обязанностями он обладает при защите своих персональных данных.

Для того чтобы защитить свои персональные данные за работниками закреплено право на полную информацию об этих данных и их обработке, на свободный бесплатный доступ к этим данным и так далее. В случае

нарушение правил защиты персональных данных работник вправе обратьсяв суд.

Таким образом, перечень прав работника в данной области способствует сохранению точных сведений о нем. За нарушение законодательства о защите персональных данных работника работодатель может быть привлечен к административной ответственности по ст. 13. 11 КоАП РФ, причем ответственной может быть признана как сама организация, так и ее руководитель.

Материальная ответственность работодателя проявляется в его обязанности возместить работнику моральный вред в результате незаконного распространения информации о его персональных данных. Также работодатель несет гражданско-правовую ответственность за причинение работнику имущественного ущерба или морального вреда в результате несоблюдения правил защиты персональных данных: согласно ст. 1068 ГК РФ, юридическое лицо либо гражданин возмещает вред, причиненный его работником при исполнении трудовых (служебных, должностных) обязанностей. Например, за размещение копии паспорта работника на стенде при входе в помещение работодатель был обязан выплатить последнему компенсацию морального вреда.

Для эффективной защиты персональных данных работников необходимо принимать организационно-технические меры. Если сведения хранятся в бумажном виде, то следует обеспечить физическую сохранность данных документов и недоступность ее для посторонних лиц. Если же персональные данные хранятся в электронном виде, необходимо сперва определить уровень защищенности персональных данных. Всего их четыре. На данных параметр влияет количество субъектов персональных данных в определенной организации или характер защищаемых данных (например, биометрические параметры).

От уровня защищенности будет зависеть перечень тех действий, которые необходимо осуществлять для защиты персональных данных.

Например, для обеспечения 1-го уровня защищенности следует создать структурное подразделение организации, которое будет отвечать за защиту данных (или возложить такую обязанность на существующее структурное подразделение).

Заключительным этапом в защите персональных данных является принятие правовых мер. К ним относятся подготовка таких документов, как приказ о назначении лица, ответственного за организацию обработки персональных данных, приказ об утверждении перечня работников, имеющих доступ к персональным данным, соглашение о конфиденциальности с работниками, имеющими доступ к персональным данным, также возможно предусмотреть регламент по работе с персональными данными, детально регулирующий данную деятельность.

1.3. Зарубежная практика в области защиты персональных данных муниципальных служащих

Большинство государств уже приняли некоторые формы защиты этих фундаментальных прав. Так, например, во многих странах мира существуют конституционные нормы, которые предназначены для защиты данных отдельных лиц, предоставляя им право доступа к имеющейся информации о них и предоставляя соответствующим лицам возможность подать жалобу в Конституционный Суд.

В статье 5 Конституции Бразилии 1988 года установлено «Хабеас данные3 предоставляются:

a) для обеспечения информации, касающейся личности заявителя, содержащейся в записях или банках данных государственных учреждений или учреждений публичного характера;

b) для исправления данных, когда заявитель не предпочитает делать это в рамках судебного или административного процесса».

В статье 15 Конституции Колумбии с поправками, внесенными в 1995 году, отмечено, что «все люди имеют право на личную и семейную тайну, неприкосновенность частной жизни и на свою хорошую репутацию, а государство должно уважать и заставлять других уважать эти права.

Аналогичным образом, физические лица имеют право знать, обновлять и исправлять информацию, собранную о них в банках данных и в записях государственных и частных организаций». В апреле 2008 года предлагался проект изменений Конституции Франции, чтобы дополнить перечень фундаментальных прав правом на уважение частной жизни и защиту персональных данных. Хотя поправка не была поддержана, французское законодательство пополнилось нормативным определением персональных данных [22, с. 69].

Несмотря на то, что в странах Европейского Союза исторически давно неприкосновенность частной жизни рассматривается как одно из фундаментальных прав человека, развитие законодательства ЕС в сфере защиты персональных данных и неприкосновенности частной жизни в основном опиралось на соответствующее законодательство США. Хотя имеются существенные отличия в понимании неприкосновенности частной жизни и защиты персональных данных в этих странах. Так, законодательство США широко использует такие термины как «неприкосновенность частной жизни»6 или «информация о частной жизни», европейское законодательство трактует «информацию о частной жизни» как «защиту персональных данных» и рассматривает ее отдельно от права на неприкосновенность. Защита персональных данных фокусируется на том, используются ли данные справедливо и надлежащим образом, в то время как «неприкосновенность подобна афинскому идеалу частной жизни» [21, с. 102].

Ключевой точкой расхождения в понимании неприкосновенности частной жизни между США и Европой стали 1970-е годы. США разработали «Кодекс справедливой информационной практики» («Code of fair information practices») [18, с. 69], которой стал основой современного законодательства о

защите персональных данных, но применили его только к правительству в форме Закона о приватности от 19741 , и к частному сектору только в сфере кредитной отчетности [25, с. 66]. Европейское законодательство использовало и расширило этот кодекс, а впоследствии применило его ко всем уровням и этапам обработки информации – как «по вертикали», то есть от правительства к гражданину, так и «по горизонтали» – от бизнеса до гражданина. К 1990 году Европейская комиссия опасалась, что различные национальные законы о защите данных будут препятствовать внутреннему рынку в ЕС3 . В том же году было опубликовало предложение по Директиве о защите данных (Data Protection Directive), принятое после пяти лет переговоров (в 1995 году)4 . Данный документ установил общий режим, основанный на Кодексе справедливой информационной практики (FIP), который применялся к большей части частного и государственного сектора (с некоторыми исключениями)5 . Директива требовала от государств-членов принятия соответствующего имплементирующего законодательства [19, с. 69]. Действие директивы сопровождалось значительными сложностями, так как она не полностью гармонизировала национальные законы в сфере неприкосновенности частной жизни.

Даже внутри Европы страны вели себя оппортунистически, пытаясь привлечь к суду крупные технологические компании с признаками слабого правоприменения и выгодных налоговых схем (например, закон о защите данных в Ирландии). Даже среди стран, приверженных неприкосновенности частной жизни и защиты персональных данных, правоприменение было достаточно слабым (например, в 2017 году Франция оштрафовала Facebook6 на 150 000 евро, можно сравнить со штрафами в 5 млрд долларов того же Facebook в США). Этот пробел в правоприменительной практике закрепил за европейскими регуляторами репутацию региона с хорошо прописанными правилами, но без реальной полицейской деятельности. В этой связи представляется, что разработка Регламента GDPR – это, прежде всего, попытка ЕС устранить эти и другие недостатки, которая зародилась в

процессе, совершенно не похожем на законодательные усилия США. Европейские политики запустили деятельность, которая включала множество экспертных консультаций, глубокое понимание процессов обработки информации. Консультации начались в 2009 году, текст предложения был опубликован Европейской комиссией в 2012 году [23, с. 52]. Два года спустя Европейский парламент принял компромиссный текст, основанный на почти 4000 предложенных поправок.

Совет Европейского Союза опубликовал свое предложение об Общем регламенте о защите данных (GDPR) в 2015 году, чтобы начать переговоры с Европейским парламентом8 . В декабре 2015 года парламент и Совет достигли договоренности по тексту Регламента GDPR и он был официально принят в мае 2016 года и применяется с мая 2018 года. Толкование GDPR поручено судам, в частности, Суду Европейского Союза (CJEU) вместе с предложениями и рекомендациями Европейского совета по защите данных (European Data Protection Board). Стоит отметить ряд драматических решений, вынесенных данными органами, касающихся неприкосновенности частной жизни, включая отмену обязательств по хранению данных, отмену соглашения США и ЕС о безопасной гавани и предоставление людям при определенных условиях «права быть забытыми» (право на забвение)[20, с. 69].

Как и в Директиве 1995 года, в первой статье GDPR подчеркивается, что GDPR преследует двойную цель – содействовать свободному потоку персональных данных в ЕС (чтобы помочь бизнесу) и защищать людей и их персональные данные. В то же время Регламент GDPR установил регуляторную среду, более неблагоприятную для ИТ-отраслей (особенно связанных с обработкой больших данных и машинного обучения) [17, с. 66] относительно Соединенных Штатов Америки. Рассмотрим основные положения общего регламента защиты данных Европейского Союза. Отметим, что для его разработки авторы изучали современные стандарты информационной безопасности, методы защиты информационной индустрии

и даже академическую литературу по передовым способам идентификации и аутентификации. По этой и другим причинам GDPR имеет чрезвычайно широкий охват по многим аспектам информационной безопасности.

Одним из базовых определений GDPR, наряду с персональными данными, является «обработка» персональных данных6 , которая охватывает весь «жизненный цикл» данных – от их создания до удаления и даже использование данных для раскрытия других данных. Что касается дальнейшего развития этого понятия, то Privacy International предлагает включение в него такого термина как «генерация данных» Это вид деятельности, который до сих пор не был четко прописан ни в одном законе о защите данных и который должен регулироваться и контролироваться, то есть отдельным лицам должна быть предоставлена защита в рамках этого способа обработки.

Данное предложение основано на анализе компании Privacy International проблем «эксплуатации (использования) данных», которые зачастую начинаются с чрезмерной генерации, поскольку именно этот процесс является предварительным условием для дальнейшей обработки. Чрезмерное генерирование данных пользовательскими информационно-коммуникационными системами наряду с такими первичными причинами, как недостаточная осведомленность, прозрачность и подотчетность, приводит к основной проблеме дисбаланса власти в цифровом мире. Это дополнение к определению «обработки» будет несколько расширять «принцип ограничения использования» и концепцию «минимизации данных» [14, с. 114].

Подотчетность и правоприменение являются ключом к успеху защиты персональных данных. В законе о защите персональных данных должны быть четко указаны стороны, ответственные за соблюдение закона, а также их функции и обязанности. Со временем произошла эволюция терминологии, используемой для обозначения лиц, ответственных за обработку персональных данных. Хотя терминология варьируется в зависимости от

правового поля страны, существует два объекта, которые контролируют персональные данные (контроллеры данных) и/или обрабатывают данные (процессоры данных)[12, с. 87].

Например, если компания Y собирает и анализирует данные опросов клиентов компании X в соответствии с инструкциями компании X, компания X является контроллером, а компания Y – процессором данных. Если две организации будут совместно определять, почему и как будут обрабатываться персональные данные, они будут рассматриваться как совместные контролеры данных, обладать соответствующими полномочиями и нести ответственность. В свою очередь, в США именно субъекты данных должны читать и критически оценивать уведомления о приватности, а также делать выбор на рынке, основываясь на тщательном исследовании и наблюдении [21, с. 52]. Европейские законодатели отвергают этот подход и возлагают ответственность на контроллеров. Процессоры данных, такие как дата-центры или провайдеры облачных услуг, должны соответствовать большинству норм Регламента GDPR. Если процессоры данных нарушают GDPR, то контроллер данных будет считаться ответственным. В то же время Регламент GDPR пытается предотвратить некоторые проблемы типа «принципал-агент» с процессорами данных, а именно требует, чтобы контроллеры гарантировали, что процессоры данных компетентны и ответственны. Для установления цепочки подотчетности процессоры данных не могут заключать субконтракты без согласия контроллера данных (GDPR, ст. 29).

Регламент GDPR применяется к автоматизированным данным и автоматизированной обработке данных, а также к структурированным форматам хранения рукописных данных, то есть он охватывает любую обработку данных на компьютере, телефоне, устройстве IoT, а также на бумажных носителях. Сфера применения GDPR ограничена в двух отношениях. Во-первых, простое ознакомление с GDPR говорит о том, что мы все постоянно нарушаем GDPR в своей личной жизни, когда мы

«обрабатываем» «личные данные» наших друзей, отправляя им электронные письма или «помечая их» на фотографии. Чтобы сфокусировать внимание регуляторов на компаниях и организациях, а не на простых людях, GDPR исключает операции с данными для «чисто личной или семейной деятельности». (GDPR, ст. 2(2)(c)).

Преамбула GDPR показывает, что «переписка и хранение адресов или социальные сети» являются примером ситуации, которая подпадает под данное исключение. (GDPR, rec 18). Например, если кто-то отправляет электронное письмо другу, в котором он пишет о своем племяннике, это обычно не подпадает под GDPR. Но исключение достаточно узкое. Суд Европейского Союза (CJEU) постановил, что когда прилежащая территория дома снимается на видеокамеру, прикрепленную к дому, с целью выявления грабителей, это не будет считаться «чисто личной или домашней деятельностью».

Во-вторых, GDPR не регулирует национальную безопасность. Национальная безопасность, предотвращение и преследование уголовных преступлений в значительной степени выходят за рамки компетенции ЕС (GDPR, ст. 23; GDPR, rec 73). Национальные государства-члены не решаются отдать такие полномочия ЕС. Директива, которая вступила в силу одновременно с GDPR, устанавливает правила обработки данных правоохранительными органами, такими как полиция. Правила этой Директивы допускают больше ограничений, чем общие рамки, предусмотренные GDPR [26, с. 87].

GDPR действительно применяется к обработке данных другими правительственными организациями, хотя это позволяет правительствам принимать специальные режимы в своих национальных законах (GDPR, ст. 23; GDPR, rec 73). Кроме того, GDPR признает, что фундаментальное право на защиту данных может вступать в противоречие с основными правами и другими общественными интересами, такими как открытость

государственных структур, свобода слова и обработка данных для целей архивирования.

В Европе свобода слова является фундаментальным правом наравне с неприкосновенностью частной жизни [17, с. 69], тогда как в США свобода слова, как правило, превосходит неприкосновенность частной жизни, когда две ценности находятся в конфликте. Кроме того, правительства очень часто вводят дополнительные исключения по обязательствам защиты прав личности.

Наиболее частыми причинами являются: национальная безопасность и оборона; общественная безопасность; предупреждение, расследование, выявление или судебное преследование по уголовным преступлениям; общественные интересы; иммиграция; экономические или финансовые интересы, включая бюджетные и налоговые вопросы; общественное здоровье и безопасность; защита судебной независимости и судопроизводства; контрольные, инспекционные или регулирующие функции, связанные с осуществлением официальных полномочий в отношении безопасности, обороны, других важных общественных интересов или предупреждения преступности; защита личности или прав и свобод других; обеспечение соблюдения гражданских прав.

Общие исключения не могут быть оправданы и должны применяться только в ограниченных случаях. При этом любые исключения должны:

– быть четко определены и установлены законом;

– уважать основные права и свободы человека;

– являются необходимыми и пропорциональными мерами в демократическом обществе;

– применимы только в тех случаях, когда их отсутствие наносит ущерб законной цели.

Таким образом, важно обеспечить, чтобы любые исключения из закона о защите персональных данных должны быть четко изложенными, точными и недвусмысленными, обнародованными и узко интерпретированными в

соответствии с принципами необходимости и соразмерности. Такой подход к исключениям позволит гарантировать, что средства защиты, предусмотренные в законе о защите данных, не будут избыточными по отношению к функциям органов безопасности и разведки. Неспособность правильно определить и ограничить эти исключения подорвет доверие общественности к защите персональных данных. Что касается принципов защиты персональных данных в GDPR, то они напоминают принципы, разработанные США в «Кодексе справедливой информационной практики» (FIP).

В GDPR и FIP сформулированы шесть принципов высокого уровня, которые должны учитывать контроллеры и процессоры данных. Во-первых, принцип законности, справедливости и прозрачности определяет основную норму закона о защите данных: персональные данные должны обрабатываться «законно, справедливо и прозрачно в отношении субъекта данных» (GDPR, ст. 5(1)(a)). Требование законности достаточно ясно: обработка персональных данных должна соответствовать требованиям GDPR и других законов. Требование справедливости (fairness)3 можно сравнить с общим требованием о добросовестности (good faith) в некоторых правовых системах [17, с. 55].

Во-вторых, принцип ограничения цели предполагает, что персональные данные «собираются для определенных, явных и законных целей и не обрабатываются способами несовместимыми с этими целями». Этот принцип также включен в Хартию ЕС2 . Цель обработки должна быть определенной и конкретной. Запрещены неопределенные и абстрактные цели, такие как «содействие удовлетворенности потребителя», «разработка продукта» или «оптимизация услуг». Например, когда служба доставки пиццы запрашивает адрес потребителя, чтобы доставить пиццу, – цель определена и конкретна. В целом, чтобы оценить, совместима ли новая цель с первоначальной целью, контроллер данных должен рассмотреть, например, связь между первоначальными и новыми целями, контекст, разумные ожидания субъекта

данных, характер и чувствительность данных, последствия предполагаемой дальнейшей обработки для субъектов данных. GDPR не считает дальнейшую обработку несовместимой с первоначальными целями, если дальнейшая обработка происходит в целях архивирования в общественных интересах, научных или исторических исследований или в статистике.

Тем не менее GDPR требует дополнительных гарантий для такой дальнейшей обработки. Ограничение по цели использования в некоторой степени угрожает отраслям, интенсивно работающим с данными, поскольку компании зачастую находят полезность этих данных, используя их непредсказуемым образом.

Действительно, самой целью машинного обучения является обнаружение паттернов, не ожидаемых или даже не воспринимаемых людьми. Хотя многие сторонники больших данных считают, что принцип ограничения цели устарел и его следует отменить, GDPR сохранил этот принцип. Следовательно, в этом вопросе ЕС сделал политический выбор в пользу неприкосновенности частной жизни и защиты персональных данных. В-третьих, принцип минимизации данных означает, что персональные данные должны быть «адекватными, актуальными и ограниченными целями их обработки» (GDPR, ст. 5(1) (c)). В преамбуле добавлено, что «персональные данные должны обрабатываться только в том случае, если цель обработки не может быть достигнута другими средствами». Могут быть получены только те данные, которые необходимы для конкретной цели обработки.

Например, служба доставки пиццы не должна собирать данные о религиозных или политических взглядах людей – такие данные не нужны для доставки пиццы.

Таким образом, принцип минимизации данных запрещает сбор большего количества персональных данных, поскольку эти данные могут быть полезны в будущем. В-четвертых, принцип точности требует, чтобы персональные данные были «точными и, при необходимости, обновлялись»

(GDPR ст. 5(1)(d)). Контроллеры данных должны предпринимать «разумные действия (…) и гарантировать, что персональные данные, которые являются неточными, с учетом целей их обработки, незамедлительно стираются или исправляются» (GDPR, ст. 5(1)(d)).

Таким образом, принцип точности не столько требует достижения полной точности, сколько точности «с учетом целей обработки персональных данных» (GDPR, ст. 5(1)(d)). Контроллеры данных должны заблаговременно обеспечивать надлежащую точность и предоставлять субъектам данных возможность их исправления. (GDPR, ст. 16). В-пятых, помимо минимизации данных, Регламент GDPR жестко ограничивает их хранение. «Персональные данные должны… храниться в форме, позволяющей идентифицировать субъекты данных не дольше, чем это необходимо для целей их обработки; Персональные данные могут храниться в течение более длительных периодов, если подразумевается их обработка исключительно для целей архивирования в общественных интересах, научных или исторических исследованиях, статистики в соответствии со ст. 89 (1) GDPR при условии выполнения соответствующих технических и организационных мер» (GDPR, ст. 5(1)(e)).

Принцип навязывает стандарт «не дольше, чем необходимо». В преамбуле добавлено, что контроллеры данных должны заранее установить временные ограничения для запланированного удаления. Так, например, служба доставки пиццы не должна хранить адреса клиентов в течение неоправданно длительного периода. Близким к идеалу будет удаление адреса после доставки пиццы, но пиццерия зачастую хранит адрес в течение нескольких месяцев, чтобы сэкономить постоянным клиентам время заказа пиццы.

В-шестых, принцип целостности и конфиденциальности налагает ответственность за безопасность данных. Безопасность должна быть «адекватной» и защищать от потери, уничтожения, повреждения и незаконной обработки, поэтому внутреннее использование данных может

являться нарушением безопасности. Ответственность контролеров и процессоров данных. Регламент GDPR усиливает роль контроллера данных как стороны, ответственной за данные, и налагает более строгий контроль, обязанности и ответственность на процессоры данных. Это произошло потому, что в соответствии с Директивой ЕС по защите данных, некоторые компании пытались избежать ответственности за защиту персональных данных и неприкосновенность частной жизни, объявив себя «процессорами», одновременно участвуя в принятии решений, подобно контроллеру данных.

В отличие от Директивы, которая предоставила государственным надзорным органам и органам по защите данных большие полномочия и функционал в мониторинге и соблюдении правил, регламент GDPR возлагает основные надзорные и контрольные полномочия на контроллеры данных

Таким образом, анализ основных положений регламента GDPR, позволяет говорить о том, что этот документ, прежде всего, – расширение и уточнение требований, установленных Директивой о защите данных 1995 года. Стабильным является ядро закона о защите данных, а также основные принципы, подобные принципам справедливой информации в США. Однако GDPR привносит и значительные изменения, особенно в понимании персональных данных и методах их обработки, интегрирует персональные данные в сложный, комплексный защитный режим регулирования, который будет иметь серьезные последствия.

Например, GDPR побуждает компании тщательно продумывать свои методы работы с персональными данными, заставляет их серьезно относиться к конфиденциальности, поощряет проверять поставщиков услуг на предмет соответствия правилам. Еще одно новшество заключается в том, что GDPR повышает уровень конфиденциальности и приватности сотрудников в организациях. Кроме того, GDPR скептически относится к правовому инструменту «информированного согласия», подчеркивает важность точных данных и предоставляет людям право на доступ и исправление данных. Основным недостатком регламента GDPR является его

объем и сложность: 99 подробных положений. Его влияние на справедливость и уважение к основным правам, можно оценить только через некоторое время. Вместе с тем Европейская комиссия начала свой следующий проект по неприкосновенности частной жизни и защиты персональных данных. Комиссия опубликовала предложение по Регламенту ePrivacy (ePrivacy Regulation), которая должно заменить предыдущий документ (ePrivacy Directive).

Предложение включает в себя правила защиты конфиденциальности сообщений в Интернете, а также правила, касающиеся файлов cookie и отслеживания в Интернете [26, с. 9]. Представляется, что законотворческая деятельность над правилами справедливой обработки персональных данных никогда не будет закончена, подобно законодательству о защите прав потребителей или природопользовании и экологии, правила будут постоянно обновляться и дополняться, чтобы адаптироваться к новым обстоятельствам и условиям цифрового мира.

Таким образом, законодательная база ЕС в сфере обеспечения неприкосновенности частной жизни и защиты персональных данных и ее значительное обновление в 2018 году представляют собой достаточно четкий перечень положений и норм. Они обеспечивают в нужной мере доверие со стороны граждан стран ЕС. Что не менее важно, с другой стороны, они создают условия для представителей бизнеса максимально использовать возможности на едином европейском цифровом рынке. Последние новации законодательства ЕС в сфере защиты персональных данных и неприкосновенности частной жизни позволяют сделать вывод о том, что существует сильная приверженность защите персональных данных и неприкосновенности частной жизни в Европе. Поэтому Регламент GDPR выполняет конституционные обязательства, которые настолько глубокие, что занимают центральное место в понимании нового значения государственных органов и частных компаний в информационную эпоху.

Представляется, что законотворческая деятельность над правилами справедливой обработки персональных данных как в ЕС, так и в других странах никогда не будет закончена. Подобно законодательству о защите прав потребителей или природопользовании и экологии, регуляторы защиты персональных данных и неприкосновенности частной жизни будут постоянно обновляться и дополняться, чтобы адаптироваться к новым обстоятельствам и условиям цифрового мира. Наглядно в этом можно убедиться при анализе мер, которые применяются странами при преодолении пандемии COVID-19. Так, после прохождения пандемии и в ЕС, и в России необходимо будет урегулировать все те изменения, которые де-факто были введены в условиях пандемии, в частности: – регулирование баланса личной свободы и общественной безопасности при применении цифровых моделей отслеживания и контроля, использования цифрового профиля; – правосубъектность цифровых платформ и цифровых решений (сервисы дистанционного образования, электронный суд и т. д.); – регулирование рисков утечки данных, нарушения прав на использование программного обеспечения вследствие удаленной работы из дома.

Также необходимо внести изменения в алгоритм доверия контрагентам, использовать новые модели верификации, законодательно закрепить правила новой электронной торговли, защищать цифровой профиль. Все это потребует особого внимания к неприкосновенности частной жизни и защите персональных данных. Завершая, вернусь к главному тезису: «правомерность» ожидания неприкосновенности личной жизни и доступа к персональным данным есть процесс уравновешивания общественного и частного интересов в праве. Правовое регулирование в странах Европейского Союза сферы неприкосновенности частной жизни и защиты персональных данных, в особенности регламент GDPR, свидетельствует о новом этапе развития законодательства и правоприменительных процедур в этой сфере, который значительно повлияет на государственную информационную политику всех стран мира, заставит изменить существующие подходы к

защите персональных данных и, в целом, подтверждает выводы о том, что персональные данные – это «валюта» современной экономики, их сбор, анализ и использование имеют огромное социальное, экономическое и политическое значение.

Таким образом, персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу.

Для эффективной защиты персональных данных работников необходимо принимать организационно-технические меры. От уровня защищенности будет зависеть перечень тех действий, которые необходимо осуществлять для защиты персональных данных.

Для защиты персональных данных используются различные варианты: технические средства (являются частью программы мероприятий по защите программного обеспечения от несанкционированного доступа); физические средства (сокращение доступа к персональным данным для посторонних лиц в виде разрешения работы с информацией только для определенных сотрудников); организационные и юридические меры (включает в себя разработку и внедрение руководства по обработке персональных данных компанией, положений о защите данных, издание указов о назначении ответственного лица и осуществление мер контроля).

Глава 2. Исследование порядка защиты персональных данных муниципальных служащих Администрации города Муравленко

2.1 Общая характеристика Администрации города Муравленко

Администрация города является исполнительно-распорядительным органом местного самоуправления муниципального образования город Муравленко, наделенным полномочиями по решению вопросов местного значения и полномочиями для осуществления отдельных государственных полномочий.

Руководство Администрацией города на принципах единоначалия осуществляет Глава города.

Структура Администрации города утверждается решением Городской Думы по представлению Главы города.

Администрация города обладает правами юридического лица.

Юридический адрес Администрации города: 629603, Тюменская область, Ямало-Ненецкий автономный округ, город Муравленко, улица Ленина, дом 80.

Администрация города осуществляет полномочия по решению вопросов местного значения в следующих сферах:

- в области комплексного социально-экономического развития территории;

- в области бюджета, финансов и учета;

- в области управления имуществом, находящимся в муниципальной собственности;

- в области содействия развитию малого и среднего предпринимательства;

- в области использования земель, других природных ресурсов и охраны окружающей среды;

- в области строительства и транспорта;

- в области жилищного хозяйства, коммунально-бытового обслуживания населения;

- в области образования, здравоохранения, физической культуры и спорта;

- в области сохранения исторических и культурных памятников, развития культуры, местных традиций и обычаев;

- в области обеспечения законности, правопорядка, охраны прав и свобод граждан.

В соответствии с законами Российской Федерации и законами автономного округа Администрация города осуществляет отдельные государственные полномочия.

Администрация города в области комплексного социально-экономического развития территории муниципального образования:

- разрабатывает проект стратегии социально-экономического развития муниципального образования;

- реализует стратегию социально-экономического развития муниципального образования;

- разрабатывает программы комплексного развития систем коммунальной инфраструктуры, программ комплексного развития транспортной инфраструктуры, программ комплексного развития социальной инфраструктуры муниципального образования;

- осуществляет привлечение материальных и финансовых ресурсов иных собственников для реализации стратегии социально-экономического развития муниципального образования;

- координирует деятельность муниципальных предприятий и учреждений по реализации стратегии социально-экономического развития муниципального образования;

- поддерживает инновационную деятельность на территории муниципального образования;

- осуществляет иные полномочия, предусмотренные законодательством Российской Федерации, законами автономного округа, иными нормативными правовыми актами органов местного самоуправления.

В структуру администрации муниципального образования города Муравленко входят (см. рисунок 2.1.)

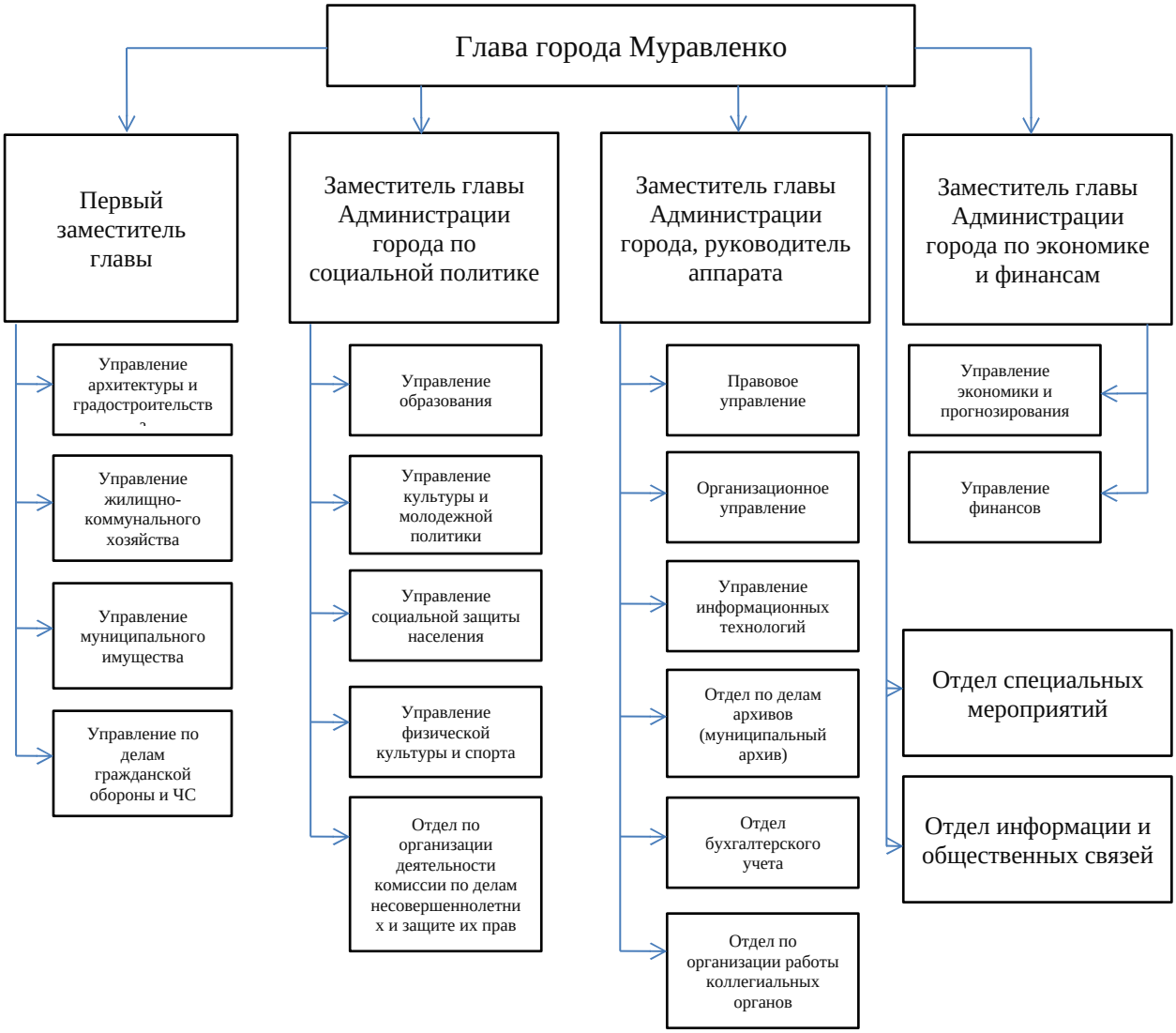

Рисунок 2.1. – Структура Администрации города Муравленко

Структуру органов местного самоуправления муниципального образования города Муравленко составляют:

- глава муниципального образования - глава муниципального образования города Муравленко;

- представительный орган муниципального образования - окружной Совет депутатов муниципального образования города Муравленко;

- исполнительно-распорядительный орган муниципального образования - администрация муниципального образования города Муравленко города Муравленко.

В непосредственном подчинении главы города находятся первый заместитель главы Администрации города, заместитель главы Администрации города по социальной политике, заместитель главы Администрации города, руководитель аппарата, заместитель главы Администрации города по экономике и финансам, а так же 2 структурных подразделения: отдел информации и общественных связей и отдел специальных мероприятий

Численность работников администрации на конец 2021 года составляет 28 человек.

Сотрудники администрации, являющиеся муниципальными служащими, в своей деятельности руководствуются также федеральным законодательством и законодательством Тюменской области о муниципальной службе, Кодексом этики и служебного поведения муниципальных служащих города Муравленко, общими принципами профессиональной служебной этики и основными правилами служебного поведения государственных и муниципальных служащих.

Администрация в соответствии с Конституцией Российской Федерации, Федеральным законом «Об общих принципах организации местного самоуправления в Российской Федерации» решает вопросы непосредственного обеспечения жизнедеятельности населения муниципального образования города Муравленко.

Глава администрации руководит деятельностью администрации на принципах единоначалия.

Исполнительные функции глава администрации осуществляет путем издания распорядительных документов. Порядок подготовки распорядительных документов и их исполнения определяются регламентом.

В случае отсутствия главы администрации его полномочия осуществляет первый заместитель (заместитель) главы администрации.

Структурные подразделения администрации с правом юридического лица имеют свои печати, соответствующие бланки и штампы. Отделы администрации без права юридического лица могут иметь собственные печати, бланки и штампы для внутреннего пользования.

Для характеристики деятельности Администрации города Муравленко проанализируем основные социально-экономические показатели муниципального образования (см. таблицу 2.1.).

Таблица 2.1. – Основные социально-экономические показатели деятельности муниципального образования города Муравленко

Показатели	Ед. измерения	2021
Общая площадь земель муниципального образования	гектар	1943,35
Общее протяжение освещенных частей улиц, проездов, набережных и т.п.	километр	24,2
Общая протяженность улиц, проездов, набережных (на конец отчетного года), километров	километр	30,1
Среднесписочная численность работников муниципальных организаций и предприятий	человек	259
Фонд заработной платы всех работников муниципальных организаций и предприятий	тысяча рублей	71349,55
Количество объектов розничной торговли и общественного питания	Единица	61
Общее число семей, получавших субсидии на оплату жилого помещения и коммунальных услуг на конец года	Единица	87
Число муниципальных дошкольных образовательных учреждений на конец отчетного года	Единица	2
Число муниципальных учреждений культурно-досугового типа (с учетом библиотечного отделения)	Единица	1

В настоящее время город Муравленко представляет собой специализированный промышленный центр с рекреационными функциями.

На территории муниципального образования кроме муниципальных предприятий, организаций и учреждений, две автозаправочные станции, два охранных предприятия, отделения почтовой связи, представительство Управления Пенсионного Фонда, межрайонная ИФНС России, отдел ЗАГС, действуют церкви с воскресной школой, действуют 606 организаций и индивидуальных предпринимателей.

Осуществляют свою деятельность бюджетное учреждение социального обслуживания «Комплексный центр», ОГУ «Центр социальной поддержки», Отделение помощи семье, женщинам и детям Областное государственное учреждение социального обслуживания «Центр социальной помощи семье и детям». Имеется пожарная часть.

2.2. Современный опыт и технологии защиты персональных данных муниципальных служащих

Особенности обработки персональных данных «на местах» раскрываются в муниципально-правовых актах, форма и содержание которых определяются муниципальными образованиями самостоятельно.

В качестве примера можно привести тот факт, что города Муравленко действует Положение об обработке персональных данных администрации муниципального района (далее – Политика). Помимо данной Политики при рассмотрении заявленной темы представляет интерес также Распоряжение Администрации города Муравленко «О принятии мер по совершенствованию системы защиты информации» от 29.04.2014 №159-р.

В соответствии со статьей 5 Федерального закона «О персональных данных» обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Исходя из этого требования, Политика применительно к муниципальным служащим закрепляет такие цели обработки их персональных данных, как:

– регистрация и учет работников и муниципальных служащих, обеспечение соблюдения законов и иных нормативных правовых актов, содействие работникам в трудоустройстве, получение образования, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества;

– соблюдение порядка и правил приема на работу, установленных ТК РФ, порядка и приема на муниципальную службу;

– регистрация и учет лиц, с которыми заключены договора.

Вслед за Федеральным Законом «О персональных данных» от 27.07.2006 № 152-Ф Политика приводит основные понятия, даваемые которым определения дословно совпадают с закрепленными в Федеральном Законе. В качестве Оператора по обработке персональных данных муниципальных служащих выступает Администрация. Конкретного перечня разновидностей персональных данных, которые могут обрабатываться Оператором (например, имя, фамилия, серия и номер паспорта) политика не содержит. Однако стоит отметить, что таковой обработке могут подвергаться не только данные самих муниципальных служащих, но и их ближайших родственников – указание на это содержится в таком документе, как

Политика обработки персональных данных распространяется на все персональные данные, как обрабатываемые при помощи средств автоматизации, так и без нее.

В целях автоматизации обработки персональных данных в Администрации применяются такие информационные системы персональных данных, как «1С: Предприятие», «1С: Зарплата+кадры», «Парус Заработная плата Кадры+Бухгалтерия», «Spu_orb». Особо регламентируется обращение со съемными носителями информации (каковым, в соответствии с Положением об учете и хранении съемных носителей конфиденциальной информации (персональных данных) в Администрации города Муравленко является любой материальный объект, используемый для хранения и передачи электронной информации). Несмотря

на название документа, помимо правил учета и хранения съемных носителей он содержит требования к их использованию и уничтожению.

Таким образом, обработка персональных данных муниципальных служащих в Администрации города Муравленко организована в соответствии со всеми требованиями, которые предъявляет к осуществлению обработки персональных данных федеральное законодательство. Непосредственные же обязанности по учету съемных носителей, организации мероприятий по защите персональных данных возложены на должностных лиц отдела информационных технологий.

2.3. Оценка эффективности защиты персональных данных муниципальных служащих

В деятельности Администрации города Муравленко сформирован механизм по защите персональных данных муниципальных служащих, главным элементом которого выступает Комиссия по соблюдению требований к служебному поведению и урегулированию конфликта интересов (аттестационная комиссия).

Основными задача и комиссии являются:

1) обеспечение соблюдения муниципальными служащими администрации муниципального образования города Муравленко ограничений и запретов, требовании о предотвращении или урегулировании конфликта интересов, а также обеспечение исполнения ими обязанностей;

2) осуществление в администрации муниципального образования города Муравленко мер по предупреждению коррупции.

Основаниями для проведения заседания комиссии являются:

- Представление главой администрации, любым членом комиссии, муниципальным служащим или непосредственным руководителем муниципального служащего материалов и иной информации, свидетельствующих:

- о представлении муниципальными служащими недостоверных или неполных сведений о доходах, об имуществе и обязательствах имущественного характера, его самого, его супруги и несовершеннолетних детей;

- о несоблюдении муниципальным служащим требований к служебному поведению и требований об урегулировании конфликта интересов;

- Поступившие в комиссию через общий отдел администрации:

- обращение гражданина, замещавшего должность муниципальной службы, включенную в перечень должностей, утвержденный муниципальным правом актом администрации о даче согласия на замещение до истечения двух лет со дня увольнения с муниципальной службы на условиях трудового договора должности в организации и выполнение в течение месяца в данной организации работ стоимостью более 100 тысяч рублей на условиях гражданско-правового договора, если отдельные функции муниципального управления данной организацией входили в его должностные обязанности;

- заявление муниципального служащего о невозможности по объективным причинам представить сведения о доходах (расходах) своих, супруги и детей;

- уведомление муниципального служащего о возникновении личной заинтересованности при исполнении должностных обязанностей, которая приводит или может привести к конфликту интересов.

Состав комиссии утвержден Распоряжением Администрации муниципального образования города Муравленко № 58 от 15.02.2020 года.

Количество заседаний комиссии по соблюдению требований к служебному поведению и урегулированию конфликта интересов за период с 2017 по 2021 год представлено в таблице 2.2.

Таблица 2.2. - Количество заседаний по соблюдению требований к служебному поведению и урегулированию конфликта интересов в Администрация муниципального образования города Муравленко

Год	Всего заседаний	Даты
2017	3	15.05.2017 12.07.2017 15.11.2017
2018	4	19.01.2018 05.07.2018 11.09.2018 11.12.2018
2019	2	15.02.2019 05.04.2019
2020	3	12.02.2020 11.07.2020 14.08.2020
2021	1	25.02.2021

По результатам проведенных заседаний нарушений в сфере защиты персональных данных муниципальных служащих не было выявлено.

Таким образом, в качестве объекта исследования в работе выступает Администрация муниципального образования города Муравленко - исполнительно-распорядительный орган муниципального образования. В структуру администрации муниципального образования города Муравленко входят: юридический отдел, отдел по мобилизационной работе и безопасности, отдел по финансам, бюджету и бухгалтерскому учету, отдел градостроительства, архитектуры и инвестиций, отдел социальной поддержки населения и здравоохранения, отдел образования, культуры, туризма и спорта, общий отдел, ЗАГС, комиссия по делам несовершеннолетних. Численность работников администрации на конец 2021 года составляет 28 человек.

В деятельности Администрации города Муравленко сформирован целый механизм по защите персональных данных муниципальных служащих в виде Комиссии по соблюдению требований к служебному поведению и урегулированию конфликта интересов (аттестационная комиссия).

Глава 3. Проблемы и пути решения защиты персональных данных муниципальных служащих Администрации города Муравленко

3.1 Проблемы обеспечения защиты персональных данных муниципальных служащих в Администрации города Муравленко

На первое место встают проблемы защиты персональных данных муниципальных служащих на уровне муниципалитета, обусловленные введением ограничительных мероприятий, связанных с распространением новой коронавирусной инфекции.

Рассмотрим, как изменилось количество проведенных заседаний Комиссии по соблюдению требований к служебному поведению и урегулированию конфликта интересов за период с 2018 по 2021 год (см. рисунок 3.1.).

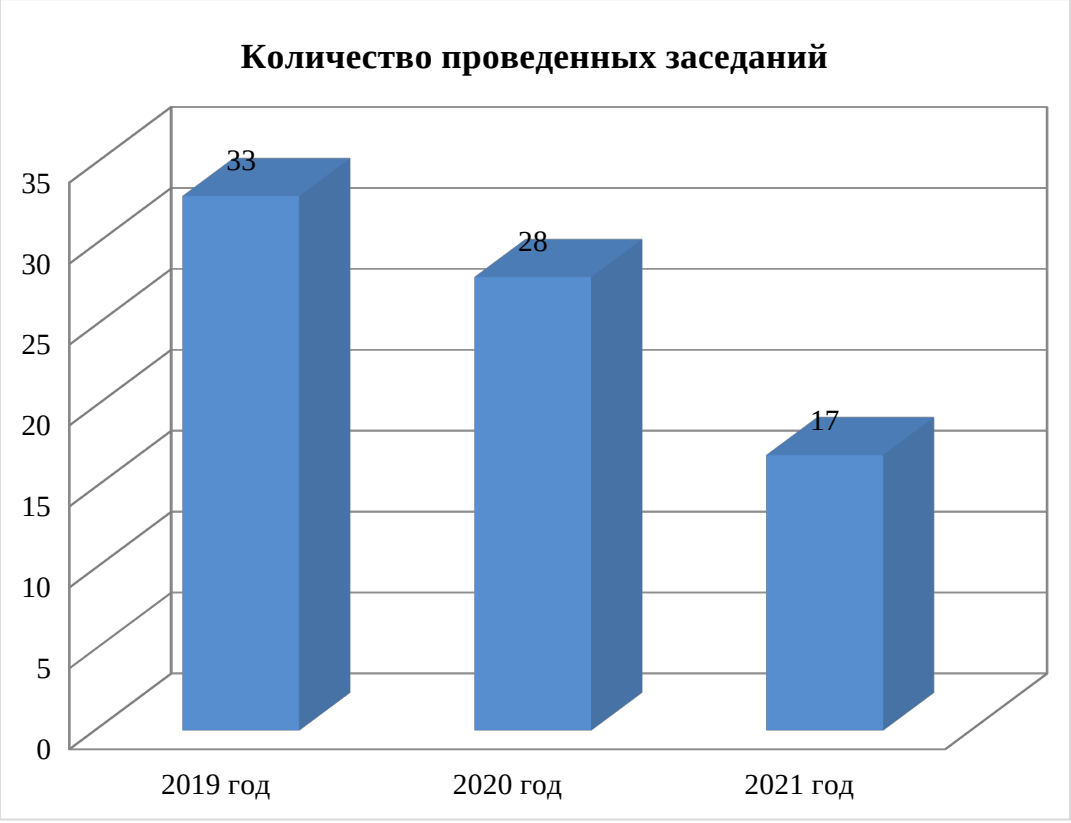

Рисунок 3.1. – Динамика количества проведенных заседаний

Как показывают данные рисунка 3.1., в динамике количества проведенных заседаний отмечается отрицательная тенденция. Особенно снижение отмечается в 2021 году: всего за год было проведено только 17 заседаний, что обусловлено неполным составом комиссии по причине введения ограничительных мероприятий (карантин).

Так же очень усложнило работу в рамках защиты информации на уровне Администрации муниципального образования города Муравленко большая доля сотрудников в возрасте 65+, которые вынуждены были соблюдать карантинные меры и не посещали рабочие места.

Соотношение возрастных групп сотрудников представлено на рисунке 3.2.

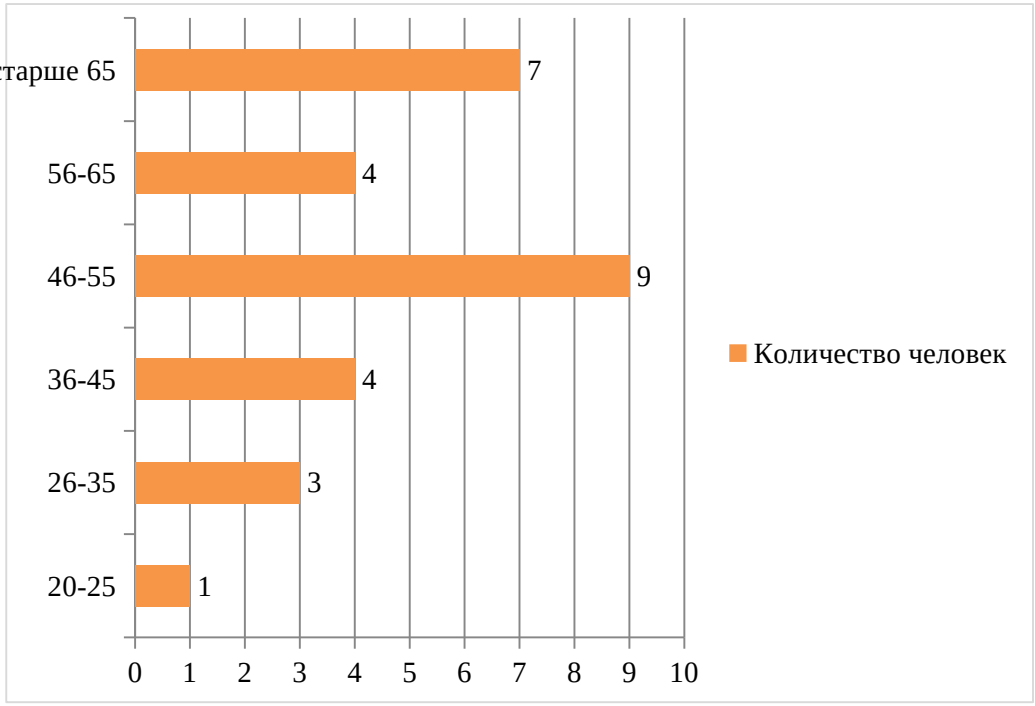

Рисунок 3.2. – Количество сотрудников различных возрастных групп

Данные рисунка 3.2. наглядно демонстрируют численность сотрудников Администрации в возрасте старше 65 лет – 7 человек или 25% от общей численности работников.

Нельзя не отметить, что в состав комиссии администрации муниципального образования города Муравленко так же входят сотрудники с возрастом 65+, всего их 4 человека, что усложняет проведение заседаний, и

соответственно негативно отражается на эффективности всего механизма защиты персональных данных.

Следующая проблема противодействия коррупции на уровне Администрации муниципального образования города Муравленко это отсутствие единого комплексного подразделения, занимающегося вопросами защиты персональных данных муниципальных служащих. На данный момент функции этого подразделения выполняют временные комиссии, организующие отдельные заседания их общей численности сотрудников, которые имеют определенный круг должностных полномочий и функций.

Формирование такого отдела затруднено по причине отсутствия кадровых ресурсов, и невозможности их привлечь из ограниченных объемов финансирования.

Так же в качестве отдельной проблемы необходимо выделить недостаточность нормативно-правовой базы, регламентирующей механизм защиты персональных данных муниципальных служащих в Администрации муниципального образования города Муравленко. Все действующие нормативно-правовые акты ограничиваются порядком создания комиссий, их работы.

Таким образом, необходимо сделать вывод о недостаточной обеспеченности типовыми положениями, касающимися комиссий, размещению информации на сайте, по разработке нормативно-правовых актов по вопросам защиты персональных данных муниципальных служащих.

Исходя из выявленных проблем, в работе предложены пути их решения.

3.2 Оптимизация и совершенствование порядка защиты персональных данных муниципальных служащих в Администрации города Муравленко

В качестве предложения по решению выявленных проблем защиты персональных данных муниципальных служащих предлагается создание в структуре Администрации города Муравленко подразделения по защите персональных данных муниципальных служащих в виде отдела. Представим его на схеме организационной структуры Администрации города Муравленко (см. рисунок 3.3.).

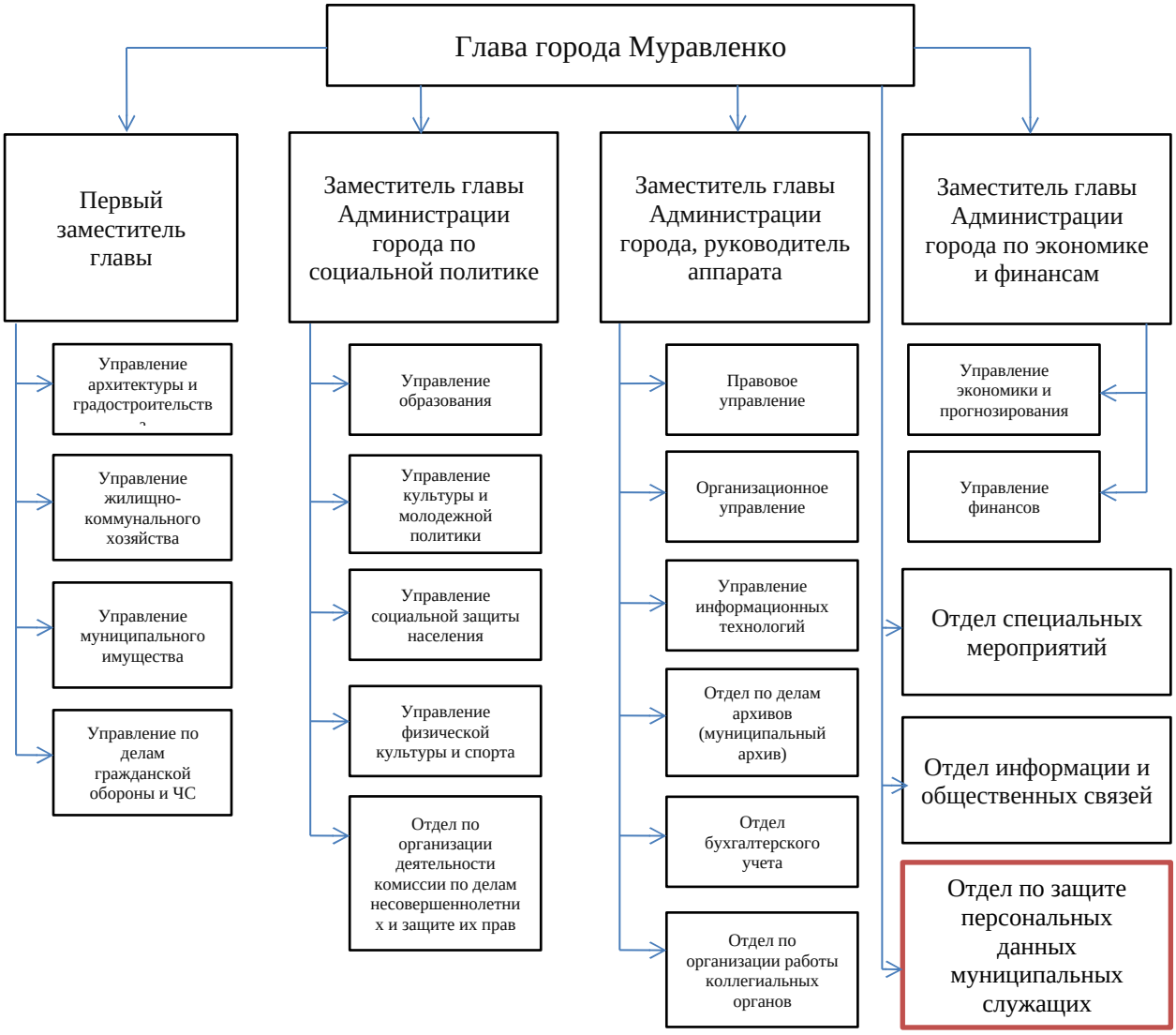

Рисунок 3.3. – Организационная структура Администрации города Муравленко

Как показывает рисунок 3.3., отдел по защите персональных данных муниципальных служащих предложено поместить под контроль непосредственно главы администрации, как и отдел информации общественных связей, а так же отдел специальных мероприятий. Численность отдел должна насчитывать не менее 5 сотрудников, для возможности организации заседаний в полном составе.

Так же в работе предлагается совершенствование системы нормативно-правового регулирования в целях детализации информации относительно защиты персональных данных муниципальных служащих.

Итак, рекомендуется разработка профессионального стандарта работника отдела по защите персональных данных муниципальных служащих.

Данный раздел должен включать все компетенции, которыми обязательно должен обладать сотрудник данного отдела, а так же его должностные обязанности.

Так же предлагается разработка национального стандарта на уровне муниципалитета города Муравленко по защите персональных данных муниципальных служащих, который будет содержать четкий регламентированный алгоритм действий должностных лиц при обнаружении факта использования персональных данных или угроз хищения информации и использования ее в корыстных целях.

Так же в работе предлагается отдельное прохождение учения в форме наставничества для новых сотрудников. Данное обучение должно осуществляться в форме анализа действующей нормативно-правовой базы по обеспечению защиты персональных данных муниципальных служащих, а так же проработка ситуаций возникновения фактов незаконного использования персональных данных и поведения сотрудника в таких ситуациях. Роль наставника состоит в оценке уровня знаний нового сотрудника в сфере защиты персональных данных муниципальных служащих, а так же

определению наличия компетенций для продолжения работы в данном учреждении.

Кроме того, рекомендуется совместно с заинтересованными региональными органами власти и организациями с привлечением экспертов в области обеспечения защиты персональных данных муниципальных служащих продолжить работу по созданию интернет-портала муниципального образования для обмена информацией о мерах предупреждения незаконного использования персональных данных в отдельных категориях организаций, консультирования работников таких организаций и налаживания обратной связи с ними по данной тематике.

Так же отдельно стоит отметить значимость и необходимость формирования методической базы предупреждения незаконного использования персональных данных муниципальных служащих Администрации:

- рекомендуется Администрации информировать вышестоящие органы о положительном опыте защиты персональных данных муниципальных служащих, используемых для этого средствах и системах, практике реализации законодательства;

- рекомендуется запрашивать информацию о применяемых в других регионах и муниципалитетах практик обеспечения защиты персональных данных муниципальных служащих с целью оценки возможностей реализации данных практик в собственной деятельности.

Итак, предложенные варианты решения выявленных в работе проблем в сфере защиты персональных данных муниципальных служащих в Администрации города Муравленко будут способствовать эффективности организации мер по предотвращению и профилактике незаконного использования персональных данных муниципальных служащих.

Таким образом, по результатам анализа существующего механизма организации защиты персональных данных муниципальных служащих в Администрации муниципального образования города Муравленко, в работе

были выявлены следующие проблемы: проблемы обеспечения защиты персональных данных муниципальных служащих на уровне муниципалитета, обусловленные введением ограничительных мероприятий, связанных с распространением новой коронавирусной инфекции; большая доля сотрудников в возрасте 65+, которые вынуждены были соблюдать карантинные меры и не посещали рабочие места; отсутствие единого комплексного подразделения, занимающегося вопросами защиты персональных данных муниципальных служащих в виде отдела со штатными сотрудниками; недостаточность нормативно-правовой базы, регламентирующей механизм защиты персональных данных муниципальных служащих в Администрации муниципального образования города Муравленко.

По результатам выявленных проблем в работе предложены следующие рекомендации: создание в структуре Администрации города Муравленко подразделения по защите персональных данных муниципальных служащих в виде отдела; совершенствование системы нормативно-правового регулирования в целях детализации информации относительно защиты персональных данных муниципальных служащих.

Заключение

Персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу.

Для эффективной защиты персональных данных работников необходимо принимать организационно-технические меры. От уровня защищенности будет зависеть перечень тех действий, которые необходимо осуществлять для защиты персональных данных.

Для защиты персональных данных используются различные варианты: технические средства (являются частью программы мероприятий по защите программного обеспечения от несанкционированного доступа); физические средства (сокращение доступа к персональным данным для посторонних лиц в виде разрешения работы с информацией только для определенных сотрудников); организационные и юридические меры (включает в себя разработку и внедрение руководства по обработке персональных данных компанией, положений о защите данных, издание указов о назначении ответственного лица и осуществление мер контроля).

В качестве объекта исследования в работе выступает Администрация муниципального образования города Муравленко - исполнительно-распорядительный орган муниципального образования.

В структуру администрации муниципального образования города Муравленко входят: юридический отдел, отдел по мобилизационной работе и безопасности, отдел по финансам, бюджету и бухгалтерскому учету, отдел градостроительства, архитектуры и инвестиций, отдел социальной поддержки населения и здравоохранения, отдел образования, культуры, туризма и спорта, общий отдел, ЗАГС, комиссия по делам несовершеннолетних. Численность работников администрации на конец 2021 года составляет 28 человек.

В деятельности Администрации города Муравленко сформирован целый механизм по защите персональных данных муниципальных служащих в виде Комиссии по соблюдению требований к служебному поведению и урегулированию конфликта интересов (аттестационная комиссия).

По результатам анализа существующего механизма организации защиты персональных данных муниципальных служащих в Администрации муниципального образования города Муравленко, в работе были выявлены следующие проблемы: проблемы обеспечения защиты персональных данных муниципальных служащих на уровне муниципалитета, обусловленные введением ограничительных мероприятий, связанных с распространением новой коронавирусной инфекции; большая доля сотрудников в возрасте 65+, которые вынуждены были соблюдать карантинные меры и не посещали рабочие места; отсутствие единого комплексного подразделения, занимающегося вопросами защиты персональных данных муниципальных служащих в виде отдела со штатными сотрудниками; недостаточность нормативно-правовой базы, регламентирующей механизм защиты персональных данных муниципальных служащих в Администрации муниципального образования города Муравленко.

По результатам выявленных проблем в работе предложены следующие рекомендации: создание в структуре Администрации города Муравленко подразделения по защите персональных данных муниципальных служащих в виде отдела; совершенствование системы нормативно-правового регулирования в целях детализации информации относительно защиты персональных данных муниципальных служащих.

Библиографический список

1. Трудовой кодекс Российской Федерации от 30.12.2001 « 197-ФЗ (ред. от 25.02.2022) (с изм. и доп., вступ. в силу с 01.03.2022) // СПС Консультант-плюс. – URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
2. Федеральный закон «О муниципальной службе в Российской Федерации» от 02.03.2007 №25-ФЗ // Российская газета. 2007. № 47
3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // СПС Консультант-плюс. – URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»// СПС Консультант-плюс. - URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
5. Кассационное определение Верховного суда Удмуртской Республики от 11.08.2010 по делу N 33-2625 // СПС Консультант-плюс. – URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
6. Апелляционное определение Московского городского суда от 18 ноября 2016 г. N 33- 45913/2016 // СПС Консультант-плюс. - URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
7. Апелляционное определение Санкт-Петербургского городского суда от 30 января 2017 г. № 33а-2104/2017 по делу № 2а-6384/2016 // СПС Консультант-плюс - URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).
8. Апелляционное определение Хабаровского краевого суда от 15.06.2017 по делу N 33- 4377/2017 // СПС Консультант-плюс. - URL: https://cloud.consultant.ru/ (дата обращения: 10.11.2022).

9. Постановление ФАС Северо-Кавказского округа от 21.04.2014 по делу № А53- 13327/2013 // СПС Консультант-плюс. - URL: https://cloud.consultant.ru (дата обращения: 10.11.2022).

10. Бундин М.В. Персональные данные как информация ограниченного доступа // Информационное право. № 1. 2019. С. 10-14.

11. Винарский С.С. Повышение эффективности социально-экономического развития муниципалитета // Форум Серия: Современное состояние и тенденции развития гуманитарных и экономических наук. 2022. № S1-2 (27). С. 61-64.

12. Девятов А.Н. Управление развитием муниципалитетов и регионов Российской Федерации на основе оценки показателей качества жизни // Вестник Удмуртского университета. Серия Экономика и право. 2022. № 4. С. 618-627.

13. Завьялкина А.А. Цифровизация управленческих процессов в деятельности органов муниципалитетов // Глобальные и локальные тренды в управлении, экономике, юриспруденции. 2022. №5. С. 301-304.

14. Капустян Л.А., Королева Е.Н., Мищенко В.В., Стрижкина И.В. Электронный муниципалитет как механизм взаимодействия власти и населения // Экономика. Профессия. Бизнес. 2022. № 4. С. 63-68.0

15. Овчинникова Е. А. Сравнительный анализ законодательства в области защиты персональных данных в Российской Федерации и Евросоюзе / Е. А. Овчинникова // Интерэкспо Гео-Сибирь. – 2022. – Т. 8. – № 2. – С. 113-117.

16. Рак В.Е., Лапина А.А. Муниципалитет online: управление коммуникациями в цифровую эпоху // Коммуникативные практики современной молодежи: перспективы и вызовы. 2022. №4. С. 416-421.

17. Салимова Т.А., Атнабаева Ю.В. Особенности обеспечения безопасности персональных данных в Российской Федерации // Юридические науки. 2021. № 11-1 (62). С. 119-122.

18. Соболь В.О. Межмуниципальное сотрудничество как инструмент консолидации муниципалитетов в условиях современных вызовов и угроз // Человек. Социум. Общество. 2022. № 8. С. 98-103.

19. Стрихорова Г.В., Моргачев И.А., Евграфова Л.Ю. Муниципалитет и его правовое регулирование // Вестник Иссык-Кульского университета. 2020. № 48. С. 312-316.

20. Талапина Э. В. Защита персональных данных в цифровую эпоху: Российское право в европейском контексте [Текст] / Э. В. Талапина // Труды Института государства и права РАН. – 2018. – Т. 13, № 5. – С. 120.

21. Холодов А.А. Процесс стратегического управления муниципалитетом // Глобальные и локальные тренды в управлении, экономике, юриспруденции. 2022. №8. С. 153-156.

22. Хронова И. А. Защита персональных данных работника / И. А. Хронова, М. М. Кудымов // Молодежь и системная модернизация страны : Сборник научных статей 7-й Международной научной конференции студентов и молодых ученых. В 5-ти томах, Курск, 19–20 мая 2022 года / Отв. редактор М.С. Разумов . – Курск: Юго-Западный государственный университет, 2022. – С. 476-479.

23. Хронова И. А. Особенности оформления трудового договора с дистанционным работником / И. А. Хронова // Современные социальные процессы в контексте глобализации: Сборник материалов III Международной научно-практической конференции, Краснодар, 2021. – С. 551-558.

24. Чернова Э.Р. Теоретико-правовые основы защиты персональных данных в Российской Федерации // Право: ретроспектива и перспектива. 2020. № 4 (4). С. 21-27.

25. Чурилов А. Ю. Принципы общего Регламента Европейского Союза о защите персональных данных (GDPR): проблемы и перспективы имплементации [Текст] / А. Ю. Чурилов // Сибирское юридическое обозрение. – 2019. – № 1.

26. Шебанова Н. А. Охрана персональных данных: опыт Европейского сообщества [Текст] / Н. А. Шебанова // Журнал Суда по интеллектуальным правам. – 2019. – № 25. – С. 5–14.

27. Якубова Л. А. Защита персональных данных в органах государственной и муниципальной власти: новые вызовы в условиях цифровизации / Л. А. Якубова, О. И. Слюсарчук // Актуальные проблемы гуманитарных наук. - 2022. – С. 176-179.