

Федеральное государственное автономное образовательное учреждение
высшего образования «Южно-Уральский государственный университет»
(национальный исследовательский университет)

На правах рукописи

Пономарева Юлия Владимировна

ПРАВОВОЙ РЕЖИМ СЛУЖЕБНОЙ ТАЙНЫ

Специальность 12.00.13 — Информационное право

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук
Минбалеев Алексей Владимирович

Челябинск – 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
1. ПРАВОВОЕ РЕГУЛИРОВАНИЕ И СУЩНОСТЬ СЛУЖЕБНОЙ ТАЙНЫ	15
1.1. История развития регулирования ограничения доступа к информации (на примере государственной и служебной тайн).....	15
1.2. Международное и зарубежное регулирование ограничения доступа к информации органов власти	35
1.3. Правовое регулирование служебной тайны в России	56
1.4. Служебная тайна как правовой режим информации.....	85
2. ОСОБЕННОСТИ ПРАВОВОГО РЕЖИМА СЛУЖЕБНОЙ ТАЙНЫ.....	118
2.1. Принципы и условия ограничения доступа к информации, охраняемой в режиме служебной тайны.	118
2.2. Категории сведений, охраняемых в режиме служебной тайны.....	133
2.3. Субъекты правоотношений, возникающих в сфере охраны и оборота сведений, охраняемых в режиме служебной тайны.....	162
2.4. Меры защиты информации в режиме служебной тайны	174
2.5. Ответственность за нарушение требований режима служебной тайны	190
ЗАКЛЮЧЕНИЕ	206
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	213
ПРИЛОЖЕНИЕ №1	241
ПРИЛОЖЕНИЕ №2.....	248

ВВЕДЕНИЕ

Актуальность темы исследования. Современные стандарты, выработанные международными нормативными актами в сфере защиты прав человека, безопасности и информационной политики в условиях активного развития глобального информационного общества, ставят задачу обеспечения принципа информационной открытости и транспарентности деятельности органов власти и иных публичных субъектов. Вместе с тем необходимость обеспечения безопасности, стратегических интересов государства, прав и законных интересов граждан и организаций обуславливает функционирование и активное развитие механизмов ограничения доступа к информации, в том числе в режиме служебной тайны. В Стратегии развития информационного общества на 2017-2030 годы обозначена необходимость обеспечения информационной безопасности и безопасности критической информационной инфраструктуры¹. Также еще в 2015 году в Стратегии национальной безопасности Российской Федерации была закреплена необходимость обеспечения информационной безопасности на фоне возрастающего значения информационных технологий в современном мире (Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»).

Решение задачи обеспечения информационной безопасности в государстве требует создания целостной системы защиты информации ограниченного доступа. Одним из слабых звеньев этой системы является регулирование защиты информации, охраняемой в режиме служебной тайны. Статьей 29 Конституции Российской Федерации предусмотрено право свободно искать, получать, передавать и производить информацию. В соответствии со статьей 9 Федерального Закона «Об информации,

¹ Указ Президента Российской Федерации от 09 мая 2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СЗ РФ. – 2017. – № 20. – Ст. 2901.

информационных технологиях и о защите информации» ограничение доступа к информации, а также условия такого ограничения устанавливаются федеральным законом. Таким образом, отсутствие регулирования защиты такой информации на уровне федерального закона противоречит требованиям Конституции Российской Федерации и действующему законодательству, порождает отсутствие единства правоприменения, а также создает предпосылки для злоупотребления возможностью введения ограничения доступа к информации со стороны субъектов служебной тайны. При этом в различных органах государственной власти существуют несколько подходов к регулированию отношений в сфере защиты внутренней информации, что также порождает определенные сложности при рассмотрении вопроса ограничения доступа к информации в режиме служебной тайны. В то же время значительное количество подзаконных нормативных актов, обуславливающих ограничение доступа к информации в органах власти и подведомственных организациях, свидетельствует о востребованности института служебной тайны.

Несмотря на существование различных подходов к пониманию служебной тайны и к механизму её регулирования, данный институт является одним из менее теоретически разработанных институтов информационного права.

Все это обуславливает актуальность исследования института служебной тайны с учетом уже сформированной системы информации ограниченного доступа в Российской Федерации, а также современных закономерностей эволюции данного института в условиях развития информационного общества.

Целью исследования является разработка и обоснование теоретических положений о правовом режиме служебной тайны, имеющих значение для развития теории информационного права, а также обоснование основных направлений совершенствования правового регулирования служебной тайны. Цель исследования определила ряд следующих задач:

- исследовать историю регулирования информации ограниченного доступа, в том числе служебной тайны в России, и проследить в динамике процессы, которые детерминировали введение ограничения доступа к информации в органах власти;

- проанализировать международные акты и национальное законодательство зарубежных стран в сфере ограничения доступа к информации в органах государственной власти и местного самоуправления, выявить основные проблемы правового регулирования;

- исследовать состояние правового регулирования института служебной тайны в России и выявить закономерности его развития;

- изучить основные теоретические подходы к формированию института служебной тайны и теоретически обосновать подход к пониманию служебной тайны как правового режима информации;

- сформулировать принципы ограничения доступа к информации в режиме служебной тайны и категории сведений, охраняемых в режиме служебной тайны;

- исследовать специфику правового статуса субъектного состава и специфику объекта правоотношений, складывающихся в сфере оборота сведений, охраняемых в режиме служебной тайны;

- выявить основные направления формирования и совершенствования правового режима служебной тайны в сфере защиты информации и ответственности за нарушение требований режима.

Объектом исследования являются общественные отношения, складывающиеся по поводу правового регулирования служебной тайны.

Предметом исследования выступают нормы российского и международного права, законодательство иностранных государств, научная доктрина и материалы правоприменительной практики, отражающие генезис концепций, представлений и моделей правового регулирования служебной тайны и ее месте в системе информации ограниченного доступа.

Степень научной разработанности темы. Проблемы отдельных видов информации ограниченного доступа, в том числе служебной тайны, исследовали такие специалисты информационного права, как: И. Л. Бачило, Н. Н. Ковалева, П. У. Кузнецов, В. Н. Лопатин, А. В. Минбалеев, А. В. Морозов, И. М. Рассолов, А. А. Стрельцов, А. А. Тедеев, Л. К. Терещенко, Т. А. Полякова, А. А. Фатьянов и другие.

Специальные исследования в сфере правовой природы служебной тайны осуществляли А. А. Антопольский, Э. П. Гаврилов, Е. К. Волчинская, А. А. Дворников, В. А. Дозорцев, Т. М. Занина, Г. Г. Камалова, В. Н. Лопатин, И. Ю. Павлов, И. И. Салихов, А. М. Сергеев, И. Н. Смирнова, С. Ф. Щадрин, Е. Н. Яковец и другие. Вместе с тем, вопросы служебной тайны как института права рассматриваются, как правило, в сравнительном аспекте с другими институтами информации ограниченного доступа. Работы, в которых исследуется правовая сущность служебной тайны, этот институт рассматривают применительно к его отраслевой специфике либо применительно к вопросам ответственности за разглашение информации.

Теоретическую основу работы составляют труды российских ученых в области теории государства и права, а также в области административного права: А. Б. Агапова, С. С. Алексеева, Д. Н. Бахраха, А. Б. Венгерова, О. А. Гаврилова, В. В. Головкин, О. С. Иоффе, В. Б. Исакова, В. П. Казимирчука, Д. А. Керимова, С. А. Комарова, В. М. Корельского, В. Н. Кудрявцева, В. И. Леушина, Я. М. Магазинера, В. И. Майорова, А. В. Малько, М. Н. Марченко, Н. И. Матузова, Ю. А. Нисневича, А.Ф. Ноздрачева, В. Д. Перевалова, А. С. Пиголкина, С. В. Полениной, В. К. Райхера, Б. В. Россинского, Ю. П. Соловья, Ю. Н. Старилова, Ю. А. Тихомирова, Ю. К. Толстого, Т.Я. Хабриевой, Р. О. Халфиной, Л. С. Явича и других ученых.

Основополагающее теоретическое и методологическое значение для исследования составили работы ученых в области информационного права: Ю. М. Батурина, И. Л. Бачило, И. Ю. Богдановской, Е. К. Волчинской, О. А. Городова, Д. В. Грибанова, В. Б. Исакова, Д. А. Ловцова, Н. Н. Ковалевой, В.

А. Копылова, П. У. Кузнецова, И.И. Кучерова, В. Н. Лопатина, А.В. Минбалеева, А. В. Морозова, В. Б. Наумова, Т. А. Поляковой, Ю. Г. Просвирнина, И. М. Рассолова, М. М. Рассолова, Н. И. Соловяненко, А. А. Стрельцова, А. А. Тедеев, Л. К. Терещенко, А. А. Фатьянова, М. А. Федотова, С. Е. Чаннова, А. А. Чеботаревой.

Ряд вопросов, связанных с регулированием отношений в информационной сфере, нашел отражение в работах И. С. Бойченко, Ю. В. Волкова, О. А. Гаврилова, Г. Г. Камаловой, Д. В. Огородова, М. И. Паршукова, О. В. Танимова, Л. В. Филатовой, С. Г. Чубуковой и др.

Методологической основой диссертации является единство общенаучных и специальных методов познания. Цель и задачи исследования, а также специфика используемых источников обусловили комплексное применение различных методов познания. Важнейшее значение оказали диалектический, исторический, формально-логический, общелогический методы, а также метод системного анализа. В диссертационном исследовании также использовались специальные юридические методы познания: историко-правовой, сравнительно-правовой, формально-юридический и др.

Нормативную базу исследования составляют Конституция Российской Федерации, международные акты, федеральное законодательство, в том числе ведомственные инструкции, приказы, положения, а также нормативные акты субъектов и органов местного самоуправления и иные нормативные документы, а также законодательство зарубежных стран.

Эмпирическую базу исследования составляют материалы судебной практики международных и национальных судов, а также материалы исследований международных организаций, официальные документы органов власти и подведомственных организаций.

Научная новизна исследования определяется поставленной научной целью и задачами, имеющими теоретическую и практическую значимость и выражается в расширении научных представлений о правовом режиме

служебной тайны, а также в определении ее правовой сущности и месте в системе информации ограниченного доступа.

В работе впервые разработана целостная авторская концепция правового режима служебной тайны, основанная на существующих теоретических подходах и новейших нормативных правовых актах, материалах правоприменительной практики.

Новизна заключается в сделанных на основании проведенного исследования научных предложениях и выводах, в том числе: выделение различных моделей правового регулирования служебной тайны на основе опыта зарубежных стран; выявление признаков сведений, охраняемых в режиме служебной тайны; обоснование научных подходов к обновлению понимания служебной тайны, а также сведений, которые охраняются в режиме служебной тайны; обоснование необходимости системного подхода к изучению ограничения доступа к информации в органах государственной власти, местного самоуправления, подведомственных организациях и государственных корпорациях; выделение принципов правового регулирования отношений в сфере служебной тайны; выявление закономерностей правового регулирования служебной тайны в условиях развития информационного общества и ее особенностей в сравнении с другими тайнами.

Научная новизна отражена в представленных и обоснованных теоретических положениях, предложениях по совершенствованию правового регулирования служебной тайны, сделанных выводах.

Разработана концепция федерального закона о служебной тайне.

На защиту выносятся следующие основные положения, являющиеся новыми или содержащими элементы новизны:

1. С целью упорядочения научно-теоретических представлений о правовой природе информации, охраняемой в режиме служебной тайны, в зависимости от единства и дифференциации используемых правовых режимов информации, в которых охраняются сведения, существующие в

органах власти, выделены следующие модели правового регулирования: модель, в основу которой положена категория «государственные секреты» (в нее, в том числе, входит такая категория, как «служебная тайна»); модель, которая характеризуется использованием единственной категории – информации ограниченного доступа в сфере управления (государственная либо служебная тайна – наименование единого института зависит от особенностей перевода); модель, которая характеризуется разграничением правового режима государственная и служебная тайн.

2. С целью развития и унификации понятийно-категориального аппарата понятие «служебная информация» рассматривается как родовое для всей информации, используемой в органах государственной власти и органах местного самоуправления, а также подведомственных им организациях и государственных корпорациях. Понятие «служебная тайна» при этом должно обозначать правовой режим соответствующей информации ограниченного доступа. В отношении информации, охраняемой в режиме служебной тайны, автором предлагается использовать такое понятие как «сведения, охраняемые в режиме служебной тайны». При этом понятия «сведения» и «информация» синонимичны по своему значению, а понятие «служебная тайна» тождественно понятию «правовой режим служебной тайны». В целях развития доктрины информационного права разработано авторское определение понятия «правовой режим служебной тайны», который представляет собой совокупность правовых, организационных и технических методов и средств, обеспечивающих защиту сведений, формирующихся в результате деятельности органов государственной власти и органов местного самоуправления, а также подведомственных им организаций, а также информации ограниченного доступа о физических и юридических лицах, ставшая известной указанным субъектам в результате осуществления возложенных на них полномочий и обязанностей.

3. Обосновано, что в целях правовой идентификации сведений, охраняемых в режиме служебной тайны, данные сведения должны обладать следующими признаками:

– Сведения формируются в результате осуществления государственной (муниципальной) управленческой и (или) связанной с ней хозяйственной деятельности либо являются информацией ограниченного доступа о физических или юридических лицах, ставшей известной органам власти и подведомственным им организациям в результате осуществления возложенных на них полномочий и обязанностей;

– характеризуются закрытым перечнем субъектов, которые могут ими обладать: органы государственной власти, органы местного самоуправления, подведомственные им организации и государственные корпорации. В некоторых случаях сведения могут передаваться в ходе исполнения договоров гражданско-правового характера;

– доступ к данным сведениям ограничен требованиями федерального закона.

4. Разработан элементный состав правового режима служебной тайны, включающий в себя следующие элементы:

– принципы ограничения доступа к сведениям в режиме служебной тайны;

– объект режима – сведения, охраняемые в режиме служебной тайны;

– субъекты правоотношений в сфере оборота сведений, охраняемых в режиме служебной тайны, на которые возложены обязанности защиты сведений, охраняемых в режиме служебной тайны;

– содержание правоотношений в сфере оборота сведений, охраняемых в режиме служебной тайны;

– совокупность организационных и технических требований обеспечения конфиденциальности сведений, охраняемых в режиме служебной тайны;

– ответственность за нарушения требований режима служебной тайны.

5. С целью формирования единого теоретического подхода к правовому регулированию института служебной тайны, автором предложена и обоснована концепция правового регулирования служебной тайны, в соответствии с которой механизмы ограничения доступа к информации должны формироваться в соответствии с правовыми принципами законности, обоснованности, срочности характера ограничения, соблюдения прав и свобод человека и гражданина, интересов общественности, контроля за ограничением доступа к сведениям, охраняемым в режиме служебной тайны. Автором обоснована необходимость учета международных принципов национальной безопасности («Тсваньские принципы»)¹ при теоретическом осмыслении и формировании пути развития законодательства в сфере служебной тайны.

6. В работе доказывается, что при формировании классификации сведений, охраняемых в режиме служебной тайны, должно учитываться существующее нормативное регулирование, а также уже существующие перечни сведений, охраняемые в настоящее время под грифом «Для служебного пользования». В состав основных разделов данной классификации необходимо включать сведения об информационной и физической безопасности, информацию о непосредственной деятельности, связанной с реализацией властных полномочий, сведения в области геодезии, картографии и проектировании, информацию о научно-технических разработках, сведения об административно-хозяйственной деятельности, а также информацию, составляющую тайну третьих лиц.

7. В целях систематизации прав и обязанностей субъектов правоотношений в сфере служебной тайны разработана их классификация по различным основаниям. В зависимости от объема возложенных полномочий субъектов предложено подразделять на: субъектов, уполномоченных

¹ Global principles on national security and the right to information (“THE TSHWANE PRINCIPLES”) // Приняты в Тсване, Южная Африка, 12.06.2013. – URL: [https://fas.org/sgp/library/tshwane.pdf]

устанавливать правила оборота и основания отнесения информации к сведениям, охраняемым в режиме служебной тайны; субъектов, уполномоченных устанавливать конкретный перечень категорий сведений, доступ к которым может быть ограничен; субъектов, которые уполномочены относить ту или иную информацию к сведениям, охраняемым в режиме служебной тайны; субъектов, обеспечивающие соблюдение режима охраны сведений, охраняемых в режиме служебной тайны; субъектов, осуществляющих работу с документами, в которых содержатся сведения, охраняемые в режиме служебной тайны. В зависимости от основания получения доступа к сведениям, охраняемым в режиме служебной тайны предложено подразделять субъектов на: субъектов, получающих доступ к сведениям в силу закона; и субъектов, получающих доступ к сведениям в силу договора.

8. В целях формирования и развития комплексного правового регулирования служебной тайны как правового института, отвечающего требованиям современного информационного законодательства, разработаны и обоснованы следующие правовые средства:

- нормативная унификация порядка работы со сведениями, охраняемыми в режиме служебной тайны;

- определение и законодательная фиксация порядка осуществления государственного надзора за процедурой отнесения информации к сведениям, охраняемым в режиме служебной тайны;

- внедрение механизма административного и судебного порядка обжалования процедуры отнесения информации к сведениям, охраняемым в режиме служебной тайны, который должен позволить эффективно разрешать вопросы обоснованности и законности ограничения доступа к данным сведениям;

- введение системы мер юридической ответственности за нарушение требований режима служебной тайны.

Теоретическая значимость исследования заключается в развитии теоретической базы информационного права, систематизации и расширении научных знаний о правовом режиме служебной тайны, а также в комплексном анализе данного института в условиях развития информационного общества. Настоящее исследование дополняет теоретические положения информационного права, а также позволяет рассматривать информационное право как целостную, интенсивно развивающуюся систему. Рекомендации и выводы, приведенные в настоящей работе, могут стать основой для дальнейших научных исследований как информационных правоотношений в целом, так и правоотношений в сфере информационной безопасности в частности.

Практическая значимость исследования заключается в возможности использования полученных результатов и выводов для дальнейшего совершенствования законодательства в информационной сфере. Материалы исследования могут использоваться в учебном процессе при подготовке курсов учебных дисциплин, читаемых как для студентов юридической специальности и направления, так и для специалистов в сфере защиты информации, а также при создании учебных и учебно-методических пособий по информационно-правовой проблематике.

Апробация результатов исследования. Основные теоретические положения, выводы и научно-практические рекомендации, которые изложены в диссертации, получили отражение в 19 статьях, 6 из которых опубликованы в ведущих рецензируемых журналах и изданиях, указанных в перечне Высшей аттестационной комиссии.

Результаты исследования были обсуждены на международных, зарубежных и всероссийских научно-практических конференциях, семинарах и круглых столах, а именно: «Актуальные проблемы права России и стран СНГ» (г. Челябинск, 2003–2011 гг.); «Современные проблемы юридической науки» (г. Челябинск, 2004–2011 гг.); «Правовая система и вызовы современности. Материалы XII Международной научно-практической

конференции студентов, аспирантов и молодых ученых» (Уфа, 3-5 декабря 2015 года); «Правовые проблемы и пути их решения в условиях развития современного общества» международная научная конференция студентов, магистрантов и аспирантов (Минск, 23-24 октября 2015 г.), «Традиции и новации в системе современного российского права: XIII Международная научно-практическая конференция молодых ученых» (г. Москва, 2014); Международная конференция iSLaCo-2015 (г. Санкт-Петербург) и др. Положения диссертационного исследования внедрены в учебный процесс Южно-Уральского государственного университета (национального исследовательского университета) при преподавании семинарских занятий по дисциплинам «Информационное право» и «Правовая защита информации».

Результаты проведенного исследования, выводы, предложения и рекомендации были обсуждены на кафедре теории государства и права, конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета).

Структура диссертации обусловлена целью и задачами исследования и состоит из введения, двух глав, включающих девять параграфов, заключения и библиографического списка, двух приложений.

1. ПРАВОВОЕ РЕГУЛИРОВАНИЕ И СУЩНОСТЬ СЛУЖЕБНОЙ ТАЙНЫ

1.1. История развития регулирования ограничения доступа к информации (на примере государственной и служебной тайн)

С древнейших времен люди осознавали значение и важность различной информации, а также нежелательность распространения информации, представляющей ценность для власти и управления. Охрана государственных секретов всегда была одной из важнейших задач, которая стояла перед аппаратом государственного управления. Пожалуй, одной из самых древних тайн в сфере государственного управления можно назвать военную тайну. Когда ограничение доступа к информации о стратегии, тактике ведения боя, а также места дислокации воинских подразделений играли жизненно важную роль для всего государства. Как отмечает А. А. Фатьянов, зарождение государственных секретов во многом начиналось с необходимости сохранения военной тайны.¹ Тем не менее, в функционировании государственного аппарата, а также в управлении государством особую роль всегда играла информация, сохраняющаяся в тайне.

До XVII века между подчиненными и правителем отношения регулировались всеобъемлющим понятием «верность»². «Сложно сказать, было ли возникновение этого понятия связано с нравственными основами служения правителю или же оно основывалось на имущественной зависимости подчиненных. Чаще всего произносилась устная клятва

¹ Фатьянов, А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве): Моногр. / А. А. Фатьянов. – М.: Изд-во МИФИ, 1998. – С. 8.

² Стефанович, П. С. Понятие верности в отношениях князя и дружины на Руси в XII–XIII в. / П. С. Стефанович // Древняя Русь. Вопросы медиевистики. – 2008. – № 1 (32). – С. 72–82.

правителю, которая и была определенной гарантией верности».¹ Понятием «верность», как правило, охватывалась готовность «сложить голову» за Князя, которому служил дружинник. В связи с этим отождествлять понятие «верности» с обязательством неразглашения определенной информации считаем не совсем корректным. Далее понятие «верность» приобрело более широкое, можно сказать всеобъемлющее значение в отношении службы государю.

Исследователи называют первым упоминанием об ограничении доступа к управленческой информации упоминание об особом порядке рассмотрения секретных дел в Указе Петра I от 4 апреля 1714 г. № 2791 «О заведении в Сенатах, в Советах Военных и Губернских протоколов для внесения в оные определения по всем делам, о недачи голосов при совещании, о подписании членами собрания протоколов, о составлении решительного определения по большинству голосов и о записи в протокол особенных мнений, несогласных с общим решением»². В этом указе прописан особый порядок рассмотрения секретных дел, а также особый порядок допроса свидетелей. Из данного Указа не явствует, что эти секретные дела носили исключительно государственный характер. Секретность понимается здесь в широком смысле. Однако, вопреки распространенному мнению, это упоминание не является первым упоминанием о соблюдении тайны в отношении дел государевых. Интересно изучить некоторые формы присяги разных чиновников и проследить определенное развитие тайности деятельности государственного аппарата. В форме присяги разных чиновников от 31 августа 1651 г. упор делается на верность Государю и несение государевой службы «без хитрости», указания на обязательность сохранения в тайне той или иной информации отсутствуют. Однако уже буквально через два года была утверждена иная форма присяги

¹ Стефанович, П. С. Дружинный строй в древней Руси и у древних германцев: существовала ли клятва верности вождю (правителю)? / П. С. Стефанович // Древняя Русь. Вопросы медиевистики. – 2008. – № 2 (32). – С. 33-40.

² См.: Сизиков, М. И. История государства и права России с конца XVII до начала XIX века / М. И. Сизиков. Учебное пособие. – М.: ИНФРА-М., 1998. – 320с.

разных чиновников, в которой чиновникам некоторых должностей предписывалось «государская думы и Боярского приговору никому до Государева указа не сказывати», а дьяк должен был «тайные государевы и всякие дела хранить в секрете». Таким образом проявляется тенденция постепенного нормативного закрепления ограничения доступа к информации о ведении государственных дел и государственной службы. Стоит отметить, что в документе отсутствует выделение государственной или иной тайны как сведений определенного свойства. Отмечается лишь необходимость неразглашения тайных государевых дел. Безусловно, следует помнить о том, что ещё в 1653 году Царем Алексеем Михайловичем был учрежден приказ тайных дел. В этом приказе заседал дьяк и 10 подьячих. Именно с введением тайного приказа можно связывать возникновение государственной тайны как политико-правового явления и, соответственно, такое закрепление формы присяги с включением соответствующих обязательств.

Одним из первых «секретных» документов (дошедших до наших дней и имеющих в свободном доступе) можно назвать царский указ «Именный, объявленный в разряд тайных дел подьячим»: О наказании кнутом подьячего за прописку государева наименования (14 августа 1658 г.).¹ Для исследования он ценен не своим содержанием, а своей формой: указ объявлен в разряд тайных дел. Эта маленькая деталь свидетельствует о том, что началось использование особого оформления и обозначения документов, содержащих информацию, относимую к государственной тайне.

Следующее упоминание о секретах в сфере государственного управления встречается в Генеральном регламенте 1720 года. В нем впервые устанавливается секретный характер ведения государственных дел: «...повелевает его величество накрепко, чтоб все, что при коллегиях чинится, а наипаче ежели такие дела, которые его царского величества высокой службе и

¹ Полное собрание законов Российской Империи. Собрание Первое. 1649-1825 гг. (Т.1) / под ред. М. М. Сперанского. – СПб: Тип. II Отделения Собственной Его Императорского Величества Канцелярии. – 1830. – С. 459.

интереса касаются, тайно содержаны и весьма прежде времени явны не были»¹. Кроме того, обязательство неразглашения государственных тайн есть и в клятве, которую должны были давать присяжные: «Когда же к службе и пользе его величества, какое тайное дело, или какое б оно ни было, которое приказано мне будет тайно содержать<...>по совести своей исправлять»². Также в этом регламенте предусматривались наказания для тех, «кто злым образом на время, или вовсе, тайно из коллегийных писем и документов что унесет». Стоит отметить, что конкретное наказание не предусматривалось, а лишь предполагалось соответствующим «важности дела». Анализ данных положений свидетельствует, что в нем не было определено какой-то конкретной тайны, не были определены критерии, которым должны соответствовать охраняемые сведения, а также не был определен порядок отнесения таких сведений к тайне. Тем не менее, в указанном нормативном акте прописаны три существенных аспекта правового регулирования:

1) установлена обязанность хранить тайну для государственных служащих (определены субъекты правоотношений) и своеобразная процедура допуска к тайне в форме клятвы;

2) закреплена необходимость ведения в коллегиях и канцеляриях дел тайно (предусмотрена диспозиция);

3) предусмотрено наказание за разглашение тайны (введена санкция).

Следует отметить, что в данном случае речь не идет о зарождении института государственной тайны в современном его понимании, так как нет предписания сохранения информации в тайне в зависимости от содержания. Полагаем, что можно говорить о зарождении института тайны государственного управления. Так в Генеральном регламенте предписывалось: «повелевает его величество накрепко, чтоб все, что при коллегиях чинится <...> тайно». В данном случае речь можно вести не только

¹ Лебедев, В. И. Реформы Петра I: сборник документов / В. И. Лебедев. – М., 1937. – С. 127.

² Лебедев, В. И. Реформы Петра I: сборник документов / В. И. Лебедев. – М., 1937. – С. 110.

о сохранении в тайне информации о делах государственной важности, но и о сохранении в тайне внутренней информации коллегии. Если в данном случае проводить аналогию с современностью, то такую внутреннюю информацию коллегий можно отнести и к служебной тайне. В дальнейшем развитие нормативной базы можно проследить в указах Петра I от 13 января 1724 г. «О неписании секретных дел в партикулярных письмах», от 16 января 1724 г. «О поручении секретных дел в Сенате благонадежным людям» и в приказе Правительствующего Сената от 5 марта 1724 г. «О надписях на пакетах, в которых секретные дела»¹. В указе от 13 января 1724 г. «О неписании секретных дел в партикулярных письмах» встречаем следующее указание: «О делах, которые тайности подлежат в государственных делах, оного отнюдь в партикулярных письмах ни к кому не писать». В этом указании можно отметить выделение круга тайной информации в зависимости от её содержания и от её государственного значения. Такое выделение очень важно, так как в данном документе уже запрещается разглашать не вообще всю информацию, которая есть в органах аппарата управления, а лишь ту, которая «подлежит тайности в государственных делах». Таким образом, буквально начинает выделяться тот объект (информация), который и должен подлежать правовой защите.

В одном из указов XVIII века предписывалось следующее: «учините <...>, чтобы секретные дела были особливо у надежных людей»². В этом документе впервые были обозначены определенные требования к людям, которым доверяли информацию, доступ к которой должен быть ограничен.

¹ Полное собрание законов Российской Империи. Собрание Первое. 1649-1825 гг. (Т.7) / под ред. М.М. Сперанского. – СПб: Тип. II Отделения Собственной Его Императорского Величества Канцелярии. – 1830. – Ст.ст. 4409, 4418, 4481.

² Указ от 16 января 1724 г. «О поручении секретных дел в Сенате благонадежным людям» // Полное собрание законов Российской Империи. Собрание Первое. 1649-1825 гг. (Т.7) / под ред. М. М. Сперанского. – СПб: Тип. II Отделения Собственной Его Императорского Величества Канцелярии. – 1830. – Ст. 4409.

В другом приказе¹ предусматривался особый порядок оформления секретных документов и их доставки: «Доношения и прочия письма, в которых писать случится о каких секретных делах, посылать за печатями в пакетах, на которых подписывать именно, что оные о секретных делах, а в сенатах таких пакетов секретарям не распечатывать»².

Петровская эпоха ознаменовала появление такого правового явления как секрет (тайна) государственной службы. Несмотря на то, что не было ещё деления информации на различные виды тайны, однако основные положения, регулирующие порядок допуска, сохранения, обращения с информацией такого рода, а также наказания за разглашение тайны были уже прописаны в законодательстве. В эпоху правления императрицы Екатерины II намеченные тенденции к повышению степени охраны и развития организационно-правовых мер получили своё продолжение. Так в 1765 г. был издан Сенатский приказ «Об обозначении на бумагах и конвертах по делам секретным как прежними указами о том предписано». В этом указе предписывалось пометать не только документы, но и конверты пометкой «секретно». Делалось это с целью сохранения тайны и вскрытия конверта только указанным адресатом. С целью дальнейшего совершенствования делопроизводства был издан Сенатский приказ от 7 января 1768 г. «О подписывании представлений, доношений и рапортов по секретным делам». В указанном документе обращается внимание на нарушение действующего порядка обращения с секретными документами, определены конкретные лица, которые должны подписывать секретные документы. Приказом устанавливается штраф, который взимается в случае нарушения предписанного порядка обращения с секретными документами. Размер штрафа составлял 10 рублей. Это, пожалуй,

¹ Приказ Правительствующего Сената от 5 марта 1724 г. «О надписях на пакетах, в которых секретные дела» // Полное собрание законов Российской империи / Т. 7 (1723-1727). – Типография 2-го отд. Собственной Его Императорского Величества Канцелярии. – 1830. – Ст.ст. 4409, 4418, 4481.

² Полное собрание законов Российской империи / Т. 7 (1723-1727). – Типография 2-го отд. Собственной Его Императорского Величества Канцелярии. – 1830. – Ст.ст. 4409, 4418, 4481.

первая четко установленная санкция за нарушение секретности государственных дел.

В дальнейшем в Уложении о наказаниях уголовных и исправительных 1845 года государственным преступлениям был посвящен целый раздел. В нем были подробно прописано, что понимается под государственной изменой. Такое детальное регулирование понятия «государственная измена» встречается в законодательстве впервые. В понятие государственной измены включалось также разглашение государственной тайны. Следует отметить, что государственной изменой могло стать разглашение не только государственной тайны, но и иной информации, которая не была секретной: план крепости, порта, гавани, арсенала, укрепленного или иного стана, тех мест, где происходят военные действия, известия о расположении и движении войск, о состоянии армии или других средствах нападения, обороны. Уложение также предусматривало наказание за опубликование планов российских крепостей, иных укрепленных мест, гаваней, портов, арсеналов без дозволения правительства.

Указанные нормативные положения представляют немалый интерес, так как «в них устанавливается запрет на разглашение не только государственной тайны, но и иной информации, имеющей стратегическую ценность в случае военных действий. Это свидетельствует о том, что массив информации, имеющей ограниченное распространение, перестает быть однородным и постепенно получает различия в правовом регулировании в зависимости от степени значимости сведений и порядка их обращения.

В Уголовном уложении 1903 г. меры ответственности за разглашение различных видов тайн получили свое активное развитие. Во многом это было связано не только с развитием общественных отношений, но и с политической обстановкой того времени. Можно сказать, что в трех главах уложения была предусмотрена ответственность за разглашение тайн: в VI главе предусмотрена ответственность за государственную измену, под которой понимается, кроме прочего, опубликование или сообщение агенту

иностранный план, рисунка, документа, находящегося в тайне, в целях охраны государственной безопасности России, кроме того в XXIX главе впервые предусматривалась уголовная ответственность за разглашение тайн. Целая глава была посвящена преступлениям, связанным с разглашением той или иной информации. Важно отметить, что под тайной в данном случае понималась не только информация, являющаяся государственной тайной, но также и тайна «другого лица». Виновный привлекался к ответственности за разглашение сведений, «если притом оглашенное сведение могло причинить имущественный ущерб или опозорить лицо, к которому оно относилось»¹. «Новое Уголовное Уложение впервые устанавливало ответственность за разглашение тайны переписки (ст. 542), секрета производства (ст. 543), банковской тайны (ст. 544), коммерческой тайны (ст. 545), налоговой тайны (ст. 546). Таким образом, впервые в уголовном законодательстве России речь шла об ответственности не только за разглашение тайны государства, но и иных тайн, кроме того, достаточно подробно была разграничена ответственность в зависимости от вида разглашаемой информации.

Необходимо особое внимание уделить также Главе XXXVII «О преступных деяниях на службе государственной и общественной» Уголовного уложения, в которой была предусмотрена достаточно развернутая система уголовных наказаний за преступления в сфере государственной службы, среди которых было оглашение сведений, которые должны храниться в тайне (правительственные распоряжения, сведения и документы), в том числе телеграмм или почтовых сообщений, а также сведений, касающихся внешней безопасности России. Впервые в Уложении в ст. 655 предусматривалась ответственность за разглашения «частной тайны», ставшей известной служащему в силу должностных обязанностей (тайна частной жизни, секрет производства, нотариальная тайна). Кроме того, была введена также

¹ Новое Уголовное уложение. Высочайше утвержденное 22 марта 1903 г. / Издание Каменноотсровского юридического книжного магазина В. П. Анимимова. – СПб. – 1903 г. – С. 171.

ответственность за разглашение такой специфической информации в сфере государственного управления как информация о способах изготовления государственных кредитных бумаг и их секретных признаках, а также тайны торгов по казенным или общественным подрядам, или поставкам, когда торги производятся через запечатанные объявления. Полагаем, что в этом случае можно констатировать начало формирования требований защиты сведений, которые были доступны лицам, состоявшим на государственной службе, которые выделяются из общего массива информации о государственном управлении и перестают быть связанными исключительно с государственной тайной. «Стоит особо отметить, что в Уложении 1845 года ответственность за разглашение государственной тайны и другой информации управленческого и военного характера предусматривалась только в разделе, посвященном государственным преступлениям. В разделе «О проступках и преступлениях по службе государственной и общественной» ответственности за разглашение информации, ставшей известной служащему в силу его служебного положения, либо за разглашение иной информации в сфере порядка управления в Уложении 1845 г. не предусмотрено. Таким образом, Уложение 1903 г. впервые разграничило различные виды информации ограниченного доступа и предоставило защиту не только сведениям в сфере государственной службы, управления и внешней безопасности страны, но и сведениям, составляющим частную тайну как физических, так и юридических лиц.

Тем не менее, отсутствие подробного «Перечня сведений, составляющих государственную тайну», как отмечают исследователи, являлось одной из проблем уголовного законодательства того времени. «На основании законодательства можно было лишь выделить отдельные группы сведений, имеющих гриф «долженствующие сохраняться в тайне»:

- планы, чертежи, рисунки или макеты российских укрепрайонов, крепостей и других фортификационных сооружений;
- технические данные о военных кораблях;

- сведения о содержании мобилизационных планов и расположении войск на случай войны».¹

Исследователи отмечают, что «из-за особенностей законодательства из 150 установленных правоохранительными органами Варшавского военного округа австрийских и германских шпионов (от мелких контрабандистов до офицеров Штаба военного округа) к уголовной ответственности было привлечено 33 человека»².

В начале 20 века во многом из-за происходящих внешнеполитических и внутривнутриполитических процессов (русско-японская война, первая революция, первая мировая война...) охрана секретов в сфере государственного управления и их регулирование сводилось к охране государственной тайны и борьбе со шпионажем. Именно поэтому нормативные акты, издаваемые в то время, были во многом направлены именно на регулирование информации в сфере военной тайны и информации, связанной с дипломатическими отношениями и имеющей отношение к внешней безопасности России.

До начала XX века не существовало единой системы охраны государственных секретов. По словам исследователей, «руководство МИДа не предпринимало почти никаких попыток создать комплексную систему защиты информации. И более того, многие чиновники просто не понимали необходимость соблюдать элементарные правила по обеспечению сохранности сведений, содержащих информацию о планах и особенностях проведения внешнеполитического курса Российской Империи»³. В качестве примера можно привести отрывок из воспоминаний министра иностранных дел В. Н. Ламздорфа (1900-1906). Всю жизнь он был связан с центральным аппаратом МИДа. Как писал сам Ламздорф в своем «Дневнике» – «странным является мое положение в данный момент, мои секретные архивы содержат

¹ Колпакиди, А. А., Север, А. Спецслужбы Российской Империи. Уникальная энциклопедия / А. А. Колпакиди, А. Север. – М.: Эксмо, 2010. – 781с.

² Зданович, А. А. Забытое дело подполковника Гримма / А. А. Зданович // Независимое военное обозрение. – 1998. – № 6. – С.1-8.

³ Колпакиди, А. А., Север, А. Спецслужбы Российской Империи. Уникальная энциклопедия / А. А. Колпакиди, А. Север, – М.: Эксмо, 2010. – 781с.

все тонкости политики последнего царствования. Ни молодой государь (Николай II), ни почтеннейший Шишкин, назначенный временно управляющим Министерством иностранных дел, ни имеют не малейшего представления о документах, доверенных в последние годы исключительно и совершенно бесконтрольно мне... Я оказался исключительным обладателем государственных тайн, являющихся основой наших взаимоотношений с другими странами»¹.

Исследователи отмечают, что изначально на законодательном уровне понятие «шпионаж» было достаточно узким. Тогда как в «Инструкции начальникам контрразведывательных отделений», утвержденной 8 июня 1911 г.², был представлен расширенный перечень сведений, разглашение которых соответствовало понятию «Шпионаж». В основном такие сведения относились к военной сфере. В 1912 году был принят новый закон, который был назван многими правоведами того времени одним из самых прогрессивных в Европе³. В законе было расширено и уточнено понятие «государственная измена», а также введено иное определение сведений, составляющих государственную тайну в военной сфере: «это сведения или предметы, касающиеся внешней безопасности России или ее вооруженных сил, предназначенных для военной обороны страны»⁴.

После начала Первой мировой войны были усилены меры по защите информации, которая относилась к военным планам и военным действиям, в том числе путем введения цензуры печати⁵. Такая цензура предусматривала запрет на публикацию в газетах и журналах значительного объема

¹ Чертопруд, С. Организация защиты государственных секретов в МИДе Российской империи в период с 1903 по 1917 год. – (<http://www.agentura.ru/press/cenzura/secret-russia/>). – Дата обращения: 17.12.2017.

² Инструкция начальникам контрразведывательных отделений от 8.06.1911 г. – (http://www.e-reading.by/chapter.php/1004112/36/Linder_Iosif_-_Specsluzhby_Rossii_za_1000_let.html)/ - Дата обращения: 17.12.2017.

³ См. Резанов, А. С. Закон 5 июля 1912 г. о государственной измене путем шпионства в мирное время / А. С. Резанов. – Варшава, 1912.

⁴ Там же.

⁵ Указ об утверждении временного Положения о военной цензуре от 20 июля 1914 г. – (<http://museumreforms.ru/load-document/nojs/13702>). – Дата обращения 17.12.2017.

информации, относящейся к развитию событий, военных действий, техническом и ресурсном оснащении войск. Далее был утвержден «Перечень сведений и изображений, касающихся внешней безопасности России и ее военно-морской и сухопутной обороны, оглашение и распространение коих в печати или в речах или докладах, произносимых в публичных собраниях, воспрещается на основании статьи I отдела II закона 5 июля 1912 года, об изменении действующих законов о государственной измене путем шпионства, и статьи II Высочайшего Указа Правительствующему Сенату от 20 июля 1914 года» (Далее – Указ 1914 года), который включил в себя 25 разновидностей сведений, публикация которых в печати была запрещена. Сведения относились к сфере ведения военных действий, планирования военных операций и состояния дел на фронтах (Считаем необходимым отметить тот факт, что в 1917 г. в основу Декларации правительства от 2 марта 1917 г. был положен принцип, который отменял данный Указ. Так в пункте 2 провозглашалась свобода слова, печати, собраний, стачек и союзов, с распространением политических свобод на военнослужащих в пределах, допускаемых военно-техническими условиями. Таким образом, Указ 1914 года играл при смене режима и политическую роль).

В дальнейшем перечень сведений, предусмотренный Указом 1914 года, с изменением военно-политической обстановки был изменен в 1915 г. «В 1915 г. были добавлены пункты военно- и социально-экономического характера (союзническое снабжение, заготовки для военной промышленности, перебои в ее работе; вместо беспорядков на занятых войсками территориях – «о всякого рода нарушениях обычного течения жизни» в местностях на положении чрезвычайной охраны и военном), а также добавления делового военного характера, видимо, по опыту применения перечня – о результатах неприятельской бомбардировки и о крушении неприятельских кораблей и др.;

Перечень 1916 г. повторял его 30 пунктов без изменений»¹. В дальнейшем до 1917 г. перечни не издавались.

В России стала постепенно формироваться система обозначения информации, охраняемой в качестве государственной тайны, а также стали вводиться определенные меры для ее охраны. Вместе с тем, ошибочным было бы утверждать наличие в стране единой системы защиты информации.

Стоит также отметить, что к государственной тайне в основном относили сведения в сфере военного управления. Как отмечают исследователи, «МИД, Военное ведомство и Департамент полиции самостоятельно прилагали усилия по обеспечению сохранности государственной тайны. При этом Департамент полиции славился своей системой конфиденциального делопроизводства, а МИД и Военное ведомство имели достижения в области криптографии. В то же время предпринимаемые мероприятия носили хаотичный характер и не могли обеспечить эффективной защиты государственных секретов. Молодой Советской республике пришлось разработать и создать эффективную систему защиты государственной тайны»².

В рамках разработки системы защиты государственной тайны было предпринято множество организационных мероприятий, создано, а в дальнейшем реорганизовано множество различных государственных органов. Историю их создания и реорганизации в рамках настоящего исследования мы не будем рассматривать подробно, так как нас интересует по большей части именно правовое регулирование и природа государственных секретов.

Вплоть до 1921 г. не предпринималось никаких попыток упорядочения последовательности обработки, хранения документов, содержащих служебную тайну. Отчасти, полагаем, это было связано с политической

¹ Батулин, П. В. Перечни военной цензуры 1912-1923 гг. / П. В. Батулин // Ленинградский юридический журнал. – 2012. – №4. – С.152-165.

² Чертопруд, С. Зарождение и становление системы защиты государственной тайны в Советском Союзе с 1918 по 1930 год. – (<http://www.agentura.ru/press/cenzura/secret-ussr/>). – Дата обращения: 17.12.2017.

неопределенностью и становлением правовой системы и всего государства в целом. Постановления и иные нормативные акты в основном касались введения военной цензуры. При этом стоит отметить, что в дальнейшем вопросы цензуры и охраны информации, составляющей государственную тайну/тайну управления, будут тесно взаимосвязаны.

Только 13 октября 1921 г. был издан Декрет СНК «Перечень сведений составляющих тайну и не подлежащих распространению», который подразделял сведения на военные и экономические. Перечень состоял из трех глав, в первой из которых были сведения военного характера (отдельно для военного и мирного времени), вторая глава содержала сведения экономического характера о денежном обращении и производстве денег, денежной реформе, валютах, ценных бумагах, импортном и экспортном плане, экспортном фонде, продмаршрутах, обеспеченности топливом и подвижным составом отдельных железных дорог, состоянии милиции, преступности и беспорядках, режиме в местах заключения и т.д.; третья глава была посвящена порядку публикации сведений, запрещенных второй главой (с разрешения наркоматов)¹.

Действующая система все же не позволяла должным образом избежать утечек информации и 30 августа 1922 г. Секретариат ЦК РКП (б) принял постановление «О порядке хранения и движения секретных документов»², которое и положила начало упорядочению секретного делопроизводства.

В дальнейшем формирование регулирования охраняемых сведений в сфере государственного управления, в сфере экономического, политического, общественного и социального развития шло двумя путями:

1) регулирование порядка обращения со сведениями, составляющими государственную тайну и сведениями, не подлежащими

¹ Батулин, П. В. Перечни военной цензуры 1912-1923 гг. / П. В. Батулин // Ленинградский юридический журнал. – 2012. – № 4 – С.152-165.

² Куренков, Г. А. Секретное делопроизводство ЦК (до Великой Отечественной войны). – (<http://www.opentextnn.ru/history/deloproizvodstvo/?id=4897>). – Дата обращения: 17.12.2017.

опубликованию, помеченными грифом «не для печати», «сведения, не подлежащие оглашению».

2) Введение цензуры, которая подразумевала ограничение доступа к ряду периодических изданий, произведений науки, литературы, искусства.

Для контроля за изданием и распространением литературы в 1922 г. был создан Главлит (главное управление по делам литературы и издательства). На него были возложены функции контроля за содержанием издаваемой литературы, а также за соблюдением требования о нераспространении в открытой печати сведений, относящихся к государственной тайне. В дальнейшем полномочия Главлита существенно расширились¹. Главлит издавал перечни сведений, запрещенных к опубликованию в открытой печати, а не только проверял издания на допустимость их содержания. Указанных Перечней до сих пор нет в Интернете, в библиотеках в правовых базах.² Не допускалась публикация сведений, большинство из которых не относилось к государственной тайне. Так в одном из перечней 1976 г. был предусмотрен запрет на публикацию сравнения зарплат советских рабочих с зарплатами рабочих за рубежом, сведений о покупательной способности рубля и иностранных валют, сведения о беспорядках и конфликтах в армии на уровне роты и выше, данные о размере и распределении зарплат в СССР, сведения о крупных авариях на производстве и так далее.

До сих пор сохраняет силу один из перечней информации, устанавливающий категории сведений, публикация которых запрещалась: «Перечень сведений, органов прокуратуры, не подлежащих опубликованию в

¹ Постановление СНК РСФСР от 06.06.1931 «Об утверждении Положения о Главном управлении по делам литературы и издательств и его местных органах» // СУ РСФСР. – 1931. – № 31. – ст. 273.

² Стоит отметить, что изучению истории цензуры посвящены многие научные исследования. См. Например: Горяева, Т. М. История советской политической цензуры, 1917-1991 гг.: автореф. дис. ... докт. ист. н. 07.00.02 / Горяева Т. М. – М., 2000. – 40 с.;

Клепиков, Н. Н. Политическая цензура на Европейском Севере РСФСР/СССР в 1920 - 1930-е гг.: дис. ... ист. н. 07.00.02 / Н. Н. Клепиков. – Архангельск, 2005. – 246 с.

открытой печати, передачах по радио и телевидению»¹. Ряд сведений из перечня составляет профессиональную тайну (тайну следствия, тайну судебного разбирательства), тогда как ряд сведений является «внутренней информацией» органов прокуратуры. При этом указанный перечень содержит запрет на распространение статистической информации. Полагаем, что на данном этапе такое указание противоречит концепции открытости органов государственной власти и праву на доступ к информации.

Также в документе встречаются упоминания о грифах, используемых во внутреннем документообороте государственных органов: грифы «для служебного пользования», «не подлежит опубликованию», «не для печати». Здесь стоит отметить, что уже само такое упоминание говорит об обособлении от государственной тайны целого пласта управленческой информации, доступ к которой был существенно ограничен и регламентирован лишь ведомственными актами, которые чаще всего не были официально опубликованы.

Как отмечают А. А. Прокопенко и А. А. Дрога, впервые нормативное разделение служебной и государственной тайны произошло в 70-е годы XX века². Только в 1984 г. было впервые упомянуто в уголовном кодексе понятие «служебная тайна», при этом вводился отдельный состав преступления, предусматривавший ее разглашение иностранной организации (Ст. 76.1. Передача иностранным организациям сведений, составляющих служебную тайну). Под служебной тайной понимались экономические, научно-технические или иные сведения, отнесенные к служебной тайне и полученные лицом, которому эти сведения были доверены по службе или работе или стали

¹ Приказ Генпрокуратуры СССР от 22 ноября 1971 № 45 «О Перечне сведений органов прокуратуры, не подлежащих опубликованию в открытой печати, передачах по радио и телевидению» // Сайт компании «Консультант Плюс». – (<http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=17318#0>). – Дата обращения: 17.12.2017.

² Прокопенко, А. А., Дрога, А. А. Правовое регулирование оборота информации, относящейся к служебной и профессиональной тайне в органах внутренних дел: монография / А. А. Прокопенко, А. А. Дрога. – Белгород: БелЮИ МВД России, 2011. – 97 с.

известны иным путем. При этом субъектный состав, исходя из формулировки, был достаточно широк.

В 1987 г. утверждена инструкция¹, которая вводила общее понятие «государственные секреты», в которые включалась государственная тайна (с грифами «особой важности», «совершенно секретно»), служебная тайна (с грифом «секретно») и информация «для служебного пользования». При этом за разглашение информации для служебного пользования предусматривалась только административная ответственность.

Пожалуй, этот документ можно назвать одним из наиболее важных официально опубликованных документов, который устанавливал определенную структуру информации ограниченного доступа в системе государственного управления.

Из информации, содержащейся в официально опубликованных документах, можно сделать вывод о том, что сама по себе служебная тайна была механизмом обеспечения нужд государственного управления, которая, с одной стороны, позволяла охранять сведения, распространение которых могло бы повредить системе государственного управления, а с другой стороны, попросту позволяла скрыть огрехи и ошибки политического управления в стране. Все же нанесение различных грифов в министерствах, ведомствах и на предприятиях, таких как «Для служебного пользования», «Не для печати», «Не подлежит опубликованию», давало неограниченные возможности для сокрытия той или иной информации. При этом статус документов с такими грифами не был достаточно определен в официально опубликованных документах. В свою очередь в 1984 году круг сведений, охранявшихся в режиме служебной тайны, был чрезвычайно широк, как и круг субъектов, на которые возлагалась обязанность защиты информации.

Как видим, институт служебной тайны и во времена Советского Союза долгое время не имел четкой юридической базы и какого-либо глубокого

¹ Инструкция по обеспечению режима секретности в министерствах и ведомствах СССР от 12.05.1987 г. № 556-126

теоретического осмысления. По большому счету, в связи с отсутствием требований открытости власти и права на информацию, такое теоретическое осмысление, возможно, было и ненужно, так как институт служебной тайны имел по большей части строго прикладной характер и решал практические задачи.

Как отмечает А. А. Фатьянов, служебную информацию составляли те сведения, которые были в так называемой «буферной зоне»¹. В этом случае сведения сами по себе не могли являться государственной тайной, однако при их интеграции становились государственной тайной, либо являлись производными от нее сведениями.

В 90-х годах XX века произошла смена политической формации, была принята Конституция нового государства, в ст. 55 которой предусмотрено, что права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. В дальнейшем и Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149 от 27.07.2006 (Далее – Закон «Об информации») в ст. 9 закрепил обязательность ограничения доступа к информации только федеральным законом. Вопреки требованиям Конституции РФ и требованиям Федерального закона «Об информации, информационных технологиях и о защите информации», соответствующий федеральный закон не принят до настоящего времени.

Еще в 2004 г. в Государственную Думу РФ вносился проект федерального закона № 124871-4 «О служебной тайне» (далее – Проект закона о служебной тайне), который был отклонен в 2011 году. Также разрабатывался проект федерального закона Министерством экономического развития, однако и он не получил нормативного воплощения.

¹ Фатьянов, А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве): Монография / А. А. Фатьянов. – М.: Изд-во МИФИ, 1998. – С. 138.

Проект закона о служебной тайне был серьезно раскритикован за оценочность используемых категорий. Как отмечают М. И. Гришанков и Е. К. Волчинская, по мнению Правительства РФ, высказанного относительно первой редакции Проекта закона, «законопроект предполагает возможность свободного отнесения к служебной тайне практически любых сведений, за исключением указанных в перечне, установленном проектом. Этот подход может привести к ограничениям прав граждан на получение информации»¹. В этой ситуации логично было бы предположить, что институт служебной тайны при таком подходе должен был изжить себя как необоснованно ограничивающий доступ к информации для граждан. Однако возможность ограничения доступа к информации в режиме служебной тайны не только не исчезла, но и в значительной мере расширилась. Таким образом, Правительство РФ, указав на ограничение конституционных прав и свобод человека и гражданина использованием режима служебной тайны, попросту оставило указанное ограничение доступа к информации вне рамок регулирования федерального закона, вне рамок правового поля.

В настоящее время институт служебной тайны остался в «подвешенном» состоянии, не имея ни достаточного нормативного обоснования, ни системно-структурной принадлежности, ни унифицированного порядка обращения с такой информацией, ни достаточного законного основания для его использования.

На основании изложенного приходим к выводу о том, что на протяжении многих веков государственные дела во многом были закрытой сферой, информация о которых защищалась от лиц, не имеющих доступа. Но механизмы и процедуры защиты служебной информации не были сформированы. При этом в советские времена, как отмечают исследователи, формировались два параллельных института информации ограниченного

¹Гришанков, М. И., Волчинская, Е. К. Некоторые проблемы формирования института служебной тайны в Российской Федерации / М. И. Гришанков, Е. К. Волчинская // Государственная служба. – 2011. – № 2. – С.39-44.

доступа: тайна государственного управления и партийная тайна. Как таковой механизм охраны информации в режиме, приближенном к режиму служебной тайны, строго нормативно не был оформлен и существовал на уровне ведомственных актов. Служебная тайна являлась внутренним механизмом регулирования информации и не находила своего единого нормативного оформления. Всесоюзное нормативное оформление служебной тайны, вписывающее этот институт в систему государственной тайны, появилось только в конце 80-х годов в Инструкции по обеспечению режима секретности в министерствах и ведомствах СССР, утвержденной постановлением Совета Министров СССР от 12.05.87 № 556-126. Однако уже в 90-х годах концепция понимания служебной тайны кардинально изменилась. В ст. 139 ГК РФ упоминалась служебная тайна по аналогии с тайной коммерческой. Образование сведений, охраняемых в режиме служебной тайны, стало возможно не только в органах государственной власти и местного самоуправления (далее – органы г.в. и м.с.у.) и подведомственных организациях, но и в коммерческих организациях. Такое изменение подхода к сущности и регулированию служебной тайны было во многом связано со сменой политического режима и смещением акцентов в сферу защиты частных интересов. Вместе с тем, стоит отметить, что подход, в соответствии с которым служебная тайна могла образовываться и охраняться в коммерческих организациях наравне с коммерческой тайной, существовал до разработки и принятия федерального закона «О коммерческой тайне» от 29.07.2004 № 98-ФЗ, в то время, пока отсутствовали на законодательном уровне правила защиты информации в режиме коммерческой тайны. Ст. 139 содержала следующее определение: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель

информации принимает меры к охране ее конфиденциальности»¹. То есть ранее критерием отнесения информации к сведениям, охраняемым в режиме служебной тайны, была её действительная или потенциальная коммерческая ценность (как было указано ранее, в то время категория «служебная тайна» служила аналогом существующего сейчас понятия «инсайдерская информация» или существующего в других странах понятия «внутренняя информация организации»). В последствии ст. 139 Гражданского кодекса РФ утратила силу и произошел отказ от концепции, в соответствии с которой служебная тайна могла охраняться и в коммерческих организациях.

Из приведенного анализа следует, что исторически служебная тайна не существовала как самостоятельный вид информации ограниченного доступа. В настоящее время объективно возникает потребность вводить ограничения на доступ как в отношении служебной информации, создаваемой в органах власти, так и в отношении информации ограниченного доступа, поступающей в органы власти от других субъектов (за исключением государственной тайны). В настоящее время регулирование служебной тайны осуществляется не на уровне специального федерального закона, а на уровне преимущественно подзаконных нормативных правовых актов. В силу же Конституции Российской Федерации ограничения конституционных прав, том числе права на информацию, должно осуществляться на уровне федерального закона. В связи с этим вопрос о принятии закона, регулирующего отношения в сфере служебной тайны, сегодня стоит очень остро. Принятие данного закона необходимо в том числе и для того, чтобы избежать возможных случаев злоупотребления правом на ограничение доступа к информации.

1.2. Международное и зарубежное регулирование ограничения доступа к информации органов власти

¹ Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 № 51-ФЗ (ред. от 29.07.2017).

В сфере регулирования доступа к информации одним из главных вопросов остается вопрос соотношения принципа информационной открытости и свободы информации с необходимостью обеспечения информационной безопасности. Немаловажным аспектом обеспечения информационной безопасности являются вопросы охраны информации в режимах конфиденциальности, поскольку базовой основой для защиты информации и информационных систем является нормативное установление требований защиты информации. Как отмечает Т. А. Полякова, «значительную роль в объединении мирового сообщества вокруг формирования информационного общества занимают вопросы правового обеспечения информационной безопасности. Важным фактором координации усилий государств является согласованное и комплексное развитие правового регулирования данной сферы общественных отношений»¹. Вместе с тем, одним из важнейших прав человека является право на информацию.

В ст. 19 Всеобщей декларации прав человека (принята Генеральной Ассамблеей ООН 10 декабря 1948 г.) провозглашена свобода «искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ»².

Аналогичные права предусматривает Международный пакт о гражданских и политических правах (принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 г.), а также ст. 10 Конвенции о защите прав человека и основных свобод (заключена в Риме 04 ноября 1950 г. странами-участницами Совета Европы) (далее – Европейская Конвенция). Ст. 10 Европейской конвенции в пункте первом предусматривает право получать и распространять информацию и идеи без какого-либо вмешательства со

¹ Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. ... докт. юрид. наук: 12.00.14 / Т. А. Полякова. – М., 2008. – С. 15.

² Всеобщая декларация прав человека. Принята Резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. – (http://www.un.org/ru/documents/decl_conv/declarations/declhr). – Дата обращения: 17.12.2017.

стороны публичных властей и независимо от государственных границ. Однако п. 2 указанной статьи вводит ряд ограничений для реализации этого права: «Осуществление этих свобод <...> может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности...». По факту же, в зависимости от политической воли в каждой конкретной стране это право может быть во многом ограничено «в интересах национальной безопасности». И вопрос о том, что такое национальная безопасность, каковы критерии обоснованности ограничений свободы доступа к информации до сих пор не является однозначно разрешенным.

Кроме того, несмотря на то, что в Европейской Хартии местного самоуправления (Подписана странами-участниками Совета Европы в Страсбурге 15 октября 1985 г.) принцип гласности не называется прямо, исследователи небезосновательно приходят к выводу о том, что деятельность демократически избранных местных органов, осуществляющих местное самоуправление, должна строиться на принципе гласности и открытости, деятельность органов местного самоуправления должна быть подчинена интересам местного населения.¹ По мнению ученых, анализ ключевых статей Европейской хартии местного самоуправления убедительно доказывает, что принцип гласности местного самоуправления является одним из существенных компонентов его структуры.²

В свою очередь идея информационной открытости была озвучена в Окинавской хартии глобального информационного общества, принятой лидерами «большой восьмерки» 22 июля 2000 г. Хартия являлась призывом к государственному и частному секторам ликвидировать международный

¹ Дементьев, А. Н. Принципы местного самоуправления / А. Н. Дементьев // Право и образование. – 2006. – № 5. – С. 131-135.

² Михеев, Д. С. Закрепление принципа гласности в Европейской Хартии местного самоуправления / Д. С. Михеев // Ученые записки Казанского Университета. – Т.155. – кн. 4. – 2013. – С. 62-68.

разрыв в обладании информацией и знаниями. Основной идеей хартии было то, что повышение прозрачности государственной власти и бизнеса может изменить методы взаимодействия по продвижению социального и экономического прогресса во всем мире¹.

Международные документы в сфере информационной открытости затрагивают вопрос борьбы с коррумпированностью власти. Этой проблеме посвящена «Конвенция Организации Объединенных Наций против коррупции»². При этом в указанной Конвенции требование информационной открытости названо как один из основных факторов, способных обеспечить снижение уровня коррупции. Вопрос национальной безопасности необходимо разрешать в непосредственной связи с правом граждан на информацию. Отчасти необходимость соблюдения такого баланса диктуется положениями Йоханесбургских принципов «Национальной безопасности, свободы выражения мнения и доступа к информации» от 1 октября 1995 г.. Исследователи высказывают позицию, в соответствии с которой «национальная безопасность, свобода самовыражения и доступ к информации установлены в качестве принципов доступа к правительственной информации, которые должны способствовать признанию ограничения свободы самовыражения и свободы информации в интересах национальной безопасности»³.

Однако информационная открытость как таковая не может быть абсолютной и безграничной. И именно вопросы ограничения доступа к информации, пределы доступа к информации являются крайне непростыми в своем практическом разрешении. Так в Рекомендации R (81) 19 «О доступе к

¹ Ковалева, Е.В. Международно-правовое регулирование права доступа к информации / Е.В. Ковалева // Власть. – 2010. – №7 – С. 106-109.

² Конвенция Организации Объединенных Наций против коррупции. Принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 года. – (http://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml). – Дата обращения: 17.12.2017.

³ Морозов, А.В. Организационно-правовое обеспечение информационной безопасности: монография / А.В. Морозов, Т.А. Полякова. – М.: РПА Минюста России, 2013. – 276 с.

официальной информации, находящейся в распоряжении государственных органов», которая была принята комитетом министров Совета Европы, сделано исключение из общей презумпции информационной открытости государственной власти для двух ветвей власти: законодательной и судебной, определено, что информационная открытость не должна быть абсолютной, но, вместе с тем, она должна быть достаточной для достижения своей социальной цели.¹ В то же время, в Рекомендациях Совета Европы «О защите данных и свободе информации» подчеркивается, что демократические режимы характеризуются обращением в обществе максимального объема информации и что *информационные права*, закрепленные в Европейской конвенции о защите прав человека и основных свобод, *должны трактоваться предельно широко*, подразумевая свободу поиска информации и, как следствие, обязанность властей обеспечивать доступность информации по вопросам, имеющим общественное значение (с учетом соответствующих ограничений).² В Конвенции Совета Европы «О доступе к официальным документам» в статье 3 предусматривается ряд случаев, в которых допускается ограничение доступа к информации. Одним из оснований для ограничения доступа к информации является необходимость защиты национальной безопасности, обороны, международных отношений и некоторых других. Можно заметить некое противоречие между положениями рекомендаций Совета Европы. И именно определение границ «необходимости и достаточности» информационной открытости является зачастую предметом спора в Европейском Суде по правам человека (далее – ЕСПЧ)³.

¹ Ковалева, Е. В. Международно-правовое регулирование права доступа к информации / Е. В. Ковалева // Власть. – 2010. – № 7. – С. 106-109.

² Афанасьева, О. Право граждан на информацию и его гарантии / О. Афанасьева // Отечественные записки. – 2004. – № 3 (18). – С. 26-30.

³ На наш взгляд, заслуживают особого внимания указанные дела: Постановление Европейского Суда по правам человека от 10.12.2007 г. Дело «Штоль против Швейцарии» [Stoll v. Switzerland] (жалоба № 69698/01) (Большая Палата) // Бюллетень Европейского Суда по правам человека. Российское издание. – 2008. – № 6.; Постановление Европейского Суда по правам человека от 12.02.2008 г. Дело «Гуджа

На рассмотрении ЕСПЧ часто выносятся вопросы о возможности доступа и разглашения той или иной «чувствительной информации», но каждый раз суд выносит решение, основываясь на конкретных обстоятельствах дела, не имея сколько-нибудь определенных критериев и требований к открытости информации. При рассмотрении споров в Европейском суде по правам человека возникает вопрос о правомерности разглашения той или иной информации, а также о правомерности ограничения доступа к той или иной информации в зависимости от установленного в той или иной стране правового режима информации ограниченного доступа.

«В Парламентской Ассамблее Совета Европы активно ведется изучение соотношения права на доступ к информации и национальной безопасности государства, а также проблемы правового регулирования государственной тайны (например, Resolution 1551 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets). Особое внимание в докладах, обсуждениях и рекомендациях уделяется вопросам разумного ограничения сферы действия государственной и служебной тайны. Во многих докладах и обсуждениях речь идет о недопустимости излишне широкого толкования понятия «национальная безопасность». Национальная безопасность, по мнению участников ассамблеи ПАСЕ (данные положения изложены в Doc. 12548, Reference 3762 of 15 April 2011), не должна служить основанием для сокрытия фактов нарушения прав человека, а также препятствовать защите нарушенных прав. В одном из документов ассамблеи ПАСЕ делается акцент на том, что «непреодолимое противоречие между ограничением и предоставлением доступа к информации усугубляется отсутствием четких правовых рамок и международных стандартов, а также их эффективным осуществлением. Чрезмерно широкие и расплывчатые исключения национальной безопасности для доступа к информации позволяют скрывать

против Молдавии» [Guja v. Moldova] (жалоба № 14277/04) (Большая Палата) // Бюллетень Европейского Суда по правам человека. – Российское издание. – 2008. – № 8.

незаконную деятельность»¹ государственных органов и отдельных должностных лиц, не позволяя заинтересованным лицам защищать свои права в судебном порядке. В результате работы ряда международных организаций, в том числе ПАСЕ, в июне 2013 г. были разработаны «Глобальные принципы национальной безопасности и права на информацию»² (Далее – Глобальные принципы национальной безопасности). Указанный документ носит лишь рекомендательный характер. В указанном документе впервые делается обобщение подходов к пониманию пределов национальной безопасности, а также дается дефиниция базовых определений, используемых при ограничении доступа к информации органами государственной власти. Документ предусматривает подробное описание 50 принципов ограничения доступа к информации.

Несмотря на то, что указанные принципы носят рекомендательный характер, на наш взгляд, их разработка является очень важным этапом в становлении информационной открытости власти. В этих принципах выражена идея оптимального подхода к вопросу соотношения информационной безопасности и доступа к информации.

Как отмечается в юридической литературе, около ста государств приняли законы о праве на информацию³. Устойчивая тенденция принятия таких законов, гарантирующих право на доступ к информации о деятельности органов государственной власти, отмечается с начала 60-х годов XX века. Такие законы были приняты во Франции, Дании, Греции, Голландии, Испании, Италии, Португалии, Бельгии и многих других.

¹ Resolution 1551 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets. – (<http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=17535&lang=en>). – Дата обращения 24.03.2017

² Global principles on national security and the right to information («The Tshwane principles») finalized in Tshwane, South Africa issued on 12 June 2013. – (<https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf>). – Дата обращения: 17.12.2017.

³ Морозов, А. В., Полякова, Т. А. Организационно-правовое обеспечение информационной безопасности: монография / А. В. Морозов, Т. А. Полякова – М.: РПА Минюста России, 2013. – 276 с.

Термин «служебная тайна» является одним из наименее унифицированных, но часто встречающихся терминов в национальных законодательствах различных стран. Термины «служебная тайна», «official secret», «Restricted», «Protect», «Limited Distribution (LIMDIS)», «For Official Use Only (FOUO)», «Sensitive But Unclassified (SBU)», «Controlled Unclassified Information, CUI», «certain official information»¹, «чувствительная информация»², «информация для служебного пользования (ДСП)» встречаются в различных вариациях в законодательствах многих стран, однако смысл данного термина напрямую связан с той правовой системой, в рамках которой он существует. Значение этого термина колеблется от разновидности государственной тайны до информации ограниченного доступа в коммерческих организациях, родственной по своему смыслу и значению профессиональной или коммерческой тайне³. Кроме того, во многих странах система информации ограниченного доступа либо не выстроена вообще, либо излишне усложнена в такой мере, что нет возможности сказать точно, является ли та или иная информация служебной тайной или же государственной тайной, или доступ к ней ограничен без видимых оснований. Иногда терминологические разночтения бывают очень существенны: термином «official secret» в одних странах обозначают правовой режим служебной тайны⁴ (информации о деятельности органов государственной

¹ Многие из этих терминов встречаются в документах США. См., например, The US Classification System. – (<http://electrospace.blogspot.ru/2013/09/the-us-classification-system.html>). – Дата обращения: 17.12.2017.

² Такое обозначение встречается в официальных документах Великобритании. См., например, The best place to find government services and information. – (www.gov.uk). – Дата обращения: 17.12.2017.

³ Так, к примеру, в США понятие «служебной тайны» само по себе достаточно «размытое» и может включать как информацию государственных органов, так и коммерческую тайну. (Зенин, И. А. Гражданское и торговое право капиталистических государств: Учеб. Пособие / И. А. Зенин. – М.: МГУ, 1992. – 192 с.)

⁴ Так, к примеру, в Великобритании с 2014 года была введена новая классификация информации ограниченного доступа, согласно которой понятие «official secrets» или «official information» входит в категорию государственных секретов – см. HMG Security Policy Framework. – (www.gov.uk). – Дата обращения: 17.12.2017.

власти с ограниченным доступом), а в других странах обозначают правовой режим государственной тайны¹.

В связи с тем, что терминология указанных режимов различна, возникают трудности с межгосударственным информационным обменом.

Как такового международного регулирования информации ограниченного доступа, единых стандартов регулирования и соотношения понятий и режимов различных правовых систем нет. В большинстве международных нормативных актов, посвященных праву на доступ к информации, идет отсылка к национальному законодательству напрямую, без установки даже неких общих базовых понятий и систем ограничения доступа к информации.² На определенных этапах становления законодательства об информации такой подход был вполне разумным и обоснованным, однако на этапе усиления роли международного законодательства и расширения международных связей, такой подход перестает быть оправданным. Возникает ряд проблем, связанных с отсутствием единства терминологии в сфере ограничения доступа к информации и несоответствием схожих правовых институтов в различных системах права.

Так, в частности, возникает вопрос о режиме информации и мерах её защиты при международном обмене информацией ограниченного доступа (будь то государственная, служебная или коммерческая тайна). В научной литературе отмечается «наличие тенденции к возрастанию по мере развития процессов глобализации значения международно-правового регулирования» информационных правоотношений³. В последнее время на международном уровне принимаются различные соглашения, направленные на укрепление международной информационной безопасности. В то же время, стоит

¹ Например, Нидерланды (The Official Secrets Act 1951), Индия (Official Secrets Act), а также такое обозначение используется в Ирландии и Малайзии.

² См., например, Международный пакт о гражданских и политических правах от 16.12.1966 года, Ст. 10 Европейской конвенции о защите прав человека и основных свобод ETS № 005.

³ Тедеев, А. А. Формирование доктринального понимания сущности источников информационного права / А. А. Тедеев // Вопросы правообразования. – 2010. – №1. – С. 111.

отметить, что в таких соглашениях во многом речь идет о противодействии терроризму и киберугрозам. В то же время, как мы можем наблюдать, регулирование конкретных мер безопасности в области межгосударственного обмена осуществляется только на уровне конкретных соглашений между странами¹.

В январе 2015 г. странами-участниками ШОС в ООН было внесено предложение о принятии «Правил поведения в области обеспечения международной информационной безопасности»². В указанных правилах предусмотрены, как и в большинстве международных актов в сфере права на информацию, два основания для ограничения права на информацию: «а) для уважения прав и репутации других лиц; б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»³. При этом, как и в иных актах, отсутствует конкретизация понятий государственной безопасности, общественного порядка, здоровья и нравственности населения. Следует также отметить, что в настоящее время в большинстве принимаемых международных договоренностях освещаются проблемы кибербезопасности и террористической угрозы, при этом акцент на безопасность межгосударственного информационного обмена не делается. Таким образом, на наш взгляд, недооцениваются внутренние угрозы безопасности, которые, так или иначе, существуют в любом государстве и органе г.в. и м.с.у.

На международном уровне классификация информации, доступ к которой ограничен, отсутствует. Нормативные акты, которые содержат классификацию информации, чаще всего являются региональными актами

¹ См. подробнее: Волчинская, Е. К. Ограничение доступа к служебной информации: административно-правовые аспекты // магистерская диссертация. – Челябинск, 2014. – С.41-62.

² Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. – (<http://www.mid.ru/documents/10180/882233/A+69+723+Ru.pdf/269baca6-5664-4651-b1a9-74e640262173>). – Дата обращения: 17.12.2017.

³ Там же. Стр. 6.

(модельными, рамочными законами некоторых государств) и зачастую противоречат друг другу и национальному законодательству договаривающихся государств (особенно наглядно это отразилось в некоторых модельных законах Содружества Независимых Государств и национальном законодательстве стран СНГ, о котором будет сказано позже).

Следует отметить, что на международном уровне отсутствует какое-либо терминологическое единство в сфере информации ограниченного доступа. Так, например, в США единое понятие «государственная тайна» не используется, информация подразделяется в зависимости от степени ее «чувствительности»¹. Категория информации, близкая к государственной тайне по смыслу, определяется как «Информация в области национальной безопасности».

При этом о недостатках правового регулирования ограничения доступа к информации на международном уровне говорят всё чаще. Одним из наиболее полных и интересных является анализ истории и практики вопроса, приведенный в докладе РАСЕ (Комитет по юридическим вопросам и правам человека)². В связи с этим считаем необходимым рассмотреть концепции служебной тайны, существующие в мире.

В СССР существовало интегрированное понятие государственных секретов. Однако после принятия закона РФ от 21 июля 1993 г. «О государственной тайне» (далее – Закон о государственной тайне) понятие «служебная тайна» было исключено из сферы регулирования указанного закона. В современном российском законодательстве институт служебной тайны так и не получил должного законодательного регулирования. В свою очередь, в бывших союзных республиках, таких как Армения, Белоруссия и Казахстан, в законодательстве была перенята концепция государственных

¹ Executive Order 13526 of December 29, 2009 Classified National Security Information. – (<http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf>). – Дата обращения: 17.12.2017.

² Текст доклада депутата Христоса Пургуридиса, представленного в Парламентской Ассамблее Совета Европы 19.04.2007 г. Депутаты ПАСЕ. – (<http://www.agentura.ru/dossier/russia/process/pace/>). – Дата обращения: 17.12.2017.

секретов СССР и сейчас в этих странах служебная тайна входит в систему государственной тайны¹ (либо государственных секретов). Такая же концепция отражена и в модельных законах Межпарламентской Ассамблеи государств-участников СНГ².

В законодательстве Республики Беларусь идет следующее разделение государственных секретов: государственная тайна и служебная тайна. Причем разделение государственной и служебной тайны идет в зависимости от того, какой вред национальной безопасности может быть нанесен в результате разглашения. В отношении государственных секретов говорится о возможном тяжком вреде для национальной безопасности, применительно к служебной тайне речь идет о возможном существенном вреде национальной безопасности в результате разглашения. Во многом, следуя традиции охраны управленческой информации в СССР, в Республике Беларусь гриф «Секретно» относится именно к служебной, а не к государственной тайне. При этом оформление доступа к служебной тайне производится в соответствии с определенной процедурой, схожей с процедурой допуска к государственной тайне.

Следует отметить, что такая правовая позиция, несмотря на свою привлекательность и простоту регулирования, всё же не лишена недостатков. Так, к примеру, будем исходить из той позиции, что к служебной тайне следует относить сведения о деятельности государственного органа, сохранение в тайне которых диктуется служебной необходимостью, а также

¹ Закон Республики Беларусь от 19.07.2010 г. № 170-З «О государственных секретах» // Сайт комитета государственной безопасности Республики Беларусь. – (<http://www.kgb.by/ru/zakon170-3/>). – Дата обращения: 17.12.2017.

Закон Республики Казахстан от 15.03.1999 года № 349-І «О государственных секретах» // «Казахстанская правда». – 1999. – № 53 (22770).

Закон Республики Армения от 30.12.1996 года № ЗР-94 «О государственной и служебной тайне» // Официальные ведомости Республика Армения. – 1996 года. – № 23-24 (1123-1124). – Ст. 298.

² См. например: Постановление Межпарламентской ассамблеи государств-участников СНГ от 16.06.2003 № 21-10 «О модельном законе «О государственных секретах» // Информационный бюллетень Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств. – 2003. – №31.

информацию, относящуюся к иной охраняемой законом тайне, предоставленной в государственный орган юридическими или физическими лицами (так называемая «чужая тайна»)¹. Если исходить из указанной позиции, то отнесение «чужой тайны» в разряд государственных секретов будет противоречить логике, поскольку информация, которая предоставляется физическими и юридическими лицами является информацией частной (охраняемой законом в качестве банковской тайны, коммерческой, личной, тайны семейной жизни и т.д.) и переводить такую информацию в разряд государственных секретов было бы не совсем корректно. Кроме того, на наш взгляд, оформление допуска в порядке, аналогичном допуску к государственной тайне, в значительной степени способно будет усложнить порядок работы со служебной тайной, если только не будет предусмотрен иной порядок допуска к такой категории сведений. Также остается вопрос об ответственности за нарушение такого режима охраны информации, поскольку за разглашение государственной тайны предусматривается уголовная ответственность, а за разглашение служебной тайны такой ответственности на данный момент нет.

Вторая позиция, которая существует в практике регулирования других стран – это существование законодательного регулирования только государственной тайны. Стоит отметить, что при изучении данного вопроса, возникают серьезные трудности перевода и понимания различных правовых категорий, связанные с отсутствием единого, выработанного в международной практике, понятийно-категориального аппарата института государственной/служебной тайны. В качестве примера государства, определяющего государственную тайну в общем, в докладе РАСЕ (Комитет по юридическим вопросам и правам человека) приводится законодательство

¹ Такая позиция встречается как в Проекте закона о служебной тайне, так и в работах ряда исследователей:

Волчинская, Е. К. Ограничение доступа к служебной информации: административно-правовые аспекты // магистерская диссертация. – Челябинск, 2014. – С.24.;

Занина, Т. М. Кораблев, П. Н. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 31-34.

Испании: статья 2 закона Испании «О служебной тайне» определяет служебную тайну как «факты, действия, документы, сведения, данные и объекты могут быть объявлены секретными, «если осведомленность о них неуполномоченных лиц может нанести ущерб или поставить под угрозу безопасность и обороноспособность государства»¹. С одной стороны, такая позиция интересна тем, что происходит достаточно четкое законодательное регулирование охраны тех или иных сведений, с другой же стороны, возникает вопрос относительно возможности дифференциации сложности процедуры доступа к определенным видам тайн и дифференциации ответственности за разглашение информации. При таком подходе возможны две крайности в правовом регулировании: либо будет достаточно громоздким и дорогостоящим механизм охраны государственной тайны (так как большой объем информации будет подлежать охране), либо будет открыт для доступа большой объем информации, относящейся к деятельности государственных органов и должностных лиц.

Существует также третья концепция, согласно которой государственная и служебная тайна различны по своему содержанию. Так в Венгрии вопросы государственной и служебной тайны определяются Законом «О государственной и служебной тайне» № LXV, принятым в 1995 году. Согласно ст. 41, 61, к служебной тайне относятся «данные, засекреченные лицами, которым разрешено выполнять такое засекречивание, данные, опубликование до окончания срока секретности которых, неразрешенное приобретение или использование, или передача лицу без соответствующего разрешения может разрушить деятельность организации, исполняющей государственные или общественные обязанности, и препятствует достижению данной организацией своих целей и применению *власти* способом,

¹ Текст доклада депутата Христоса Пургуридиса, представленного в Парламентской Ассамблее Совета Европы 19.04.2007 г. Депутаты ПАСЕ. – (<http://www.agentura.ru/dossier/russia/process/pase/>). – Дата обращения: 17.12.2017.

свободным от неразрешенного влияния»¹. Закон Литовской Республики от 25 ноября 1999 г. № VIII-1113 «О государственной и служебной тайнах» также предусматривает различие в содержании служебной и государственной тайн, кроме того, отличительной особенностью законодательства Литовской республики является наличие детализированного перечня сведений, которые могут охраняться в режиме служебной тайны. Также различие в правовом режиме государственной и служебной тайны есть и в законодательстве Польши.² При таком правовом подходе есть один существенный недостаток: значительная сложность в выработке единого подхода к пониманию и регулированию «служебной тайны», и, как следствие, отсутствие единого понимания правовых категорий, возникающее при международном сотрудничестве в том случае, когда необходимо предпринять те или иные меры к обеспечению безопасности и сохранению в тайне передаваемой или получаемой информации. Различие правового регулирования служебной и государственной тайн также существует и в Германии.

В странах с англо-саксонской системой права, применяется концепция, в соответствии с которой определяется только степень важности и «чувствительности» информации. Так, например, в США понятия служебная и коммерческая тайна часто совпадают в своем значении.³ Это связано с тем, что в США большую роль играет также сохранение в секрете не только информации, составляющей коммерческую тайну, но и внутренней информации предприятия. Такая информация, как правило, называется либо «инсайдерская информация», либо «непубличная информация» предприятия⁴.

¹ Римаренко, Ю. І. Приватне життя і поліція. Концептуальні підходи. Теорія та практика / Ю. І. Римаренко. – К.: КНТ, 2006. – 740 с.

² Текст доклада депутата Христоса Пургуридиса, представленного в Парламентской Ассамблее Совета Европы 19.04.2007 г. Депутаты ПАСЕ. – (<http://www.agentura.ru/dossier/russia/process/pase/>). – Дата обращения: 17.12.2017.

³ Соболева, В. Служебная тайна и коммерческая тайна: о чем должен молчать профессионал / В. Соболева // Секретарское дело. – 2009. – №3. – С. 20-25.

⁴ Policy Statement on Inside Information and Securities Trading. – (<http://www.usamobility.com/pdf/InsiderTradingPolicyStatement.pdf>). – Дата обращения: 17.12.2017.

Подобный подход имел место и в законодательстве нашей страны, когда в ст. 139 Гражданского кодекса РФ было введено понятие «служебная тайна» наравне с понятием «коммерческая тайна».

Вместе с тем, считаем, что в таких странах как Канада, Великобритания и США последние 10 лет проявилась тенденция упорядочивания классификации информации в сфере государственного управления: так, к примеру, в США в акте¹ 2009 года была приведена классификация информации, циркулирующей в органах государственной власти. Схожей по статусу со служебной тайной можно назвать информацию, обозначаемую как «контролируемая несекретная информация» CUI², для которой предусмотрены конкретные категории защищаемой информации, а также лица, допускаемые для работы с указанной информацией.

В Канаде существует схожая классификация информации ограниченного доступа³, при этом есть также и маркировка так называемой «защищенной» информации⁴, но она не является той информацией, которая охраняется в органах государственной власти.

В связи с указанным, полагаем, что правовое регулирование информации ограниченного доступа в сфере государственного управления таких стран англо-саксонской системы права само по себе не образует

Стандарты информационной политики в системе CFA. – (<http://www.investopedia.com/exam-guide/cfa-level-1/ethics-standards/standard-nonpublic-information.asp>). – Дата обращения: 17.12.2017.

¹ Executive Order 13526 of December 29, 2009 by President of the United States Classified National Security Information. – (<https://www.archives.gov/isoo>). – Дата обращения: 17.12.2017.

² Подробнее можно посмотреть классификацию Controlled Unclassified Information. – (<https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf>). – Дата обращения: 17.12.2017.

CUI Registry - Categories and Subcategories. – (<https://www.archives.gov/cui/registry/category-list>). – Дата обращения: 17.07.2017.

³ Security of Information Act, Canada, R.S.C., 1985. с. O-5. – (<http://laws-lois.justice.gc.ca/eng/acts/O-5/FullText.html>). – Дата обращения: 17.12.2017.

⁴ Chapter 5 - Handling and Safeguarding of Classified and Protected Information and Assets. – (<http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/ch5-eng.html>). – Дата обращения: 17.12.2017.

отдельную модель регулирования информации ограниченного доступа в органах государственной власти.

Исходя из изложенного, на основании изучения опыта регулирования ограничения доступа к информации в сфере государственной власти, нами выявлены три основных модели регулирования в зависимости от единства и дифференциации используемых правовых режимов информации, в которых охраняются сведения, существующие в органах власти:

1. Модель, в основу которой положена категория «государственные секреты» (в нее, в том числе, входит такая категория, как «служебная тайна»);
2. Модель, которая характеризуется использованием единственной категории – информации ограниченного доступа в сфере управления (государственная либо служебная тайна – наименование единого института зависит от особенностей перевода);
3. Модель, которая характеризуется разграничением правового режима государственная и служебная тайн.

На уровне Межпарламентской Ассамблеи стран СНГ существует ряд модельных законов в области права на информацию. В 2004 г был принят «Модельный закон о праве на доступ к информации»¹, в качестве одной из целей его принятия в нем указано «обеспечение информационной открытости деятельности органов государственной власти, иных государственных органов и организаций, органов местного самоуправления»². В указанном модельном законе раскрыто понятие «право на доступ к информации» как «право каждого гражданина свободно осуществлять поиск информации и

¹ Модельный закон о праве на доступ к информации. Принят в г. Санкт-Петербурге 17.04.2004 Постановлением 23-14 на 23-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2004. – № 34. – С.258 - 270.

² Модельный закон о праве на доступ к информации. Принят в г. Санкт-Петербурге 17.04.2004 Постановлением 23-14 на 23-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2004. – № 34. – С.258 - 270.

получать ее от государственных органов и организаций, иных органов и организаций, наделенных государством властными полномочиями, органов местного самоуправления (далее - органов и организаций), их должностных лиц, обладающих этой информацией на законных основаниях»¹. Таким образом, сфера регулирования данного акта значительно уже сферы доступа к информации в целом. Любопытным является тот факт, что в первой статье модельного закона дано определение понятию «общественный интерес» как «интерес любого лица (лиц), связанный с обеспечением благополучия, стабильности, безопасности и устойчивого развития общества»². В решениях международных судов категория «общественного интереса» является своего рода противовесом категории «национальной безопасности» и одним из гарантов обеспечения доступа к информации, однако в модельном законе указанное понятие в самом тексте не используется и не используется ни в качестве основания для оспаривания законности и обоснованности ограничения доступа к информации, ни в качестве основания для предоставления доступа к информации.

В структуру режимов информации ограниченного доступа в указанном модельном законе входят следующие режимы: государственные секреты; коммерческая тайная; служебная тайна; персональные данные; тайна личной жизни.

Для нас, с точки зрения изучения места служебной тайны в системе информации ограниченного доступа, представляют интерес используемые в различных нормативных актах структуры режимов информации ограниченного доступа. В данном случае режим государственных секретов отделен от служебной тайны, что, на наш взгляд, не вполне корректно, поскольку в странах, где существует режим государственных секретов, служебная тайна входит в структуру государственных секретов, а в странах,

¹ Там же.

² Там же.

где служебная тайна выделяется отдельно, существует режим «государственной тайны», но не государственных секретов.

Буквально на следующий год был принят «Модельный закон об информатизации, информации и защите информации»¹, в котором большое внимание уделено праву на доступ к информации.

Полагаем, что он должен был появиться раньше своего предшественника, поскольку в нем раскрываются основополагающие вопросы информационной открытости. Так в указанном Модельном законе уделено внимание определению сущности права на доступ к информации. Право на доступ к информации понимается как право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. При этом существенно то, что в законе предусмотрено важное условие ограничения права на информацию: ограничение должно быть необходимым, обоснованным и соразмерным, не затрагивающим самого существа настоящего права. На наш взгляд, это фундаментальное положение для понимания оснований ограничения доступа к информации, поскольку основной смысл в праве на доступ к информации заключается в том, что ни одно из положений законодательства не должно это право нивелировать. Важно также то, что в Модельном законе сделана попытка классификации режимов информации ограниченного доступа, конфиденциальная информация в данном случае выступает родовым понятием для иной информации ограниченного доступа (отметим, что в Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» содержалось понятие «конфиденциальная информация», тогда как в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. №149 законодатель отказался от

¹ Модельный закон об информатизации, информации и защите информации Принят в г. Санкт-Петербурге 18.11.2005 Постановлением 26-7 на 26-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2006. – № 37. – С. 188-222.

использования термина «конфиденциальная информация» в пользу термина «конфиденциальность информации», как свойства информации, доступ к которой должен быть ограничен).

Схему, использованную в Модельном законе можно представить следующим образом: в понятие «конфиденциальная информация» входит информация о частной жизни лица и информация персонального характера; коммерческая тайна; служебная тайна; профессиональная тайна; государственная тайна; иные виды тайн, в том числе тайна следствия и тайна судопроизводства. Интересно отметить, что в данной структуре служебная тайна отделена от государственной тайны, в Модельном законе нет упоминания о государственных секретах, что противоречит использовавшимся формулировкам в Модельном законе. Также представляет интерес способ выстраивания системы информации ограниченного доступа, в соответствии с важностью охраняемых интересов, где первостепенную роль играет именно защита интересов личности, частного интереса и только потом – интересов, охраняемых путем введения режимов служебной и государственной тайны.

В данном случае вполне справедлив открытый перечень информации ограниченного доступа, однако на наш взгляд, не совсем понятно, по какому основанию отдельно выделена тайна следствия и судопроизводства. Интересным представляется и тот факт, что в Модельном законе упоминается не только ограничение доступа к информации, но также и ограничение распространения информации, однако, на наш взгляд, этот вопрос недостаточно полно освещен. В частности, освещен лишь вопрос достоверности информации и согласия получателя, в то время как ограничения распространения информации гораздо шире.

Еще одним модельным актом, который должен был стать базовым документом в унификации законодательства стран-участниц СНГ, является

Модельный информационный кодекс 2012 г.¹, который, в свою очередь, противоречит первым двум модельным законам используемыми формулировками и систематизацией. В кодексе выделяется такой вид информации как информация с ограниченным доступом. При этом по правовому режиму она, в свою очередь, подразделяется на конфиденциальную и секретную. При этом в указанном акте также упоминается государственная тайна и другие тайны, предусмотренные законом. В то же время, в Модельном законе стран-участников СНГ «Об информации, информатизации и обеспечении информационной безопасности»² дается следующая классификация информации ограниченного доступа: государственные секреты, коммерческая тайна, служебная информация ограниченного распространения, персональные данные, профессиональная тайна, тайна личной жизни. В данном случае не учтен тот момент, что в тех странах, в которых используется понятие «государственные секреты», в него входит и государственная тайна, и служебная (к примеру, Республика Казахстан, Республика Беларусь, Республика Узбекистан, Кыргызская республика, Республика Туркменистан). В данном случае излишне дублировать отдельно понятие «служебная информация», если же законодатель в этом случае имел что-то кроме внутренней информации о деятельности государственных органов, то в данном случае необходимо разъяснение данного положения, которого в тексте нормативного акта нет.

Базовые модельные законы, которые должны стать основой единого правового регулирования информации в странах СНГ зачастую противоречат

¹ Модельный информационный кодекс для государств-участников СНГ. Принят в г. Санкт-Петербурге 23.11.2012 Постановлением 38-6 на 38-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2013. – №57 (часть 1). – С. 44 - 73.

² Модельный закон «Об информации, информатизации и обеспечении информационной безопасности». Принят в г. Санкт-Петербурге 28.11.2014 Постановлением 41-15 на 41-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Сайт компании «Консультант Плюс». – <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=41358#0>. – Дата обращения: 17.12.2017.

друг другу, в результате чего не могут быть положены в основу единого правового регулирования.

Кроме того, на основании изложенного можно сказать о том, что в модельных законах стран СНГ отсутствует согласованность и иерархия принимаемых нормативных актов, которая помогла бы решить проблемы коллизий нормативных актов хотя бы на региональном уровне. В то же время, принятие на международном уровне модели базового регулирования межправительственного обмена информацией с установлением обязательного круга информации, доступ к которой может быть ограничен с определенными организационными и технологическими требованиями, могло бы значительно упростить межправительственный и межгосударственный обмен информацией, а также лечь в основу единой информационной политики.

1.3. Правовое регулирование служебной тайны в России

В российском законодательстве идея информационной открытости получила свое отражение только в начале девяностых годов прошлого века после провозглашения нашей страны демократическим государством. Идеи информационной открытости впервые были закреплены в ст. 29 Конституции Российской Федерации, отразившись в праве граждан на доступ к информации, а также в ч. 3 ст. 55 Конституции, предусматривающей возможность ограничения прав и свобод только федеральным законом. Во многом необходимость информационной открытости была продиктована политическими процессами демократизации и реформированием всего общества, вхождением России во многие международные организации, присоединением к международным актам в сфере права на доступ к информации. В дальнейшем принцип гласности деятельности органов государственной власти нашел свое отражение во многих нормативных актах:

ст. 3 ФКЗ «О Правительстве Российской Федерации» выделяет гласность как основной принцип деятельности правительства¹.

Вместе с тем, Т. А. Полякова отмечает, что практика формирования нормативной правовой базы носит недостаточно системный характер, не всегда в должной мере учитывает рекомендации международных организаций, членами которых является Российская Федерация².

Основы правового регулирования информационной открытости общества и власти были закреплены в федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в котором открытость информации о деятельности органов г.в. и м.с.у., свободный доступ к такой информации является одним из основополагающих принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Помимо базовых требований информационной открытости, в 2013 г. в указанный федеральный закон было внесено важное изменение, введившее такую категорию как «открытые данные», под которой понимается «общедоступная информация о деятельности государственных органов и органов местного самоуправления», которая «предоставляется государственными органами и органами местного самоуправления»³. Опубликование открытых данных осуществляется на сайте государственного органа в сети Интернет. Указанный нормативный акт⁴ дает достаточно подробный и обширный список сведений, которые должны размещаться в сети Интернет в форме открытых данных (ст. 13). Обширный перечень

¹ О Правительстве Российской Федерации: федер. конституц. закон от 17.12.1997 № 2-ФКЗ (ред. от 28.12.2016).

² Полякова, Т.А. Доктрина информационной безопасности России: правовые вопросы модернизации / Т.А. Полякова // Информационное право: актуальные проблемы теории и практики: сб. докладов науч.-практ. конференции, 3 апреля 2015 г. / ред. совет: Ю.Л. Васильченко, И.М. Рассолов, С.Г. Чубукова. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2015. – С. 18-34.

³ Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 09.02.2009 г. № 8-ФЗ (ред.от 09.03.2016).

⁴ Там же.

общедоступной информации представлен в ряде подзаконных нормативных актов.¹ Следует отметить, что помимо устоявшегося разделения информации на общедоступную и информацию ограниченного доступа², некоторые исследователи выделяют в категории общедоступной информации такую информацию, как «информация, представляющая особую социальную значимость» и информация, составляющая общественное достояние³.

В то же время, в литературе ставится вопрос относительно того, насколько информационная свобода может быть безграничной, чем она может быть ограничена безотносительно информации ограниченного доступа⁴. В соответствии с принципом открытости ст. 9 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» устанавливается требование о том, что доступ к информации может ограничиваться только на основе федерального закона. Такое требование является одним из основополагающих для обеспечения реального права на доступ к информации, наряду с требованиями Конституции РФ и Закона об информации.

¹ Постановление Правительства РФ «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных». Постановление Совета Федерации Федерального Собрания РФ «Об информации о деятельности Совета Федерации Федерального Собрания Российской Федерации, размещаемой в сети Интернет» от 25.12.2009г. № 556-СФ (ред. от 29.01.2014) Постановление Государственной Думы Федерального Собрания РФ «Об обеспечении доступа к информации о деятельности государственной Думы Федерального Собрания Российской Федерации» от 23.12.2009г. № 3018-5 ГД (ред. от 14.11.2012).

Приказ Следственного комитета РФ «Об утверждении Инструкции о порядке ведения официального сайта Следственного комитета Российской Федерации в сети Интернет» от 30.09.2011г. № 141. и др.

²Копылов, В.А. Информационное право //В.А. Копылов. – М., 2005. – С. 44-47.

³Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства: Монография / Л.К. Терещенко. – М.: ИНФРА-М, 2013. – 227 с.

⁴Кузнецов, П.У. К вопросу об информационной свободе как правовой категории гражданского общества / П.У. Кузнецов // Информационное право и становление основ гражданского общества в России. Материалы теоретического семинара по информационному праву 2007г. – М: ИГП РАН, 2008. – С.31-36.

В то же время законодательство об ограничении доступа к информации не в достаточной мере систематизировано и структурировано. Как отмечают исследователи, «развитие законодательства об информации ограниченного доступа, в том числе определение принципов соотношения видов тайн и формирования соответствующих правовых режимов конфиденциальности, законодательное урегулирование режима служебной тайны»¹ является одной из приоритетных задач правового обеспечения информационной безопасности.

В настоящее время федеральными законами предусмотрено более 50 видов информации ограниченного доступа².

Попытки классификации информации как общедоступной, так и информации ограниченного доступа, неоднократно предпринимались как на теоретическом уровне, так и на уровне законодательном. В настоящее время нельзя сказать о том, что существует единая позиция в подходе к построению системы информации ограниченного доступа. Так, к примеру, Закон об информации подразделяет информацию «в зависимости от категории доступа на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)»³. На наш взгляд, необходимо также выделить такую категорию как «информация ограниченного распространения», которую необходимо отличать от категории информации ограниченного доступа. Она, в свою очередь, включает в себя различные условия и ограничения распространения информации в зависимости от ее содержания. Так, в частности, информация ограниченного

¹ Полякова, Т. А. Доктрина информационной безопасности России: правовые вопросы модернизации / Т. А. Полякова // Информационное право: актуальные проблемы теории и практики: сб. докладов науч.-практ. Конференции, Москва, 3.04.2015 г. / ред. Совет: Ю. Л. Васильченко, И. М. Рассолов, С. Г. Чубукова. – М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2015. – С. 18-34.

² Перечень нормативных актов, относящих сведения к категории ограниченного доступа // Сайт компании «Консультант плюс». – (http://www.consultant.ru/document/cons_doc_LAW_93980/). – Дата обращения: 17.12.2017.

³ Бундин М. В. Система информации ограниченного доступа и конфиденциальность / М. В. Бундин // Вестник ННГУ. – 2015. – №1.

распространения может отличаться в зависимости от возрастной категории лиц, на которую рассчитана информация, от способа ее распространения либо контекста ее использования (запрет пропаганды гомосексуализма, запрет экстремистской литературы, запрет демонстрации нацистской символики и т.д.).

Однако вопрос о системе информации ограниченного доступа до сих пор является неразрешенным. А. В. Минбалеев отмечает, что «данный классификационный критерий является ключевым в механизме правового регулирования информационных отношений. Именно на основе закрепления права каждого на информацию и возможных его ограничениях в государстве устанавливаются различные правовые режимы доступности информации»¹.

Исходя из порядка закрепления информации в ст. 9 в ч. 3 ст. 5, составлена классификация информации в зависимости от условий распространения:

- 1) информация, свободно распространяемая;
- 2) информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информация, распространение которой в Российской Федерации ограничивается или запрещается.

В ст. 9 закона об информации указываются следующие виды информации ограниченного доступа:

1. государственная тайна;
2. коммерческая, служебная и иная тайна, обязательность соблюдения конфиденциальности которой устанавливается федеральным законом;

¹ Минбалеев, А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: дис. ... докт. юрид. наук. / А. В. Минбалеев. – Челябинск, 2012. – С. 79.

3. профессиональная тайна¹.

Законом также устанавливается запрет требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну; устанавливается порядок доступа к персональным данным в соответствии с законом о персональных данных².

Следует отметить, что сами по себе персональные данные не относятся в полной мере к информации ограниченного доступа, однако порядок их обработки, получения и передачи оговорен в федеральном законе.

Считаем, что указанная в ст. 9 классификация информации ограниченного доступа построена на основании критерия степени защиты той или иной информации, а не на степени важности для общества той или иной информации. Хотя такая точка зрения является достаточно спорной: если сопоставить законодательство об информации с уголовным законодательством и провести логические параллели, то вспомнится именно то, что расположение глав в Уголовном кодексе Российской Федерации в особенной части построено на основании важности защищаемых общественных интересов, и первой главой, открывающей особенную часть, является глава преступлений против личности. Кроме того, в Конституции Российской Федерации первой главой обозначены основы конституционного строя, в котором первое место отдано положению о том, что Российская Федерация является демократическим государством. Во второй статье речь идет о том, что человек, его права и свободы являются важнейшей ценностью. Таким образом, законодатель подчеркивает значимость закрепляемых в Конституции Российской Федерации положений. Кроме того, аналогичный принцип расположения закрепляемых положений в зависимости от степени их значимости можно увидеть и в других нормативных актах. В то же время, представленное расположение информации в федеральном законе приводит к

¹ Ст. 9 Закона об Информации.

² О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017).

выводам о том, что в системе законодательного регулирования приоритетное место отдается именно охране государственной тайны, в то время как личная тайна и персональные данные расположены ниже. На наш взгляд, такой подход не является оптимальным в демократическом обществе, в котором приоритетной является именно охрана личности.

Кроме указанной классификации, существует классификация конфиденциальной информации, которая дана в Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (Далее - Указ Президента РФ №188).

Содержание режима служебной тайны раскрывается в двух подзаконных актах: Указе Президента РФ №188 и постановлении Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (Далее – постановление Правительства РФ №1233).

Следует отметить, что юридический статус этих двух документов не позволяет говорить о надлежащем закреплении режима служебной тайны: Указ Президента РФ №188 не только принят в нарушении требований Конституции Российской Федерации и Закона об информации, поскольку вводит ограничение на доступ к информации, не являясь федеральным законом, а также давно противоречит действующему законодательству. Так в п. 3 указано, что к сведениям конфиденциального характера относятся служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна). Однако из Гражданского кодекса Российской Федерации в 2006 г. была исключена ст. 139, которая содержала положения о служебной тайне. Этот Указ был принят в дополнение к Указу Президента Российской Федерации от 23.05.1996 № 763 «О порядке

опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» (Далее – Указ Президента РФ №763), который содержит порядок вступления в силу нормативных актов. В п. 8 Указа Президента РФ № 763 установлена необязательность официального опубликования нормативных актов, затрагивающих права, свободы, законные интересы граждан, если они содержат сведения, составляющие государственную тайну или конфиденциальную информацию¹, что прямо противоречит ч. 3 ст.15 Конституции Российской Федерации, в соответствии с которой «любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения»². Кроме того, исходя из анализа смысла указанных актов во взаимосвязи, можно сделать вывод о том, что сам Указ Президента РФ № 188 не является регулирующим актом, не может устанавливать режим ограничения доступа к информации и основания для ограничения доступа. Указ должен выполнять функцию систематизации: упорядочивать те основания для ограничения информации, которые уже существуют в федеральных законах. Данный Указ, исходя из содержания преамбулы, принимался «в целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти»³, а не в целях введения самостоятельных оснований для ограничения доступа к информации. Вместе с тем, даже в судебной практике Верховного суда часто идет отсылка к

¹ См. также Павлов, И. Ю. Правовое обеспечение доступа к официальной информации: автореф. дис. ... канд. юрид. наук: 12.00.14 / Павлов И. Ю. – М.: ИГП РАН, 2008. – 34 с.

² Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993. – 25 дек. – Ст. 15.

³ Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6.03.1997 № 188 (ред. от 13.07.2015).

данному Указу как обоснованию возможности ограничения доступа к информации в том или ином режиме¹.

Постановление Правительства РФ № 1233, как и Указ Президента РФ №188 не может устанавливать ограничение доступа к информации в режиме служебной тайны в соответствии с требованиями Конституции Российской Федерации и Закона об информации. Исходя из названия, указанное постановление Правительства Российской Федерации имеет достаточно узкую сферу регулирования – порядок работы со служебной информацией ограниченного доступа, однако в постановлении речь идет не только о порядке работы со служебной информацией ограниченного доступа, но и о самом порядке ограничения доступа, о том, какие сведения не могут быть отнесены к служебной информации ограниченного доступа. Таким образом, постановление по факту является системообразующим документом института служебной тайны вопреки требованиям законодательства.

Критически оценивая законность Указа № 188, все же рассмотрим классификацию конфиденциальной информации, предложенную в данном акте. Конфиденциальная информация включает в себя:

1. персональные данные, а также сведения о событиях, фактах, обстоятельствах частной жизни гражданина;
2. сведения, составляющие тайну следствия и судопроизводства;
3. служебные сведения, доступ к которым ограничен органами государственной власти (Служебная тайна);
4. сведения, связанные с профессиональной деятельностью, доступ к которым ограничен (Профессиональная тайна);
5. сведения, связанные с коммерческой деятельностью, доступ к которым ограничен (Коммерческая тайна);

¹ См. например Решение Верховного Суда РФ от 15.01.2015 № АКПИ14-1334. – (http://www.supcourt.ru/stor_pdf.php?id=1249982). – Дата обращения:17.12.2017.
Апелляционное определение Верховного Суда РФ от 04.12.2014 по делу № АПЛ14-583. – (www.vsr.ru/stor_pdf.php?id=700134). – Дата обращения:17.12.2017.

6. сведения о сущности изобретения до официального опубликования информации о нем;

7. сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

Очевидно, что эта классификация не является полной и не включает в себя все виды тайн. Юридическая сила указанного нормативного акта вызывает сомнения, однако представляет для нас интерес с теоретической точки зрения.

Вместе с тем, стоит отметить одно нововведение 2015 г.: в Указ был добавлен п. 7, который относит сведения, содержащиеся в личных делах осужденных, к конфиденциальной информации. Этот пункт заслуживает особого внимания, так как из формулировки не явствует, для кого такая информация является конфиденциальной, на каком основании ограничивается доступ к информации, в каком федеральном законе закреплено такое ограничение, имеет ли заключенный право получить информацию, содержащуюся в его личном деле, имеет ли на это право его адвокат? Сейчас, по-видимому, могут стать недоступны личные дела осужденных вообще для ознакомления. Такой подход является недопустимым и противоречащим законодательству (Конституции Российской Федерации, Закону об информации), которым установлен запрет на ограничение доступа к информации, затрагивающей права и свободы человека. Кроме того, в очередной раз вводится ограничение доступа к информации не федеральным законом, а подзаконным нормативным актом. В случае же, если конфиденциальность информации, содержащейся в личных делах осужденных, касается только запрета истребования ее третьими лицами без согласия осужденного, то в данном Указе необходимо сделать указание на этот момент.

Как видим, предложенная в Указе классификация является неполной и во многом устаревшей, кроме того, достаточно сложно выделить в ней какой-

либо классификационный признак, несмотря на вынесенное предположение о приоритетности интересов, охраняемых в режиме конфиденциальности. Говоря о приказе, следует упомянуть о терминологии, которая не соответствует закону об информации, так как конфиденциальность в Указе Президента РФ № 188 не распространяется на государственную тайну, тогда как в Законе об информации конфиденциальность как свойство присуща всей информации ограниченного доступа.

В теоретических разработках ученых встречаются системы, построенные иным образом. Так, например, М. В. Пермяков предлагает достаточно развернутую систему информации ограниченного доступа, построенную на критерии объекта правовой охраны,¹ в которой категория «служебной тайны» отнесена к большой подгруппе государственных секретов, которая находится на одном уровне с коммерческой тайной и информацией о гражданах. В этой системе «служебная тайна» относится исключительно к государственным секретам и не пересекается с так называемой «чужой тайной» – информацией, накапливаемой в органах г.в. и м.с.у. о физических и юридических лицах. В данном случае возникает вопрос о том, в каком режиме будут охраняться сведения, полученные органами г.в. и м.с.у. от третьих лиц, а также каков порядок перехода информации ограниченного доступа из одного правового режима в другой.

Е. К. Волчинская предлагает подразделять информацию в зависимости от источника формирования информации на тайну «первичную» и тайну «производную». Так к первичной тайне относится личная и семейная тайна (тайна физлица); коммерческая тайна (тайна лица, осуществляющего коммерческую деятельность); государственная и служебная тайна в части внутрисистемной информации. К вторичной тайне в соответствии с классификацией отнесены профессиональные тайны (врачебная тайна, тайна исповеди, тайна банковских вкладов и т.д.); коммерческая тайна; служебная

¹ Пермяков, М. В. Категория «тайна» в системе правового регулирования: дис. ... канд. юрид. наук: 12.00.01 / М. В. Пермяков. – Екатеринбург, 2006. – 234с.

тайна в части переданной в органы власти от физ- и юрлиц информации ограниченного доступа. В соответствии с этой классификацией «служебная тайна» относится к первичной тайне в той части, в которой составляет «информацию, создаваемую (генерируемую) в органе государственной власти, информацию, доступ к которой временно ограничен в интересах государственного управления по решению руководителя»¹.

Аналогичной точки зрения в части подразделения служебной тайны на внутреннюю информацию государственных органов и так называемую «чужую» тайну, полученную государственными органами в результате выполнения государственных функций, придерживается А. А. Антопольский².

Считаем, что такая классификация допустима и вполне логична, однако в данном случае требует разрешения вопрос о том, каким образом сочетаются различные правовые режимы информации, в том числе то, каким образом происходит переход информации из одного правового режима в другой.

Однако при рассмотрении того или иного подхода к системе информации ограниченного доступа нельзя сделать вывод об исчерпывающем характере какого-либо из этих подходов. За время правоприменительной практики служебная тайна в значительной мере претерпела существенные трансформации. В настоящий момент она включает в себя информацию, образующуюся в органах г.в. и м.с.у. и подведомственных организаций, а также информацию, составляющую тайну третьих лиц. При этом стоит отметить, что поступающие в органы г.в. и м.с.у. сведения, составляющие различные тайны, не могут охранять в тех же режимах, установленных для них обладателями соответствующих сведений, поэтому и предлагается охранять их в едином режиме служебной тайны. Стоит отметить, что такой переход информации из одного режима в другой возможен не только в случае

¹ Волчинская, Е. К. О проблемах формирования правовой системы ограничения доступа к информации / Е. К. Волчинская // Информационное право. – 2013. – № 4. – С. 3-7.

² Антопольский, А. А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: дисс. ... канд. юрид. наук: 12.00.14. / А. А. Антопольский. – М., 2004. – 289 с.

со служебной тайной, но и в иных случаях: например, коммерческая тайна может переходить в государственную тайну и обратно, государственная тайна может переходить в служебную. При этом особую сложность представляет как переход информации из одного правового режима в другой, так и определение условий ограничения доступа к внутренней информации государственного органа.

Нам представляется, что именно такой подход наиболее полно отвечает существующим реалиям ограничения доступа к информации в настоящее время.

Вместе с тем, недостатком всех рассмотренных систем информации ограниченного доступа можно назвать то, что ни в одной из систем не отображен институт инсайдерской информации. Вместе с тем, отражение его соотношения с режимами информации ограниченного доступа необходимо для выстраивания полной и целостной картины ограничения доступа к информации.

На наш взгляд, некорректны положения законодательства об инсайдерской информации, в соответствии с которыми инсайдерская информация, охраняемая в режиме той или иной тайны, должна быть раскрыта. Такой подход некорректен, поскольку Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ «Об инсайдерской информации») не имеет приоритета перед остальными нормативными актами и юридическое нивелирование иных режимов защиты информации таким режимом информации не находит логического объяснения в законе.

Ввиду отсутствия должного законодательного регулирования института служебной тайны, в научной юридической литературе наблюдается плюрализм мнений в отношении самой сущности правовой природы института служебной тайны. Обусловлено это во многом историей правового

регулирования информации ограниченного доступа в органах государственной власти. Как отмечалось ранее, по мнению некоторых ученых, четкое оформление институт служебной тайны получил в 1987 году, когда было введено интегрированное понятие государственных секретов, которые по степени важности подразделялись на государственную и служебную тайны¹.

Существовала точка зрения, в соответствии с которой правовые режимы служебной и коммерческой тайны совпадают по содержанию, а одно и то же лицо без всяких ограничений может быть обладателем и той, и другой тайны². Такая позиция была обусловлена старой редакцией ст. 139 ГК РФ. При этом некоторые исследователи отмечали, что такое изменение значений понятия могло быть вызвано тем, что необходимо было оградить определенную управленческую информацию от преждевременного разглашения или тем, что принимались попытки манипулирования рынками с помощью информации предприятия.

Как отмечают исследователи³, до принятия ФЗ «Об инсайдерской информации» «фактическим аналогом понятия «инсайдерская информация» было понятие «служебная информация». Это понятие определялось в Федеральном законе от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» (Далее – ФЗ «О рынке ценных бумаг») как «любая, не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими

¹ Занина, Т. М., Кораблев, П. Н. Особенности защиты служебной тайны / Т.М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 31-34.

² Жилинский, С. Э. Предпринимательское право (правовая основа предпринимательской деятельности) / С. Э. Жилинский. – М.: Издательство НОРМА, 2001. – 672с.

³ Вавулин Д. А. Комментарий к Федеральному закону «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» / Д. А. Вавулин. – М.: Деловой двор, 2015. – 288с.

субъектами рынка ценных бумаг»¹, а в ГК РФ как «информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности»². Исследовав указанные формулировки, мы можем отметить, что, в результате смены политического и общественного строя, в праве понятие «служебная информация» перешло из сферы государственных секретов в сферу коммерческого оборота, и одним из новых институтов, вошедших в правовую систему Российской Федерации, является институт инсайдерской информации – информации о деятельности предприятий, организаций, которая способна в значительной степени повлиять на цены финансовых инструментов, иностранной валюты и (или) товаров. В период принятия закона об инсайдерской информации была дискуссия о том, как соотносятся понятие «инсайдерская информация» с понятием «служебная информация», какое из этих понятий шире, и оправданно ли использование в законодательстве понятия «служебная информация».

После принятия Федерального закона «Об инсайдерской информации» из ФЗ «О рынке ценных бумаг» было исключено понятие «служебная информация», однако вопрос о соотношении понятий и правовых режимов до конца снят не был.

В настоящее время понятие и регулирование инсайдерской информации практически не сохранило схожих черт со служебной тайной, когда-то фигурировавшей в первоначальной редакции ФЗ «О рынке ценных бумаг». В настоящее время категория инсайдерской информации включает в себя, в том числе, информацию, составляющую государственную, коммерческую, служебную тайны и иные виды информации ограниченного доступа. Считаем необходимым привести в соответствие с системой нормативных актов ФЗ «Об

¹ О рынке ценных бумаг: Федер. закон от 22.04.1996 № 39-ФЗ.

² Ст. 139 Гражданский Кодекс РФ. Часть 1: Федер. закон от 30.11.1994 № 51-ФЗ (ред. от 29.06.2004 N 58-ФЗ)

инсайдерской информации», установив исключения в случае обязательного раскрытия для государственной и налоговой тайн. Такая позиция основана на том, что в тексте закона коммерческая и государственная тайна во многих случаях являются исключениями предоставления информации, в том числе в случае предоставления информации по запросу Центрального банка.

Несмотря на то, что вопрос соотношения понятий до конца так и не был снят (в том числе ввиду отсутствия должного нормативного регулирования режима служебной тайны), полагаем, что в коммерческих организациях сведения не могут охраняться в режиме служебной тайны ввиду того, что большой массив информации организации возможно охранять в режиме коммерческой тайны, а информация, которая не может охраняться в режиме коммерческой тайны, а также не попадает под иные категории тайн, не может быть информацией ограниченного доступа вообще, исходя из положений Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (далее – ФЗ «О коммерческой тайне») и законодательства Российской Федерации.

Есть позиция, согласно которой служебная тайна это информация, «которая стала доступна (известна) гражданину при исполнении им своих трудовых (служебных) обязанностей. При этом не имеет значения, работает такой гражданин в государственной (муниципальной) или частной организации, заключен ли трудовой договор с юридическим лицом или индивидуальным предпринимателем»¹. Исследователи полагают, что «попытки ограничить понятие служебной тайны взаимоотношениями, возникающими только в рамках государственных организаций, не только не находят опоры в законе, но и неверны по самой своей сути; подобные попытки могут нанести лишь ущерб общему правовому регулированию»². Схожей точкой зрения является точка зрения исследователей, которые предлагают «в целях устранения споров вокруг термина «служебная тайна»

¹ Гаврилов, Э. К вопросу об охране коммерческой, служебной и личной тайны. Гражданско-правовые аспекты / Э. Гаврилов // Хозяйство и право. – 2003. – № 5 – С. 27.

² Там же.

предлагается заменить его на другой, более ясный термин – «трудовая тайна»¹. С аргументом об отсутствии законодательного подтверждения ограничению служебной тайны рамками отношений, возникающих в государственных организациях, сложно спорить, прежде всего, ввиду того, что соответствующее законодательное регулирование на уровне федерального закона отсутствует вообще. В то же время, стоит отметить то обстоятельство, что относить к сведениям, охраняемым в режиме служебной тайны, всю и любую информацию, ставшую доступной гражданину при исполнении трудовых обязанностей, недопустимо. О соотношении понятий «служебная информация» и «служебная тайна» речь пойдет в 4 параграфе настоящей главы. В то же время, считаем, что такой режим защиты информации как «служебная тайна» должен быть характерен непосредственно для государственной и муниципальной службы, поскольку во всех других случаях ограничение доступа к информации в сфере трудовых отношений возможно в режимах коммерческой либо профессиональной тайны.

Как видим, в литературе, как и в практике не разрешен вопрос о субъектном составе отношений в сфере служебной тайны. Так, например, в официальном отзыве Правительства Российской Федерации на проект ФЗ «О служебной тайне» особое внимание было уделено вопросу конкретизации субъектного состава правоотношений и сферы действия нормативного акта. Также в ходе обсуждения законопроекта не раз возникал вопрос относительно определения круга субъектов, которые могут быть наделены полномочиями отнесения информации к разряду служебной тайны.

Следует отметить, что в ходе обсуждения законопроекта возникал вопрос о том, могут ли органы местного самоуправления наделяться полномочиями по отнесению информации к сведениям, охраняемым в режиме служебной тайны. Неоднократно возникал вопрос также о возможности

¹ Мирских, И. Ю. Коммерческая тайна как вид конфиденциальной информации: Трудоправовой и цивилистический аспекты: дис. ... канд. юрид. наук. / И. Ю. Мирских. – Пермь, 2005. – С. 51.

относить к сведениям, охраняемым в режиме служебной тайны информацию, образующуюся либо передаваемую в подведомственные государственным органам организациям, и насколько широк может быть круг этих субъектов.

Как видим, вопрос о субъектном составе правоотношений в сфере служебной тайны достаточно специфичен. Вместе с тем, он перекликается во многом с кругом субъектов правоотношений в сфере государственной тайны. Именно поэтому заслуживает особого внимания.

По мнению И. Ю. Павлова, «наличие дополнительной самостоятельной разновидности информации о деятельности государственных органов и органов местного самоуправления, относящейся к категории ограниченного доступа, представляется чрезмерным, поскольку характеристика объекта, который охраняется в режиме «служебной тайны» в его сегодняшнем понимании, эквивалентна характеристике объекта, охраняющегося в режиме «государственной тайны»¹. Также автор указанной точки зрения считает, что рассматривать служебную тайну целесообразно как «чужую» тайну, а именно как конфиденциальную информацию, которая стала известной государственным органам, должностным лицам при исполнении ими государственных полномочий. И при таком подходе, с точки зрения И. Ю. Павлова, не возникнет потребности в принятии закона «о служебной тайне». Такая точка зрения достаточно распространена, вместе с тем возникает вопрос о том, что делать с «внутренней информацией» органов государственной власти? В случае принятия концепции, обозначенной И.Ю. Павловым, сложится ситуация, при которой вся внутренняя информация будет беспрепятственно распространяться, что, по нашему мнению, не является выражением взвешенного подхода к информационной безопасности. Кроме того, информация, являющаяся «чужой тайной», не может охраняться в органах г.в. и м.с.у. в тех же режимах, в которых она охранялась до ее

¹ Павлов, И.Ю. Современные проблемы правового регулирования государственной и служебной тайны в России / Павлов И.Ю. //Ленинградский юридический журнал. – 2013. - №1 (31). – С.29-35.

передачи, поскольку иное бы означало, что в рамках одного органа существует огромное разнообразие режимов защиты информации с различными техническими и организационными требованиями, что фактически бы поставило под вопрос возможность функционирования органа ввиду невозможности осуществления всех правил и требований защиты различных видов информации в рамках одной системы документооборота в органах власти.

Т. М. Занина предлагает относить сведениям, охраняющимся в режиме служебной тайны, следующую информацию:

«конфиденциальные сведения в области военного управления (военная тайна); сведения, охватываемые понятием «тайна связи» (в той мере, в которой операторами выступают органы государственной власти и подведомственные им организации, учреждения); информация, образующаяся на стадии предварительного расследования; банковская тайна (которая обеспечивается органами государственной власти и ЦБ РФ); конфиденциальная информация, хранящаяся о гражданах в органах государственной власти и местного самоуправления»¹.

В отличие от И. Ю. Павлова она предлагает принять отдельный Федеральный закон «О служебной тайне», который бы детально регулировал отношения в сфере охраны служебной тайны. Однако вряд ли можно сказать, что эта точка зрения лишена недостатков, так как фактически автор перечислил некоторые виды тайн, которые становятся известны государственным органам и должностным лицам, при этом абсолютно неясно, по каким причинам не включены в перечень иные виды профессиональных тайн. Не ясно, почему другие профессиональные тайны не могут оказаться в органах государственной власти, например, касающиеся усыновления, здоровья и т.п., каким образом будет отделена информация, составляющая военную тайну и относящаяся к тайне служебной, от информации,

¹ Занина, Т.М., Кораблев, П.Н. Особенности защиты служебной тайны / Т.М. Занина, П.Н. Кораблев // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 33.

составляющей военную тайну и относящейся к государственной тайне, а также на каком основании к служебной тайне отнесена банковская тайна, поскольку, являясь сама по себе для государственных органов производной тайной, при этом является лишь частным случаем «чужой тайны», поступающей в органы государственной власти.

Существует также еще одна точка зрения, которая кардинально отличается от всех предыдущих. Согласно этой точке зрения, «категорию служебная тайна в настоящее время государственные органы не могут использовать вообще, так как использование такой категории тайны не урегулировано федеральным законодательством»¹. Эта позиция не лишена здравого смысла. Исходя из позиций действующего законодательства, мы не можем ограничивать доступ к информации (а такое ограничение устанавливается в случае охраны информации в режиме служебной тайны), если основание и механизм такого ограничения не будет прописан в федеральных законах. Тем более, вопрос ограничения доступа к информации в сфере государственного и местного управления относится к сфере публичного, а не частного права, где господствует императивный метод регулирования и подход «запрещено все, что не разрешено». Кроме того, в законодательстве отсутствует единство терминологии: в различных нормативных актах используются такие понятия как «служебная тайна»², «информация с пометкой «для служебного пользования»³, «служебная

¹ Такая точка зрения высказывается на сайте Фонда свободы информации (в 2014 году фонд был включен перечень иностранных агентов. В 2015 году прекратил свою деятельность). Согласно высказанной точки зрения, использование такой категории для ограничения доступа к информации является незаконным в существующей правовой обстановке и прямо нарушает право граждан на доступ к информации. – (<http://www.svobodainfo.org/ru/node/146>). – Дата обращения 12.04.2013.

² См. Например ч. 2 ст. 23 О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 30.11.2011 № 342-ФЗ.

³ Например Приказ Роскомнадзора «Об утверждении Инструкции о порядке обращения с документированной служебной информацией ограниченного распространения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органов» от 16.09.2016 № 234.

информация»¹, «служебная информация ограниченного распространения»². Нельзя говорить об использовании института «служебной тайны», если не разрешен вопрос о соотношении используемых понятий и отсутствует единый понятийно-категориальный аппарата института служебной тайны.

Безусловно, и эта точка зрения не является бесспорной, однако проблемы заключается отнюдь не в достаточной аргументированности точек зрения, а в отсутствии должного правового регулирования института служебной тайны на законодательном уровне и отсутствии четкого места служебной тайны в системе информации ограниченного доступа.

В. Н. Лопатин высказывает точку зрения, согласно которой к основным объектам служебной тайны можно отнести в том числе тайну следствия, судебную и военную тайну, кроме того, под признаки служебной тайны полностью попадает тайна налоговая³. На наш взгляд вопрос перехода некоторых режимов профессиональных тайн в органах государственной власти в режим служебной тайны возможно разрешить только при полном соотношении элементов правового режима охраны информации. Так можно обнаружить, что тайна следствия не совпадает со служебной тайной по субъектному составу, как и тайна судопроизводства. В настоящее же время говорить о соотношении понятии именно в таком ключе преждевременно в силу отсутствия унифицированных мер охраны информации и ответственности за ее разглашение, а также существенной разницы в степени общественной опасности разглашения информации, охраняемой в различных правовых режимах.

¹ См., например, О Центральном банке Российской Федерации (Банке России): федер. закон от 10.07.2002 № 86-ФЗ (ред. от 18.07.2017); О рынке ценных бумаг: федер. закон от 22.04.1996 № 39-ФЗ (ред. от 25.11.2017).

² См., например, Постановление ЦИК России «Об Инструкции по делопроизводству в Центральной избирательной комиссии Российской Федерации» от 20.01.2016 № 321/1831-6.

³ Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство: Монография / В. Н. Лопатин. – СПб.: Фонд «Университет», 2000. – С. 214-215.

Логично было бы предположить, что именно в федеральных законах о государственной гражданской службе (Далее – Закон о государственной гражданской службе)¹ и о муниципальной службе (далее – Закон о муниципальной службе)² содержатся положения об охране информации в режиме служебной тайны. Однако указанные законы не оперируют понятием «служебная тайна» вообще. Вместо этой категории в законах используется такое понятие как «служебная информация». При этом определения понятия «служебная информация» в законах не дается. Трактоваться это понятие, исходя из контекста, может максимально широко: как информация, ставшая известная служащему в связи с исполнением им должностных обязанностей. Гипотетически это абсолютно весь массив информации, который образуется в органах государственной власти. Такой подход не может быть практически реализуем, поскольку для охраны всего массива служебной информации нет ни достаточного юридического обоснования, ни технической возможности.

В судебной практике, как правило, под служебной информацией понимается либо иная профессиональная тайна, либо информация в сфере обеспечения безопасности информационных систем³.

Следует отметить существенный недостаток при указании на нарушение режима охраняемой законом тайны: в заключениях о проведении служебной проверки, а также в судебных решениях зачастую указывается на разглашение «служебной информации» либо «служебной конфиденциальной информации» без конкретизации режима конфиденциальности информации, что не позволяет проверить обоснованность и законность принимаемых решений.

¹ О государственной гражданской службе Российской Федерации: федер. закон от 27.07.2004 № 79-ФЗ (ред. от 29.07.2017).

² О муниципальной службе в Российской Федерации: федеральный закон от 02.03.2007 № 25-ФЗ (ред. от 26.07.2017).

³ (Апелляционное определение Саратовского областного суда от 08.09.2016 по делу № 33-6631/2016; Апелляционное определение Верховного суда Республики Карелия от 22.04.2014 по делу № 33-1536/2014; Кассационное определение Новосибирского областного суда от 05.07.2011 по делу № 33-4880/2011г; Решение по делу 1-151/2014 Йошкар-Олинского городского суда от 05.03.2014)

При этом определение «служебной информации ограниченного распространения» дается в Указе Президента РФ № 188 и постановлении Правительства РФ №1233 и является крайне размытым («к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью»), как и критерий отнесения информации к служебной тайне (служебная необходимость).

При рассмотрении служебной тайны в контексте информации ограниченного доступа и ее правового регулирования вопросы возникают относительно ограничения доступа к информации органами государственной власти. Насколько правомерно такое ограничение доступа к информации, особенно если рассматривать этот вопрос в свете принципа открытости и доступности информации о деятельности государственных органов и органов местного самоуправления?¹ На каком основании, чем руководствуясь, принимают решение об ограничении доступа к той или иной информации руководители о.г.в. и м.с.у.? И допустимо ли определять содержание понятия «служебная необходимость» лишь внутренним убеждением уполномоченного лица?

Кроме того, в указанных подзаконных актах (Указе Президента РФ № 188 и постановлении Правительства №1233) право отнесения той или иной информации к сведениям, охраняемым в режиме служебной тайны, имеет ряд должностных лиц соответствующего органа, что может являться причиной бесконтрольного и безосновательного ограничения доступа к информации в органах государственной власти.

При такой модели ограничения доступа к информации необходимо обозначение принципов ограничения доступа к информации в режиме служебной тайны как системообразующих основ института служебной тайны,

¹ Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 09.02.2009 №8-ФЗ (ред. от 09.03.2016).

на которые можно опираться при установлении перечня информации ограниченного доступа, а также установлении мер ответственности за неправомерное ограничение доступа к информации.

Между тем, возможность бесконтрольного ограничения доступа к информации является мощным коррупциогенным фактором в системе управления. Как отмечается в литературе, в «законодательстве о доступе к информации о деятельности государственных и судебных органов содержатся нормы, позволяющие отказывать гражданам и организациям в доступе к несекретной информации, отсутствуют нормы, обязывающие государственные органы раскрывать информацию»¹. Также в литературе делается акцент на необходимость рассмотрения информационной открытости как важного фактора противодействия коррупции².

К тому же, отсутствие четкого правового регулирования института служебной тайны может привести к злоупотреблениям со стороны субъектов служебной тайны. Так, к примеру, неоднократно на рынке обнаруживались полные базы данных органов государственной власти, при этом информация, входившая в эти базы, включала не только персональные данные граждан, но и информацию об анонимных обращениях граждан о правонарушениях, информацию об осведомителях и иную информацию, распространение которой влияет прямо на безопасность граждан³.

¹ Полякова, Т. А. Обеспечение информационной открытости при противодействии коррупции в Российской Федерации: проблемы правового регулирования / Т. А. Полякова, Е. В. Семизорова, О. А. Александрова // Эволюция государственных и правовых институтов в условиях развития информационного общества/ Сборник научных работ. – М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. – 340 с.

² Там же

³ Из ФСКН утекли в свободную продажу секретные базы данных. – (<https://www.novayagazeta.ru/articles/2015/01/20/62713-iz-fskn-utekli-v-svobodnuyu-prodazhu-sekretnye-bazy-dannyh>). – Дата обращения: 17.12.2017.

Данные автовладельцев утекли в интернет. – (<https://www.vedomosti.ru/technology/articles/2016/05/20/641711-dannie-avtovladelcev-utekli-internet>). – Дата обращения: 17.12.2017.

Россия заняла второе место в мире по числу инцидентов утечки информации. – (<https://www.infowatch.ru/presscenter/news/3868>). – Дата обращения: 17.12.2017.

Кроме того, ответственность за разглашение служебной тайны не прописана в законодательстве с достаточной степенью ясности. Можно говорить о следующих видах ответственности за нарушение режима служебной тайны – дисциплинарной либо административной ответственности, что в свете круга субъектов и специфики сведений, защищаемых в режиме служебной тайны, не отвечает в полной мере целям защиты информации и не позволяет соотносить служебную тайну с иными режимами ограничения доступа к информации. В остальных же случаях к ответственности за разглашение информации можно привлечь только со ссылкой на нарушение требований иного правового режима.

А. А. Тедеев, исследуя проблему источников информационного права, отмечает, что многие ученые не оперируют категорией «источники информационного права», подменяя ее понятием «информационное законодательство». «При этом, под таким законодательством, в совокупности, понимаются как собственно законы, так и подзаконные нормативные правовые акты, а нередко и рекомендательные акты ненормативного характера»¹. По мнению профессора А. А. Тедеева, такая подмена понятий и смешение понятий «законодательство» и «подзаконные акты» является недопустимым, «поскольку потенциально создает дополнительные правовые проблемы при формировании эффективного правового механизма налогообложения субъектов электронной экономической деятельности»². В свою очередь, мы можем отметить, что такие проблемы возникают не только при формировании механизма налогообложения, но и в нашем случае – при формировании эффективного правового механизма защиты информации.

Следует отметить, что в последние годы было принято большое количество ведомственных нормативных актов, определяющих порядок работы с информацией ограниченного доступа, в преамбуле которых

¹ Тедеев, А.А. Формирование доктринального понимания сущности источников информационного права / А.А. Тедеев // Вопросы правоведения. – 2010. – № 1. – С. 107.

² Там же

указывается, что они приняты в соответствии и во исполнение п. 1.5. Положения, утвержденного постановлением Правительства РФ № 1223.¹ Таким образом, в области нормативного регулирования образовался большой массив актов, основанных на данном постановлении правительства, которое по своей сути противоречит требованиям Конституции РФ и Закона об информации. Таким образом, и принятые в соответствии с указанным постановлением ведомственные нормативные акты, на наш взгляд, не в полной мере соответствуют положениям Конституции РФ и Закону об информации.

В настоящее время регулирование такого режима как «служебная тайна» происходит исключительно на подзаконном уровне, что противоречит как требованию Закона об информации, так и требованиям Конституции Российской Федерации. Кроме того, такое регулирование является недопустимым, также существует мнение, что если регулирование ограничения информации осуществляется не федеральным законом, как того требует законодательство, то исполнение таких требований не является обязательным.

Существует интересное решение² по этому вопросу, которое было вынесено Верховным Судом Российской Федерации ещё в 2005 г.: И. Ю.

¹ См. Приказ ГУСП Об упорядочении обращения со служебной информацией ограниченного распространения в Главном управлении специальных программ Президента Российской Федерации и подведомственных ему организациях (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения», «Порядком организации защиты служебной информации ограниченного распространения») от 28.11.2016 № 72.

Приказ Росфинмониторинга Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральной службе по финансовому мониторингу (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения», «Порядком организации защиты служебной информации ограниченного распространения») от 16.11.2016 № 375.

и др.

² Решение Верховного Суда РФ от 22.12.2005 № ГКПИ05-1426 // Сайт компании «Консультант Плюс». – (http://www.consultant.ru/document/cons_doc_LAW_86585/). – Дата

Павлов обратился в Верховный Суд Российской Федерации с заявлением о признании недействующими нормы Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти (утвержденного постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233), ссылаясь на то, что они нарушают предусмотренное статьей 29 Конституции Российской Федерации право заявителя свободно искать и получать информацию.

В заявлении указано, что в силу ст. 10 Федерального закона от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» государственные информационные ресурсы являются открытыми и общедоступными, критерии идентификации конкретной информации для отнесения ее к категории ограниченного доступа должны быть определены специальным федеральным законом. Вместе с тем в Российской Федерации не принимался федеральный закон, ограничивающий доступ к несекретной служебной информации.

По мнению заявителя, оспариваемые предписания Положения противоречат статьям 10 и 12 Закона об информации, статьям 4, 40 и 47 Закона Российской Федерации «О средствах массовой информации». С указанными доводами суд не согласился, в удовлетворении заявленных требований отказал. Суд мотивировал своё решение тем, что в силу пункта 5 ст. 10 Закона отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных ст. 11 данного Федерального закона (информация о гражданах).

Следует отметить, что заявитель не мотивировал свою позицию тем, что предписания Положения прямо противоречат требованиям, установленным ч.

3 ст. 55 Конституции РФ, в соответствии с которыми права и свободы человека и гражданина могут быть ограничены федеральным законом.

В решении суд указал, что «использование в приведенной норме Закона об информации двух терминов, а именно, «законодательство Российской Федерации» и «федеральный закон», свидетельствует о том, что отнесение информации к конфиденциальной в случаях, не попадающих под действие ст. 11 Закона, может осуществляться в порядке, установленном не только федеральными законами, но и Указами Президента Российской Федерации и постановлениями Правительства Российской Федерации»¹.

Любопытно отметить, что в ранее действовавшем Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (Далее - Закон об информации №24) до 2006 г. действительно использовались формулировка, в соответствии с которой отнесение информации к конфиденциальной осуществлялось в порядке, установленном законодательством Российской Федерации. И в тот момент суд совершенно справедливо, исходя из анализа норм закона, пришел к указанному выводу. Однако в действующем Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». формулировка более точная: «Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение» (п. 4 ст. 9 Закон об информации). Исходя из положений действующего федерального закона, решение Верховного Суда могло бы звучать совершенно иначе.

На наш взгляд, несмотря на острую необходимость нормативного регулирования института служебной тайны, разработка такого регулирования

¹ Публикуется по статье: Пономарева, Ю. В. Актуальные проблемы служебной тайны / Ю. В. Пономарева // Вестник УРФО. безопасность в информационной сфере. – 2013. – №4(10). – с.17-30.

затягивается во многом из-за отсутствия на то четкой политической воли. При этом продолжает развиваться порочная практика регулирования отношений в сфере служебной тайны вопреки требованиям Конституции Российской Федерации.

Так, к примеру, в Приказе Федерального архивного агентства есть положение о возможности доступа к документу с грифом «ДСП» для граждан только при наличии разрешения организации, которая проставила указанный гриф (фондообразователя).¹ Указанное требование прямо противоречит требованиям Конституции Российской Федерации, а также Закону об информации и Федеральному закону от 29.12.1994 № 78-ФЗ «О библиотечном деле» (далее – Закон о библиотечном деле), поскольку в соответствии с п. 4 ч. 4 ст. 7 указанного закона пользователь общедоступной библиотеки вправе бесплатно получать во временное пользование любой документ из библиотечных фондов.

В свою очередь, отсутствие регулирования режима служебной тайны на уровне федерального закона влечет за собой бессистемность регулирования и бесконтрольный характер ограничения доступа к информации.

Таким образом, установлено, что в России отсутствует регулирование такого режима ограничения доступа к информации как служебная тайна, основанное на требованиях Конституции Российской Федерации и Закона об информации.

Существующее регулирование на уровне подзаконных актов не соответствует установленным требованиям ограничения доступа к информации по уровню правового регулирования, а также является устаревшим и не соответствующим действующему законодательству (постановление Правительства Российской Федерации № 1223 и Указ Президента Российской Федерации № 188), при этом на основании указанных подзаконных актов принято огромное количество ведомственных

¹ Приказ Росархива Об утверждении Порядка использования архивных документов в государственных и муниципальных архивах Российской Федерации от 01.09.2017 №143.

нормативных актов, что привело к разрастанию массива нормативных актов, которые заведомо противоречат действующему законодательству. При этом стоит отметить, что такое регулирование не отвечает в полной мере практической цели: защита информации. Ввиду отсутствия четких и единых организационных и технических требований к работе с информационными базами, а также предусмотренных мер ответственности, нередки случаи утечки информации и полностью баз данных из органов государственной власти.

Таким образом, на основании проведенного исследования можно сделать вывод о том, что служебная тайна носит комплексный характер и представляет собой режим защиты информации, в котором охраняются сведения в сфере государственного управления, отнесение которых к разряду государственной тайны является в силу своего содержания нецелесообразным, а также сведения, составляющие тайну третьих лиц. Вместе с тем, как в литературе, как и в нормативном регулировании, отсутствует единый подход к месту служебной тайны в системе информации ограниченного доступа.

1.4. Служебная тайна как правовой режим информации

Правовое регулирование любого явления сложно представить себе без установления правового режима объекта регулирования. Определение правового режима разрабатывалось в научной литературе как теоретическая категория достаточно длительный период времени. Вопросом о сущности правового режима задавались такие представители юридической науки, как С. С. Алексеев, Б. Н. Бахрах, С. Н. Братановский, Б. В. Россинский, Ю. Н. Стариков, А. В. Малько, Н. И. Матузов, Л. Ю. Павлова, О. С. Родионов, И. С. Розанов, Э. Ф. Шамсумова и многие другие. Л. А. Морозова высказала позицию о том, что правовой режим является «результатом регулятивного воздействия на общественные отношения системы юридических средств,

присущих конкретной отрасли права и обеспечивающих нормальное функционирование данного комплекса общественных отношений»¹. Не можем согласиться с данной позицией, поскольку, на наш взгляд, сами отношения, на которые происходит воздействие, постоянно находятся в развитии. Рассматривать правовой режим только с точки зрения результата регулирования отношений было бы неверно, поскольку сам правовой режим предполагает регулирование отношений во всей их динамике. И как таковой целью правового режима является именно установление правил поведения в рамках отношений, а не только итогового состояния объекта регулирования.

В свою очередь С. С. Алексеев дает следующее определение понятию правовой режим: «это порядок регулирования, который выражен в комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных связываний и создающих особую направленность регулирования»². При этом многие исследователи так или иначе склоняются к такой точке зрения³. Мы согласимся с указанным определением лишь отчасти, поскольку, на наш взгляд, само понимание правового режима не может строиться исключительно лишь на функциональной части нормативных предписаний. При определении правового режима важно понимать, что является «ядром» отношений – тем объектом, вокруг или по поводу которого начинают выстраиваться социальные отношения и их правовое регулирование. Именно специфика объекта предопределяет применимые способы регулирования. К примеру, специфика правового режима информации заключается, прежде всего, в ее нематериальной природе⁴, что и обуславливает многие особенности правового режима информации.

¹ Морозова, Л. А. Конституционное регулирование в СССР / Л. А. Морозова. – М., 1985. – С. 123.

² Алексеев, С. С. Теория права / С. С. Алексеев. — М.: Издательство БЕК, 1995. — С. 283

³ Подробнее см. Братановский, С. Н. Специальные правовые режимы информации / С. Н. Братановский. – М.: Изд-во Директ-Медиа, 2012. – С. 28.

⁴ Терещенко, Л. К. Правовые основы специальных режимов информации / Л. К. Терещенко // Юридический консультант. – 2007. – № 9. – С. 5-14.

Л. К. Терещенко предлагает следующее определение правового режима информации: «объектный режим, вводимый законодательным актом и позволяющий обеспечить комплексность воздействия посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое значение дозволений, запретов и обязываний, а также гарантий по его соблюдению»¹.

В то же время, Л. К. Терещенко выделяет следующие признаки правового режима информации: «правовой режим информации – это характеристика такого объекта права, как информация, вытекающая из ее нематериальной природы; правовой режим информации устанавливается для достижения желаемого социального эффекта; содержание правового режима информации отражается в правилах, которые в своей совокупности призваны обеспечить достижение поставленной цели; правила установлены или санкционированы государством, т. е. имеют общеобязательную силу; правила представляют собой систему, сочетающую в себе в различном соотношении запреты и обязывания, льготы и дозволения»².

Указанное определение и выявленные признаки достаточно четко отражает специфику информации как объекта правоотношений, поскольку делается акцент на регуляции и охране информации как объекта режима, но не на закреплении определенного состояния, поскольку, по большому счету, правовой режим информации предопределяется действиями субъектов правового режима в отношении информации как объекта регулирования. Сама зафиксированная на материальном носителе информация, безотносительно субъекта правового регулирования, представляет собой не что иное, как набор символов. Будучи не распознанными, символы так и остаются исключительно символами, не имея ни практического значения, ни ценности.

¹ Терещенко, Л. К. Правовой режим информации. Автореф. ... дисс. докт. юрид. наук. / Л. К. Терещенко. – М. 2011. – С. 15.

² Терещенко, Л. К. Правовые основы специальных режимов информации / Л. К. Терещенко // Юридический консультант. – 2007. – № 9. – С. 5-14.

Так П. У. Кузнецов выделяет, применительно к области правового обеспечения информационной сферы, следующие элементы правового режима:

1. Целенаправленность;
2. Носитель правового режима;
3. Правовой статус субъектов;
4. Режимные правовые средства и правила как особое сочетание правовых средств.¹

Как видим, в указанной классификации акцент сделан на субъектном составе правоотношений, что отвечает указанным ранее особенностям правового режима информации. В то же время, Л. К. Терещенко в своей диссертации предлагает схожий набор элементов правового режима, однако отдельно выделяет объект правового регулирования, отмечая при этом, что целевым назначением режима является обеспечение информационной безопасности субъекта.² Считаем, что такое разделение элементов является более полным, поскольку учитывает также специфику объекта правового режима: разницу правовых режимов предопределяет зачастую именно содержание информации, выступающей в качестве объекта правового регулирования.

Вместе с тем, в представленных точках зрения, как в отношении правового режима информации, так и в отношении правового режима как общеправовой категории, исследователями выделяется такой признак как целенаправленность правового регулирования. Целенаправленность как таковая является вектором формирования и развития правового режима. В то же время должны существовать определенные идеи, правила, так называемый каркас правового регулирования, который будет определять в том числе и

¹ Кузнецов, П. У. Правовой режим как категория и метод информационного права / П. У. Кузнецов // Правовые понятия и категории в контексте информационного права. Материалы теоретического семинара по информационному праву. – М., 2006. – С. 12-32.

² Терещенко, Л. К. Правовой режим информации: автореф. ... дисс. докт. юрид. наук. / Л. К. Терещенко. – М., 2011. – С. 15.

соответствие правового регулирования в рамках режима всей системы права. На наш взгляд, таким определенным каркасом правового регулирования являются принципы. Как отмечает Г. С. Беляева, «приоритет при характеристике правового режима должен быть отдан принципам как исходным, определяющим идеям, положениям, установкам»¹. Освещение вопроса принципов права встречается в работах многих ученых². При этом С. С. Алексеев считал, что принципы являются единым духом, пронизывающим целостную регулируемую нормативную систему: «Принципы представляют собой концентрированное выражение права данной страны, своего рода чистые сгустки правовой материи, выкристаллизованные в правовой системе»³. Вместе с тем, нельзя отрицать и тот факт, что для формирования правового режима необходимо руководствоваться определенными принципами регулирования, которые и будут предопределять все существенные черты правового режима. Так, к примеру, в Законе об информации, как и в Законе о государственной тайне, закрепляются принципы регулирования информационных отношений и ограничения доступа к информации. Особенно определение принципов регулирования важно при формировании нового правового режима, которым является режим служебной тайны, для встраивания правового регулирования в систему существующих нормативных предписаний и дозволений.

Помимо прочего, необходимым условием функционирования правового регулирования является ответственность как непреходящий элемент системы права. Вместе с тем, считаем, что все же ответственность, хоть и направлена

¹ Беляева, Г. С. Принципы правового режима / Г. С. Беляева // Пробелы в российском законодательстве. – 2013. – № 4. – С. 23-26.

² Например: Матузов, Н. И. Принципы права как объект научного исследования (вместо введения в книгу) / Н. И. Матузов // Принципы российского права: общетеоретический и отраслевой аспекты. – Саратов, 2010. – С. 11.

Фролов, С. Е. Принципы права: Вопросы теории и методологии: дисс. ... канд. юрид. наук: 12.00.01 / С. Е. Фролов. – Кострома, 2001. – С. 168.

Лаврус, С. Ю. Реализация принципов права в юридической практике: дисс. ... канд. юрид. наук / С. Ю. Лаврус. - Самара, 2005. – 238 с.

³ Алексеев, С. С. Теория права / С. С. Алексеев. – М.: Издательство БЕК, 1995. – С. 283.

на регулирование общественных отношений, сама по себе несколько выходит за пределы правового режима, поскольку наступает в случае нарушения установленных нормативных предписаний. Тем не менее, ответственность как таковая должна рассматриваться и включаться как одна из составляющих регулирования отношений, поскольку сама по себе является мерой принуждения к соблюдению норм права¹.

Резюмируя вышесказанное, считаем необходимым выделить следующие элементы правового режима тайны:

1. Принципы правового режима.
2. Объект – это сведения, охраняемые в режиме тайны.
3. Субъектный состав правоотношений, который определяет круг лиц, которым предоставляются определенные права и на которых накладываются обязанности в рамках правового режима.
4. Содержание правового режима – элемент, представляющий собой совокупность регулирующих норм, направленных на создание определенных условий и правил обработки и использования информации.
5. Ответственность за нарушение правил оборота информации.

Как было отмечено ранее, законодательство подразделяет в общем всю информацию на общедоступную и информацию ограниченного доступа (Закон об информации), вместе с тем, нельзя не отметить и такую категорию информации, как информация, запрещенная или ограниченная в распространении, специфика которой заключается не в мерах, направленных на защиту информации, а в требовании о воздержании от ее распространения в различной степени, которая может зависеть от возрастной категории лиц, на которую рассчитана информация, от способа ее распространения либо контекста ее использования. При этом как таковая классификация по критерию доступа к информации не дает четкого представления о правовых режимах той или иной информации.

¹ Иоффе, О. С., Шаргородский, М. Д. Вопросы теории права / О. С. Иоффе, М. Д. Шаргородский. – М., 1961. – С. 318.

Такая категория как «информация ограниченного доступа» (далее – ИОД) включает в себя различные категории сведений, доступ к которым ограничивается в том или ином режиме тайны. Такая категория достаточно широко используется в современном законодательстве Российской Федерации. Несмотря на это, отсутствует терминологическая определенность в использовании различных понятий в сфере регулирования ИОД. Так для обозначения информации такого рода используются, по крайней мере, четыре понятия: «Конфиденциальные сведения» или «Сведения конфиденциального характера», «Информация ограниченного доступа», «тайна». Из-за отсутствия четкого терминологического разграничения понятий, правовое регулирование ИОД трудно назвать упорядоченным, логичным и систематизированным.

В последнее время в науке информационного права все большее внимание уделяется четкой выверенности и стройности терминологического аппарата. Так, в частности, П. У. Кузнецов выделил ряд принципов, на которых должно строиться формирование понятийно-категориального аппарата информационного права. По мнению автора, к ним можно отнести следующие: адекватность, когнитивность, априорность, универсальный характер, рациональность и обновляемость формулируемых понятий¹.

В настоящее время в законодательстве фактически отсутствуют определения базовых понятий, таких как «информация ограниченного доступа» и «тайна». По мнению И. О. Бондаря, «это приводит, прежде всего, к путанице в самом законодательстве, к размытости правотворческих ориентиров в информационной сфере, к разной трактовке пределов охраняемой законом тайны. Одно из негативных последствий такого состояния проблемы – крупные дефекты правореализационного процесса»². Как отмечает В. Н. Лопатин, отсутствие четкого единого понятийного

¹ Кузнецов, П. У. Методологические проблемы информационного права: [выступление на] V Международной научно-практической конференции «Право и информация: вопросы теории и практики», 17.04.2015. – (<http://www.prlib.ru/Lib/pages/item.aspx?itemid=133065>). – Дата обращения: 17.07.2017.

² Бондарь, И. В. Тайна по российскому законодательству (проблемы теории и практики): автореф. дисс. ... канд.юрид.наук / И. В. Бондарь. – Нижний Новгород, 2004. – 24 с.

аппарата правового регулирования информации ограниченного доступа приводит к произвольному толкованию понятий и затрудняет реализацию законов¹.

Точное определение данных понятий, а также выявление их существенных признаков послужило бы базой для структурирования нормативных актов, повышения степени согласованности законодательного регулирования, а также дальнейшего повышения качества юридической техники.

Как отмечают исследователи, «определение дефиниций в информационном праве – это не только юридическая техника, но и логика языка, которая имеет не только теоретический характер, но и существенное значение в правоприменительной и судебной практике»². В юридической литературе еще недостаточно разработаны подходы к формированию юридических категорий и классификаций понятийного аппарата информационного права. И. Л. Бачило отмечала, что в формировании понятийного аппарата существует три оси: онтологическая ось, целевая (аксиологическая) ось, а также организационная ось³. Соблюдение осевого построения понятийно-категориального аппарата должно подразумевать ответы на вопросы о сущности правового явления, цели правового регулирования, а также методах ее достижения.

В юридической литературе неоднократно предпринимались попытки выделения существенных признаков правового содержания понятия «тайна». Также следует отметить, что зачастую понятие «тайна» отождествляется с

¹ Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство: Монография / В. Н. Лопатин. – СПб.: Фонд «Университет», 2000. – С. 173.

² Полякова, Т. А., Акулова, Е. В. Правовое обеспечение информационной безопасности: проблемы понятийного аппарата. / Т. А. Полякова, Е. В. Акулова // Понятийный аппарат информационного права. Сб. Науч. Работ. – М.: ИГП РАН Издательство «Канон +» РООИ «Реабилитация», 2015. – С. 117.

³ Бачило, И. Л. О методологии выявления и классификации понятийного аппарата в информационном праве // Понятийный аппарат информационного права / отв. Ред. И. Л. Бачило, Э. В. Талапина. Сб. науч. Работ. – М.: ИГП РАН Издательство «Канон+» РООИ «Реабилитация», 2015 – С.8-18.

понятием «информация ограниченного доступа», и выводятся общие признаки информации, доступ к которой не является всеобщим.

А. А. Антопольский в своем исследовании дает следующие критерии понятия «тайна»: разновидность социальной информации; предназначена для строго ограниченного круга субъектов и умышленно скрывается ими от прочих субъектов; угроза причинения вреда общественным интересам в случае разглашения¹.

Указанные критерии, по нашему мнению, относятся именно к информации, составляющей тайну, и применимы в том случае, когда тайна понимается в качестве информации, а не в качестве правового режима. А. А. Фатьянов выделяет следующие признаки правового понятия «тайна»: ущерб, который может возникнуть в случае разглашения информации; реальная или потенциальная ценность информации; легальность ограничения доступа к информации; защита информации от несанкционированного доступа.

Указанный подход является, на наш взгляд, более комплексным и включает в себя не только существенные признаки информации, но также и существенные элементы правового режима, такие как легальное ограничение доступа к информации и ее защита.

Однако, на наш взгляд, эти критерии, включающие в себя ряд признаков правового режима, не являются исчерпывающим, поскольку не отражают полностью критерии тайны как правового режима.

В. Н. Лопатин отмечает, что законодательство Российской Федерации устанавливает следующие обязательные признаки и условия охраноспособности права информации с ограниченным доступом: защита информации; защите подлежит лишь документированная информация; соответствие ограничениям, которые установлены в законодательстве².

¹ Антопольский, А. А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: дисс. ... канд. юрид. наук: 12.00.14. / А. А. Антопольский. – М., 2004. – 289 с.

² Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин. / Санкт-Петербургский университет МВД России. – Спб.: Фонд

В данном случае вынуждены не согласиться с предложенными критериями, во-первых, потому, что свойства информации как таковой и ее сущность не отражены, а, во-вторых, потому, что не только документированная информация подлежит защите. Так, к примеру, сведения, составляющие тайну личной жизни либо тайну исповеди, как правило, не документируются.

На наш взгляд, наиболее полным является перечень признаков тайны, предложенных И. В. Бондарем:

1. «Тайна есть информация, которая может быть отражена в материальной форме, а также в идеальной форме.

2. Статус информации, составляющей тайну, должен быть юридически определен федеральным законодательством путем ограничения доступа к ней.

3. Сведения должны быть известны ограниченному кругу лиц.

4. Сведения имеют действительную или потенциальную ценность.

5. Ценность информации носит духовно-нравственный, коммерческий либо иной общественно значимый характер и достигается за счет неизвестности ее третьим лицам.

6. К указанной информации нет свободного доступа на законном основании.

7. Владелец информации принимает меры к охране ее конфиденциальности.

8. Разглашение сведений может повлечь наступление негативных последствий для собственника информации (материальный, моральный ущерб).

9. За разглашение этих сведений устанавливается законом юридическая ответственность»¹.

Между тем, если рассмотреть конкретные категории информации ограниченного доступа и их определение в законодательстве или научной литературе, можно заметить одну особенность: в Законе о государственной тайне дается следующее определение понятию «государственная тайна» – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации; в то же время в законе под коммерческой тайной понимается «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду», налоговую тайну определяют как «любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике». Кроме того, в научной литературе при определении «служебной тайны» происходит определение понятия через определение свойств сведений, защищаемых в этом режиме.

Так, например, И. Л. Бачило определяла служебную тайну через свойства объекта правового режима – охраняемой информации.² М. В. Пермяков³, Г. Отнюкова⁴ подходят к определению понятия «служебной тайны» аналогичным образом. В то время как Г. Г. Камалова⁵ подходит к

¹ Бондарь, И. В. Тайна по российскому законодательству: Проблемы теории и практики: автореферат дис. ... кандидата юридических наук: 12.00.2001 / Нижегород. акад. МВД России. – Нижний Новгород, 2004. – С. 19.

² Бачило, И. Л., Лопатин, В. Н., Федотов, М. А. Информационное право: учебник / под ред. Б. Н. Топорнина. – СПб.: Юридический центр Пресс, 2001. – С. 383.

³ Пермяков, М. В. Категория «тайна» в системе правового регулирования: Дис. ... канд. юрид. наук: 12.00.01 / М.В. Пермяков. – Екатеринбург, 2006. – 234 с.

⁴ Отнюкова, Г. Д. Коммерческая тайна / Г. Д. Отнюкова // Закон. – 1998. – № 2. – С. 58.

⁵ Камалова, Г. Г. О правовом режиме служебной тайны // Вестник УдмГУ. – 2014. – № 2-4.

вопросу определения служебной тайны через определение существенных элементов правового режима информации ограниченного доступа.

Сопоставляя различные подходы к определению признаков и сущности тайны как таковой и определению конкретных видов тайн как в законодательстве, так и в теории, возникает одно противоречие: говоря о сущности и признаках тайны в общем, авторы зачастую в признаки включают и меры защиты информации, и ограничения доступа к ней по кругу лиц, и меры ответственности за ее разглашение, в то же время, при определении признаков служебной тайны, авторы исходят в основном из объектного состава отнесенной к ней информации, а также нормативного регулирования отнесения той или иной информации к сведениям, охраняемым в режиме служебной тайны, зачастую не упоминая ни о мерах ее защиты, ни о мерах ответственности.

Такая дихотомия в определении «тайн» объясняется тем, что существуют два понимания одного термина, обозначающего «информацию ограниченного доступа». В первом случае речь идет только о признаках той информации, доступ к которой ограничен, и в этом случае фактически все заканчивается на определении объекта охраны. Во втором же случае речь идет о правовом режиме, в котором охраняется та или иная информация. Следует отметить, что некоторые ученые настаивают на том, что понятие «тайна» сама по себе может рассматриваться исключительно в качестве определенного режима ограничения доступа к информации, а не в качестве самой информации¹. Другие ученые полагают, что наиболее соответствует, с практической точки зрения, определение тайны через определение категорий информации, в отношении которой происходит защита, поскольку в этом случае критерий «неизвестность третьим лицам» не является определяющим в

– С. 145-152.

¹ Фатьянов, А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве): Моногр. / А. А. Фатьянов. – М.: Изд-во МИФИ, 1998. – С. 138.

вопросе защиты сведений¹.

Вопрос, на наш взгляд, неоднозначный, поскольку даже в законодательстве, к примеру, под «коммерческой тайной» понимают определенный правовой режим, тогда как понятие налоговой, аудиторской и даже государственной тайны определяется через состав сведений, формирующих ту или иную категорию тайны. В Законе о государственной тайне фактически правовой режим государственной тайны назван «системой защиты государственной тайны» как совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях. Вместе с тем, на наш взгляд, понимание тайны как определенного режима информации, может стать одним из ключевых моментов при построении понятийно-категориального аппарата всей информации ограниченного доступа, поскольку это позволило бы рассматривать возникающие отношения более всесторонне и полно, а не только с точки зрения перечня сведений.

Сопоставляя такие понятия как «тайна» и «информация ограниченного доступа», можно было бы предположить, что сведения, в отношении которых должна соблюдаться конфиденциальность, охраняются фактически способами, предусмотренными для защиты иных видов информации ограниченного доступа, которые установлены у того или иного субъекта и уже переходят в режим тайны. Так, к примеру, отсутствует единый режим охраны сведений, составляющих персональные данные². В свою очередь они охраняются, как правило, в органах государственной власти в режимах «конфиденциальной информации органа государственной власти» (мы его понимаем как аналог служебной тайны) либо в режиме коммерческой тайны

¹ Бундин, М. В. Система информации ограниченного доступа и конфиденциальность // Вестник ННГУ. – 2015. – №1. – С. 120-130.

² В то же время, Е. К. Волчинская указывает на то, что сама по себе категория «персональные данные» не является категорией информации ограниченного доступа. См. Волчинская Е. К. Место персональных данных в системе информации ограниченного доступа / Е. К. Волчинская // Право. – 2014. – № 4. – С. 193–207.

организации, также они могут охраняться в режиме государственной, банковской тайн. Вместе с тем, такое понимание не полностью бы отражало правовую реальность и существующее нормативное закрепление информации ограниченного доступа. Так, к примеру, в Федеральном законе «О рынке ценных бумаг» существует ряд сведений, в отношении которых должна соблюдаться конфиденциальность. Фактически, у держателей реестра и депозитариев должна быть собственная система защиты информации¹. Вместе с тем, такую защиту информации нельзя рассматривать в контексте какого-либо из установленных режимов тайн. Нельзя, в то же время, говорить о том, что тайна личной жизни, семейная тайна или тайна переписки охраняется в каком-то конкретном режиме, устанавливающим в том числе организационные или технические меры защиты.

В связи с этим, полагаем, что невозможно с учетом существующего нормативного регулирования информации ограниченного доступа разделить четко понятие «тайна» и понятие «информация ограниченного доступа», поскольку отсутствует единообразие нормативного регулирования как при определении понятия «тайна» (как категория сведений либо правовой режим защиты информации), так и при установлении понятийно-категориального аппарата в отношении понятия «тайна» или «информация ограниченного доступа»). Так в науке существует позиция, согласно которой обилие и разнообразие используемых терминов в сфере ограничения доступа к информации связано как с «особенностями перевода, заимствования терминов и правовых институтов из зарубежного законодательства и практики, так и с особенностями традиционно специфической терминологии в разных отраслях права или сферах деятельности»².

¹ Об этом свидетельствует также Положение о деятельности специализированных депозитариев» (утв. Банком России 10.06.2015 № 474-П), которым установлены специальные требования к системе учета специализированных депозитариев.

² Бундин, М. В. Система информации ограниченного доступа и конфиденциальность /М. В. Бундин // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2015. – № 1. – С. 122.

В то же время, исследователи, давая определение понятию «тайна», так или иначе затрагивают такой признак как требование конфиденциальности информации (ее защита/отсутствие свободного доступа к информации/неизвестность третьим лицам/и т.д.). При этом в последние 20 лет смысл понятий «конфиденциальная информация», «конфиденциальность», «секретная информация» существенно менялся. При этом все три понятия не ушли из законодательства. Именно поэтому полагаем, что одним из важных вопросов понятийно-категориального аппарата института служебной тайны является вопрос о соотношении понятий «конфиденциальная информация», «конфиденциальность информации», «секретная информация».

На первый взгляд, указанные понятия «являются схожими, даже тождественными, однако при внимательном их изучении можно обнаружить различную природу этих понятий и определенное изменение этих понятий во времени.

«Конфиденциальный – конфиденциальный, доверительный, секретный»¹. Такое немногословное определение дается в большинстве словарей и энциклопедий. Это понятие раскрывается, как правило, через ряд синонимов, которые не позволяют получить полного представления о содержании понятия.

Обратимся к понятию «секретный»: «Секрет – это то, что содержится в тайне, скрывается от других»². Такое определение, встречающееся часто в различных словарях, также не является исчерпывающим для такого сложного правового и социального явления как «секретность». Таким образом, этимология слов «конфиденциальность» и «секретность» не раскрывают юридического содержания этих понятий.

¹ Советский энциклопедический словарь / под ред. Гусева А. А., Кнунянц И. Л., Кузнецова М. И., Панова В. Г., Федосеева П. Н., Храпченко М. Б. – М.: Советская энциклопедия. – 1987. – С. 623.

² Ожегов, С. И., Шведова, Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова. – 4-е изд., дополненное. – М.: Азбуковник, 1999. – С. 698.

Есть определение, встречающееся в специализированных справочниках, трактующее понятие «секретность» как свойство объекта, который отнесен к государственной или служебной тайне и скрывается от третьих лиц с помощью специальных мер технического, административно-правового и оперативного характера. На наш взгляд, такое определение из всех представленных наиболее полно отвечает целям нашего исследования. Вместе с тем, использование мер сокрытия информации характерно в целом для различных режимов ограничения доступа к информации, а не только для режимов государственной или служебной тайны.

Рассмотрим использование этих категорий в международном и национальном законодательстве.

В «Модельном информационном кодексе для государств – участников СНГ»¹ (ст. 34) выделяется информация с ограниченным доступом как отдельный вид информации. При этом она, в свою очередь, подразделяется на информацию конфиденциальную и секретную. Проанализируем определения, которые приводятся в указанном нормативном акте:

«Секретная информация – информация, которая содержит сведения, составляющие государственную или другую предусмотренную законом тайну»².

«Конфиденциальная информация. Обладатели информации имеют право самостоятельно устанавливать правовой режим конфиденциальности, если это не противоречит требованиям национального законодательства»³.

Из изложенного следует, что в указанном модельном кодексе даётся определение только понятию «секретная информация» (возникают некоторые сомнения относительно корректности самого определения,

¹ Модельный информационный кодекс для государств-участников СНГ. Принят в г. Санкт-Петербурге 23.11.2012 Постановлением 38-6 на 38-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2013. – №57 (часть 1). – С. 44 - 73.

² Там же.

³ Там же.

поскольку под категорию «секретная информация», в силу формулировки определения, подпадает вся без исключения информация ограниченного доступа), в то время как понятие «конфиденциальная информация» в документе раскрыто через права обладателей информации. В соответствии с определением конфиденциальной информации, правообладатели информации имеют возможность устанавливать по своему усмотрению ограничение доступа к информации. Получается, что ограничение доступа к информации устанавливается не в силу прямого указания на закон, а в силу желания правообладателя (и соответствующей юридической возможности). Считаем необходимым акцентировать внимание на этом полномочии правообладателя как единственном отличии двух видов информации ограниченного доступа. В то же время в указанном нормативном акте четкие отличия секретной и конфиденциальной информации отсутствуют, дается лишь отсылка к национальному законодательству, при этом не объясняется правовой смысл разграничения информации с ограниченным доступом на два правовых режима.

Обратимся к национальному законодательству. Базовое определение дается в Законе об информации: «конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя»¹. Схожее определение дано в Федеральном законе от 08.12.2003 №165-ФЗ «О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров»²: «конфиденциальная информация не должна разглашаться без разрешения представившего ее заинтересованного лица, за исключением случаев, предусмотренных федеральными законами»³. Определения «секретности» в законодательстве не встречается. Закон о государственной тайне дает лишь определение понятия

¹ Закон об информации.

² О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров: федер. закон от 08.12.2003 № 165-ФЗ (ред. от 04.06.2014).

³ Там же.

«гриф секретности». В указанном нормативном акте многократно используется такое понятие как «степень секретности», при этом его определение также не приводится. На основании анализа указанного закона, а также постановления Правительства Российской Федерации от 04.09.1995 № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну к различным степеням секретности»¹ можно сделать вывод о том, что степень секретности зависит от степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. То есть фактически степень секретности – это степень важности, и, как следствие, степень скрываемости сведений. И тут возникает вопрос: если конфиденциальность – это свойство тайны, которое обозначает отсутствие на законных основаниях свободного доступа к информации, а секретность обозначает по сути то же самое, то существует ли разница между этими понятиями?.

Обратимся к нормативным актам, использующим эти понятия. В Законе об информации в ст. 9 речь идет об обязательности условия соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами. В то время как защита информации, составляющей государственную тайну, выделена в отдельный пункт, в соответствии с которым защита информации, составляющей государственную тайну, происходит в соответствии с законодательством о государственной тайне. При анализе указанной статьи возникают вопросы о том, является ли свойство конфиденциальности общим как для государственной тайны, так и для иной информации, доступ к которой ограничен, и каково соотношение конфиденциальности и секретности информации? Если исходить из базового определения «конфиденциальности», то можно говорить о том, что это общее свойство для информации ограниченного доступа вообще. Тогда возникает

¹ Об утверждении Правил отнесения сведений, составляющих государственную тайну к различным степеням секретности: Постановление Правительства РФ от 04.09.1995 № 870 (ред. от 18.03.2016).

закономерный вопрос о целесообразности использования в законодательстве такого термина как *секретность*.

В Законе об информации №24 в ст. 10 информация с ограниченным доступом по условиям её правового режима подразделялась на информацию, отнесенную к государственной тайне и конфиденциальную¹. Исходя из указанной формулировки, можно было сделать вывод о том, что разница между государственной тайной и иной информацией ограниченного доступа заключается в различии установленных правовых режимов. Несмотря на это, в Законе об информации № 24 понятие «конфиденциальная информация» определялось как «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации». То есть под это определение также попадала и государственная тайна. В результате получалась логическая ошибка: в статье 2 «конфиденциальная информация» включала в себя весь массив информации ограниченного доступа, в том числе и государственную тайну, а в статье 10 государственная тайна уже исключается из понятия «конфиденциальная информация». Несмотря на такие противоречия в старом законе, было хотя бы понимание разницы правовых режимов конфиденциальной информации и государственной тайны. В новом же нормативном акте законодатель упразднил существовавшую ранее классификацию, при этом не дав ответа на вопрос о соотношении понятий «секретности» и «конфиденциальности», а только устранив формулировку, ранее вызывавшую споры. Исходя из смысла внесенных изменений в законодательные акты в 2006 г., можно сделать вывод о том, что понятие «конфиденциальность» стало общим по отношению ко всем режимам информации ограниченного доступа, в том числе к режиму государственной тайны, и стало обозначать именно свойство информации

¹ Такая позиция законодателя в своё время вызывало серьезную критику (См. например Алексеенцев, А. И. «О составе защищаемой информации / А. И. Алексеенцев // Безопасность информационных технологий. – 1999. – № 2. – С.5-7.), которая основывалась на том, что понятия «секретный», «конфиденциальный», «тайна» являются тождественными, поэтому попытки дифференцировать их лишены смысла и приводят лишь к терминологической путанице.

ограниченного доступа, а не определенную группу информации ограниченного доступа. С этим было связано то, что понятие «конфиденциальная информация» стало исключаться из нормативных актов. Вместе с тем, понятие «конфиденциальная информация» не ушла полностью из нормативных актов. Так, к примеру, знаковым является использование понятия «конфиденциальная информация» в постановлении Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», которая четко обозначает конфиденциальную информацию как информацию, не содержащую сведения, составляющие государственную тайну, но защищаемую в соответствии с законодательством Российской Федерации юридическими лицами и индивидуальными предпринимателями.

Проанализируем также нормативные акты, в которых используется понятие «конфиденциальность» и понятие «секретность». Следует отметить, что использование понятия «секретность» в нормативных актах значительно уже. Основным законом, в котором употребляется указанный термин, является Закон о государственной тайне, также понятие употребляется в параграфе 7 главы 72 Гражданского кодекса в отношении секретных изобретений. В нормах указанного параграфа есть прямая отсылка к Закону О государственной тайне, также упоминается это понятие в Федеральном законе «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» от 15.08.1996 № 114-ФЗ в нормах статьи о выдаче загранпаспорта гражданину, имеющему допуск к государственной тайне. В указанном нормативном акте идет также прямая отсылка к нормам Закона о государственной тайне. В ряде иных федеральных законов также упоминается термин «секретность» и дается отсылка к указанному закону. При этом стоит отметить, что даже в отношении такого понятия как «служебная тайна»

законодатель использует такое определение как «несекретные сведения»¹. Кроме того, в ряде подзаконных актов режим служебной информации ограниченного распространения и режим работы с секретными документами различаются².

Термин «конфиденциальность» используется в федеральных законах применительно к иным видам информации ограниченного доступа. Так, к примеру, требование соблюдения конфиденциальности содержит в себе ст. 9 Федерального закона «Об аудиторской деятельности» от 30.12.2008 № 307-ФЗ, в которой речь идет об аудиторской тайне, также требование конфиденциальности содержится в Налоговом кодексе Российской Федерации (ст. 82), Гражданском кодексе Российской Федерации (ст. 727) и других нормативных правовых актах.

В теории, однако, существует оригинальный подход к пониманию того, что является тайной. Так М. В. Бундин полагает, что «термин «конфиденциальный», дословно «доверительный», по отношению к информации следует использовать скорее в случаях передачи ее обладателем другим субъектам, то есть «конфидентам» – лицам, на которых возложена обязанность «сохранить ее в тайне» или, иными словами, обеспечить ее конфиденциальность»³. Лексически такое понимание выглядит вполне логично, однако оно слабо подходит для характеристики той или иной информации ограниченного доступа, поскольку само по себе требование «конфиденциальности» должно быть применимо только к «производной» информации ограниченного доступа – информации третьих лиц, в отношении которой установлено требование неразглашения и защиты такой информации.

¹ Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности: Постановление Правительства РФ от 3.11.1994 № 1233.

² Об утверждении Регламента Министерства транспорта Российской Федерации: приказ Минтранса России от 03.03.2006 № 27.

³ Бундин, М. В. Система информации ограниченного доступа и конфиденциальность / М. В. Бундин // Вестник ННГУ. – 2015. – №1. – С. 120-130.

Вместе с тем, такие «конфиденты», на которых возложена обязанность сохранения информации в тайне, присутствуют также и в отношениях, связанных практически с любой информацией ограниченного доступа: работники организации, в которой введен режим коммерческой тайны, государственные служащие, получившие доступ к государственной тайне и т.д. – все эти лица являются конфидентами. В то же время, на наш взгляд, такое понимание не несет практического смысла, поскольку, строго говоря, не всегда статус конфиденнта (лица, обязанного обеспечивать конфиденциальность информации) приобретает только то лицо, которому передана (доверена) информация иного лица. Так, к примеру, в режиме коммерческой тайны работники должны охранять не только сведения, полученные от работодателя, но также «ставшие известными в связи с исполнением ими должностных обязанностей», созданные работником в процессе своей трудовой деятельности (к примеру, особые условия сотрудничества с привлеченными клиентами). Несмотря на то, что указанные сведения были созданы самим работником, а не доверены ему работодателем, работник не перестает быть конфиденнтом – лицом, обязанным сохранять конфиденциальность информации.

Таким образом, можно сделать вывод об отсутствии единого понимания в законодательстве понятия «конфиденциальность» и его соотношения с понятием «секретность». К сожалению, преобразование Закона об информации №149 не привело к формированию единого понимания конфиденциальности и регулированию информации ограниченного доступа. На наш взгляд, разделение конфиденциальной и секретной информации обусловлено, прежде всего, определенной правовой традицией, в соответствии с которой, еще в эпоху существования СССР большинство информации ограниченного доступа относилось именно к институту государственного управления (об этом свидетельствует исследование, проведенное в первом параграфе настоящей главы). Сам по себе режим

«секретности» представляет собой частный случай режима «конфиденциальности».

Проведем сравнительный анализ различных правовых режимов (см. Таблица №1)

Режимы / Критерии сравнения	Секретность	Конфиденциальность
Субъектный состав.	Отнесение информации к государственной тайне происходит на основании закона компетентными федеральными органами государственной власти	Отнесение информации к категории ограниченного доступа может быть как в силу закона (личная, семейная тайна, адвокатская тайна, банковская тайна, тайна исповеди и т.д.), так и в отдельных случаях в силу воли на то владельца закона, если такая возможность предусмотрена законодателем (коммерческая тайна)
Защищаемые интересы	Публичные интересы. стратегические интересы государства	Частные интересы физических, юридических лиц.
Сущность правового режима защищаемой информации	Специальная процедура допуска к государственной тайне, особые требования к лицам, имеющим доступ к секретной информации. Использование специальной процедуры сертификации средств защиты государственной тайны.	Отсутствуют нормативно установленные специальные процедуры допуска к информации ограниченного доступа. Средства защиты информации должны соответствовать иным требованиям, чем те, которые установлены для государственной тайны.

Таблица №1

На основании представленного анализа можно сделать вывод о том, что режим секретности, применительно к государственной тайне, является частным случаем режима конфиденциальности, и необходимость его юридического обособления обуславливается спецификой объекта охраны. На наш взгляд, необходимо более четкое правовое разграничение режима

секретности, что позволит избежать не только терминологической путаницы, но и создать определенные юридические рамки, каркас правового регулирования такого понятия как государственная тайна.

Что же касается отнесения информации к сведениям, охраняемым в режиме служебной тайны, несмотря на кажущуюся очевидность ответа о том, что служебная тайна является все же конфиденциальной информацией в общем виде (об этом свидетельствует и Указ Президента РФ № 188, и некоторые определения, в которых говорится о том, что служебная тайна – это несекретная информация....), все же есть определенные моменты, которые свидетельствуют о двойственной природе служебной тайны. Так, к примеру, отнесение информации к сведениям, охраняемым в режиме служебной тайны, должно происходить только на основании решения компетентных должностных лиц, кроме того, в той части, в которой служебная тайна охраняет внутреннюю информацию государственных органов, она все же частично отвечает признаку «охраны публичных интересов».

Как было сказано ранее, понятие служебной тайны активно используется, но четкого закрепления данного понятия в нормативных актах нет. Существует лишь определение, закрепленное в Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Оно звучит следующим образом: «служебная тайна – это служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами»¹. Кроме указанного в нормативных актах используется понятие «служебная информация ограниченного доступа». Это понятие определяется как «несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой

¹ Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188.

диктуются служебной необходимостью»¹. При сопоставлении этих двух понятий, возникает вопрос об их соотношении: являются ли они тождественными? Указанные формулировки хоть и схожи, однако имеют различия: «в первом случае служебная тайна – это сведения, доступ к которым ограничен, во втором случае – это НЕсекретная информация, с ограничением на распространение». Возникает вопрос: что такое секретная информация, а что такое тайна? И может ли быть тайна несекретной информацией? Если исходить из общелексического толкования, то можно сказать, что слова «секрет» и «тайна» являются синонимичными по смыслу². Если же исходить из контекстного толкования, то можно предположить, что такое различие в понятиях вызвано особенностями юридической техники. Так как выше нами был приведен анализ терминов «конфиденциальность» и «секретность», можно сделать вывод о том, что в данном случае имеется в виду то, что служебная тайна не является тайной государственной (проведена аналогия с секретными сведениями, защита которых предусмотрена Законом о государственной тайне).

Итак, мы полагаем, что понятия «служебная тайна» и «служебная информация ограниченного доступа» являются тождественными.

Кроме того, в законодательстве достаточно часто упоминается такая категория информации как «служебная информация», статус которой является также достаточно неоднозначным. Так в одном из постановлений Правительства Российской Федерации³ используется термин «служебная

¹ Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии: постановление Правительства РФ от 03.11.1994 г. № 1233 (ред. от 18.03.2016). – п. 1.2.

² «Секрет – то, что держится в тайне, скрывается от других». Ожегов, С. И., Шведова, Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова. – 4-е изд., дополненное. – М.: Азбуковник, 1999. – 944 с.

³ Об утверждении типового Кодекса профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с формированием и инвестированием средств пенсионных накоплений, и Правил согласования Кодексов профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с

информация». Примечательно, что этот термин во всех формулировках логически обособлен от других видов информации ограниченного доступа. В постановлении используется формулировка «служебная и конфиденциальная информация», то есть законодатель фактически разграничил служебную и иную информацию ограниченного доступа. Интересно также то, что в постановлении дается определение «служебной информации»: это «любая не являющаяся общедоступной и не подлежащая разглашению информация, находящаяся в распоряжении должностных лиц и сотрудников организации в силу их служебных обязанностей, распространение которой может повлиять на рыночную стоимость активов, в которые размещаются средства пенсионных накоплений».

Также само понятие «служебная информация» без упоминания понятия «служебная тайна» встречается в двух основных федеральных законах, регулирующих отношения в сфере государственной и муниципальной службы: Закон о государственной гражданской службе и Закон о муниципальной службе. При этом в указанных законах служебная информация понимается как информация, не подлежащая разглашению. Проблему указанного определения мы затрагивали в третьем параграфе первой главы. Стоит только отметить, что при рассмотрении такого понятия как «служебная информация» и требования ее неразглашения возникают вопросы относительно того, на каком основании происходит ограничение доступа к данной категории информации, если эта информация не является информацией ограниченного доступа? И чем отличается информация ограниченного доступа от информации, не подлежащей разглашению?

В связи с этим можно сделать следующий вывод: либо налицо непроработанность с точки зрения юридической техники, либо в данном контексте разделяются понятия «служебная тайна» и «служебная информация». Во втором случае абсолютно неясно, на каком основании

формированием и инвестированием средств пенсионных накоплений, с Федеральной службой по финансовым рынкам: постановление Правительства РФ от 12.12.2004 № 770.

разграничиваются эти два понятия. Так как если не отождествлять служебную информацию со служебной тайной, то малейшие основания для ограничения доступа к такой информации просто отсутствуют. Можно предположить, что режим такой информации в контексте рассматриваемого постановления сопоставим с режимом инсайдерской информации за исключением требования о раскрытии информации.

В других же правовых актах, использующих понятие «служебная информация», такая категория информации характеризуется как чисто техническая, вспомогательная информация, указывающая на «адрес» места хранения тех или иных сведений. Так, например, такое понимание данной категории информации встречается в Указаниях Центробанка¹.

Такое различие в понятиях «служебная информация» и «служебная тайна» далеко не редкость, при этом из смысла законов о государственной гражданской службе и о муниципальной службе следует, что понятие «служебная тайна» подменяется понятием «служебная информация», что является недопустимым. На наш взгляд, понятие «служебная информация» значительно шире по своей сути, чем понятие «служебная тайна» либо «служебная информация ограниченного доступа». Она охватывает весь объем информации, образующийся в результате деятельности, в том числе информацию, входящую в категорию «открытые данные». И доступ к ней не может быть ограничен в произвольном порядке.

Исследователи выделяют различные признаки служебной тайны. Стоит отметить, что зачастую исследователи не определяют тайну в качестве определенного правового режима. Возможно, с этим связаны и встречающиеся в литературе различия при характеристике признаков служебной тайны как свойств информации либо как условий ограничений доступа к информации.

¹ См. например, О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом и от проведения операции с денежными средствами или иным имуществом: указание Банка России от 26.11.2004 № 1519-У.

В примерно схожем виде признаки служебной тайны встречаются в большинстве работ, посвященной этой тематике. К основным признакам можно отнести следующие: «отнесение информации федеральным законом к служебной тайне; информация является «чужой тайной» другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна); не является государственной тайной и не попадает под перечень сведений, доступ к которым не может быть ограничен; получена представителем государственного органа и органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом»¹.

А. А. Антопольский дает следующее определение понятию «служебная тайна»: «сведения, доступ к которым ограничен органами государственной власти и органами местного самоуправления в случаях и порядке, предусмотренных федеральными законами, а также конфиденциальные сведения, переданные в эти органы физическими и юридическими лицами»².

В. А. Мазуров под служебной тайной понимает «охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необходимости, а также ставшие известными в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющие действительную или потенциальную ценность в силу неизвестности их третьим лицам, к ним нет свободного доступа на законном основании, обладатель сведений принимает меры к их конфиденциальности, незаконное получение или разглашение которых создает угрозу причинения вреда

¹ (цитата не является дословной). Бачило, И. Л., Лопатин, В. Н., Федотов, М. А. Информационное право: учебник / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. – СПб: Юридический центр Пресс, 2001. – С. 383.

² Антопольский, А. А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: дисс. ... канд. юрид. наук: 12.00.14. / А. А. Антопольский. – М., 2004. – С. 238.

владельцу данных сведений и предоставляет ему право на защиту в соответствии с законодательством РФ»¹.

По всему очевидно, что в данном определении автор смешивает понятие правового режима и свойства определенной информации, доступ к которой является ограниченным.

В. Н. Лопатин под служебной тайной понимает защищаемую по закону конфиденциальную информацию, ставшую известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости»².

Следует отметить, однако, что в данном определении используется категория «служебная необходимость», которая в силу ее неопределенности может значительно снижать степень эффективности правового регулирования служебной тайны.

В Проекте федерального закона «О служебной тайне» указывалось на то, что орган государственной власти вправе отнести к служебной тайне сведения, полученные им в процессе управленческой деятельности, если их распространение может воспрепятствовать либо иным образом отрицательно сказаться на реализации полномочий, предоставленных ему федеральными законами, законами субъектов Российской Федерации, иными нормативными правовыми актами. В качестве законодательных ограничений при принятии решений об ограничении доступа к информации указывались принципы законности, обоснованности, разумной достаточности и своевременности.

¹ Мазуров, В. А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: Учебное пособие / В. А. Мазуров. – М.: Издательско-торговая корпорация «Дашков и К0», 2003. – 152 с.

² Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин / Санкт-Петербургский университет МВД России. – СПб.: Фонд «Университет», 2000. – С. 214.

В официальном отзыве Правительства РФ на указанный Проект федерального закона отмечалось, что использование принципов в качестве правовых ограничений в деятельности государственных органов в условиях достаточно общего их определения законопроектом может привести к злоупотреблениям в осуществлении последними своих полномочий¹. Такая формулировка основания для ограничения доступа к информации (возможный вред в случае разглашения), является, пожалуй, одной из наиболее спорных в литературе, поскольку сами по себе оценочные категории в праве являются одними из самых сложных для правоприменителя. Кроме того, если по оценочным категориям, которые достаточно часто встречаются в вопросах судебной практики, все же удастся выработать определенные единые подходы именно в силу сущности самого судебного процесса, возможности обжалования и пересмотра судебных актов, то вот в такой достаточно закрытой системе как государственное управление, выработка единого подхода на основании многочисленной практики обжалования и пересмотра решений органов выглядит крайне сомнительно в силу отсутствия многочисленной судебной практики по вопросам управления и специфики работы самих государственных органов.

Вместе с тем, как отмечалось ранее, камнем преткновения многих исследований также становится вопрос о том, каков состав сведений, которые могут быть отнесены к сведениям, охраняемым в режиме служебной тайны. Так Е. К. Волчинская предложила интересный подход, в соответствии с которым собственно служебная тайна является информацией, которая образуется в органах власти, а так называемая «чужая» тайна охраняется в режиме служебной тайны². Вместе с тем, полагаем, что если сама служебная тайна понимается в качестве правового режима, то и нет смысла так дробить

¹ Официальный отзыв Правительства РФ от 24.10.2006 № 3901п-П4 на проект Федерального закона № 124871-4 «О служебной тайне». – (<http://sozd.parlament.gov.ru/bill/124871-4>). – Дата обращения: 17.12.2017.

² Волчинская, Е. К. Ограничение доступа к служебной информации: административно-правовые аспекты // магистерская диссертация. – Челябинск, 2014. – С. 24.

категории информации, охраняемой в этом режиме. При таком подходе оба вида информации охраняются в режиме служебной тайны. Отметим, что такой подход встречается также в работах Н. Н. Ковалевой¹.

На основании представленного анализа подходов к определению информации, охраняемой в режиме служебной тайны, предлагаем следующее определение: сведения, охраняемые в режиме служебной тайны – это сведения, образующиеся в результате деятельности органов государственной власти и местного самоуправления, а также подведомственных им организаций и государственных корпораций, доступ к которым ограничен в соответствии с федеральным законом, а также информация ограниченного доступа о физических и юридических лицах, ставшая известной государственным и муниципальным служащим в результате осуществления возложенных на органы государственной власти и местного самоуправления полномочий и обязанностей.

В целом же, если принять концепцию отнесения к сведениям, охраняемым в режиме служебной тайны, конфиденциальной информации, ставшей известной органам государственной власти в процессе их деятельности, а также информацию, образующуюся в органах государственной власти и охраняемую на основании (еще непринятого) федерального закона, остаются все же вопросы об объекте правового регулирования. Так, в частности, в литературе не решается однозначно вопрос о соотношении служебной и профессиональной тайны (к примеру, тайны следствия, тайны усыновления, налоговой тайны, и т.д.). На наш взгляд, режим «служебной тайны» мог бы стать родовым по отношению к сведениям, образующимся в органах государственной власти и относимых к профессиональным тайнам. Однако проблема во многом заключается в степени охраны информации, степени значимости сведений и охраняемых интересов, а также мерах ответственности, предусмотренных за нарушение

¹ Ковалева Н. Н. Информационное право России / Н. Н. Ковалева. – учебное пособие. – М.: Изд-во «Дашков и Ко», 2007. – С. 109.

режима той или иной профессиональной тайны. Именно поэтому говорить о возможности унификации служебной тайны и профессиональной тайны преждевременно. В случае унификации режимов конфиденциальности будет необходимо также криминализовать разглашение служебной тайны.

Полагаем, что унификация понятийного аппарата служебной тайны необходима для создания четкой системы правового регулирования. В связи с чем считаем целесообразным использовать понятие «служебная информация» как родовое понятие для всей информации, используемой в органах г.в. и м.с.у., а также подведомственных им организациях и государственных корпорациях; в отношении информации, охраняемой в режиме служебной тайны, автором предлагается использовать такое понятие как «сведения, охраняемые в режиме служебной тайны».

Исходя из изложенного, можем сделать следующие выводы: само понятие «тайна» должно пониматься в качестве определенного правового режима информации, а не только категории сведений, разглашение которых не допускается. Ранее в законодательстве была сделана попытка введения категории «тайны» как правового режима в законе о «коммерческой тайне», при этом сам закон имеет достаточно хорошую проработку и понимание коммерческой тайны как определенного правового режима значительно меняет подход к пониманию того, в каких случаях возможна ответственность за разглашение коммерческой тайны. Понимание тайны как определенного правового режима позволяет оценивать возникающие отношения по поводу информации ограниченного доступа комплексно. Сам понятийно-категориальный аппарат, использующийся в регулировании служебной тайны, должен быть существенно проработан и унифицирован.

Понятие служебной информации является родовым по отношению к служебной тайне и обозначает весь объем информации, циркулирующий в органах власти и местного самоуправления, в свою очередь понятия «служебная информация ограниченного доступа» и «служебная тайна» при понимании служебной тайны как правового режима будут соотноситься как

целое и частное, поскольку в этом случае служебная информация ограниченного доступа будет обозначать категории сведений, охраняемых в режиме служебной тайны.

Полагаем также, что для дальнейшего исследования необходимо выделить следующие составляющие правового режима:

1. принципы правового регулирования;
2. объект правоотношений как совокупность сведений, охраняемых в режиме тайны;
3. субъекты правоотношений в сфере оборота сведений, охраняемых в режиме служебной тайны, на которые возложены обязанности защиты сведений, охраняемых в режиме служебной тайны;
4. содержание правоотношений как совокупность юридически предписаний, дозволений и обязываний;
5. совокупность организационных и технических требований обеспечения конфиденциальности сведений, охраняемых в режиме служебной тайны;
6. ответственность как особый элемент правового режима, играющий роль государственного принуждения к исполнению требований правового режима.

Из указанного определения понятия «сведения, охраняемые в режиме служебной тайны» и выявленных элементов правового режима, предлагаем следующую формулировку правового режима служебной тайны:

Правовой режим служебной тайны представляет собой совокупность правовых, организационных и технических методов и средств, обеспечивающих защиту сведений, формирующихся в результате деятельности органов государственной власти и органов местного самоуправления, а также подведомственных им организаций, информации ограниченного доступа о физических и юридических лицах, ставшая известной указанным субъектам в результате осуществления возложенных на них полномочий и обязанностей.

2. ОСОБЕННОСТИ ПРАВОВОГО РЕЖИМА СЛУЖЕБНОЙ ТАЙНЫ

2.1. Принципы и условия ограничения доступа к информации, охраняемой в режиме служебной тайны

Для определения объекта правового регулирования служебной тайны необходимо определиться с тем кругом информации, которая так или иначе попадает под защиту в режиме служебной тайны. Ограничение доступа к информации в демократическом государстве предопределяют принципы права, а подробную регламентацию ограничение доступа к информации находит в критериях отнесения информации к категории информации ограниченного доступа.

Для исследования вопроса принципов определимся с терминологическим аппаратом.

Под принципами права в теории понимают, как правило, «выраженные в праве исходные нормативно-руководящие начала, характеризующие его содержание, его основы, закрепленные в нем закономерности общественной жизни»¹. В свою очередь под условиями отнесения информации к категории информации ограниченного доступа, находящейся в ведении органов государственной власти, мы будем понимать конкретные требования, которые предъявляются к содержанию сведений и определению степени их важности.

А. А. Тедеев, теоретически осмысливая информационное право как отрасль права как таковую, высказал мысль о теоретическом делении права на общую и особенную часть. При этом он отмечает, что принципы информационного права и регулирующие структуру, порядок и принципы

¹ Алексеев, С. С. Собрание сочинений. В 11 томах. / С. С. Алексеев. – М.: Статут, 2010. – 3 т. – С.100.

функционирования информационной среды должны устанавливаться общей частью информационного права¹.

Мы полностью разделяем указанную позицию. Вместе с тем, нельзя не отметить, что институт служебной тайны как таковой имеет некоторую специфику касательно иных отношений, возникающих в сфере ограничения доступа к информации, что позволяет отграничивать институт служебной тайны от тайны государственной.

Для института служебной тайны принципы отнесения информации к сведениям, охраняемым в таком режиме, особенно важны, поскольку институт служебной тайны, являясь во многом смежной категорией, нуждается, для избежания размытия границ? такого института, в конкретизации и отграничении сферы его использования, экономии юридических, организационных и технологических мер защиты информации.

Проанализируем основные принципы ограничения доступа к информации, находящейся в ведении органов государственной власти, которые выделяются в теории, законодательстве и практике правового регулирования.

Вопрос обоснованности ограничения доступа к информации давно является предметом многочисленных дискуссий на международном уровне. Как было указано ранее, очень часто вопросом судебных разбирательств в Европейском суде по правам человека выступает вопрос обоснованности ограничения доступа к информации.

«В деле «Штоль против Швейцарии»² был поднят достаточно спорный вопрос разглашения служебной тайны редакцией одной из газет. Дело касается осуждения журналиста на уплату штрафа за обнародование в прессе конфиденциального доклада швейцарского посла в США.

¹ Тедеев, А. А. Предмет информационного права в условиях Интернета / Тедеев А. А. // Информационное право. – 2006. – № 3. – С. 3-5.

² Постановление Европейского Суда по правам человека от 10.12.2007 г. Дело «Штоль против Швейцарии» [Stoll v. Switzerland] (жалоба № 69698/01) (Большая Палата) // Бюллетень Европейского Суда по правам человека. Российское издание. – 2008. – № 6.

«В декабре 1996 г. швейцарский посол в США в ходе указанных переговоров подготовил «стратегический документ» под грифом «конфиденциально». Копии документа были направлены 19 другим лицам в швейцарском правительстве и федеральных органах власти, а также в швейцарских дипломатических представительствах. Заявитель получил копию документа в результате нарушения служебной тайны. Цюрихская воскресная газета напечатала две статьи заявителя с заголовками «Посол Ягметти оскорбляет евреев» и «Посол в халате и альпинистских ботинках кладет ноги на стол». На следующий день цюрихская ежедневная газета воспроизвела значительную часть стратегического документа. Суд приговорил заявителя к штрафу в 800 швейцарских франков за разглашение «секретной официальной переписки» в значении ст. 293 Уголовного кодекса»¹.

Первоначально в постановлении Палаты Европейский Суд установил («за» - 4 голоса, «против» - 3 голоса), что произошло нарушение ст. 10 Конвенции. Далее дело было передано на рассмотрение Большой Палаты. Основной вопрос, стоящий перед Европейским Судом, заключался в том, были ли установленные ограничения свободы информации и примененные к нарушителям санкции «необходимыми в демократическом обществе». В конечном счете, Большая Палата сделала вывод, что «Статьи, написанные с искажениями и упрощениями, могли ввести читателей в заблуждение относительно личности и возможностей посла, что значительно подорвало их вклад в общественную дискуссию, защищаемую ст.10 Конвенции»² и не признала в этом случае нарушение положений Конвенции. Это постановление интересно тем, что в случае корректного отображения информации журналистами, решение по делу могло быть совершенно иным. А это значит,

¹ Вопрос о соблюдении права на уважение личной и семейной жизни. – (<http://www.echr.ru/documents/doc/2466505/2466505-005.htm>). – Дата обращения: 17.12.2017.

² Постановление Европейского Суда по правам человека от 10.12.2007 г. Дело «Штоль против Швейцарии» [Stoll v. Switzerland] (жалоба № 69698/01) (Большая Палата) // Бюллетень Европейского Суда по правам человека. Российское издание. – 2008. – № 6.

что грань между обоснованностью и необоснованностью ограничения или доступа к информации относительна и не имеет конкретных критериев. И в любом из таких дел возникает вопрос о политической подоплеке и степени беспристрастности ЕСПЧ. Несмотря на то, что ЕСПЧ является независимым международным судом, однако, он и выносит решения, в которых так или иначе отражается позиция европейского сообщества в отношении тех или иных обстоятельств.

В другом интересном для настоящего исследования деле «Гуджа против Молдавии»¹ рассматривался вопрос о разглашении государственным служащим внутренней информации государственных органов и опубликовании указанной информации в СМИ – двух писем, адресованных генеральному прокурору спикером парламента по поводу громкого уголовного дела в отношении четырех полицейских и последующим увольнении государственного служащего (в данных письмах указывалось на наличие факта политического давления на органы прокуратуры). В этом случае ЕСПЧ отметил, что «ни молдавское законодательство, ни внутренние предписания Генеральной прокуратуры Молдавии ни содержали положений касательно того, каким образом работники должны сообщать о происходящих нарушениях (см. выше § 32). Таким образом, создается впечатление, что, за исключением непосредственных начальников заявителя, отсутствовали иные уполномоченные органы, которым он мог бы сообщить о своих наблюдениях, кроме того, отсутствовала какая-либо процедура сообщения о таких вопросах. В этом случае ЕСПЧ признал нарушение положений ст.10 Конвенции о защите прав человека и основных свобод, поскольку указанная информация имела общественный интерес.

В сущности, приведенные выше дела, исходя из представленных обстоятельств, различаются только манерой, в которой представлены

¹ Постановление Европейского Суда по правам человека от 12.02.2008 г. Дело «Гуджа против Молдавии» [Guja v. Moldova] (жалоба № 14277/04) (Большая Палата) // Бюллетень Европейского Суда по правам человека. – Российское издание. – 2008. – № 8.

конфиденциальные материалы в СМИ. Считаем, что стиль изложения информации не может являться основным фактором, определяющим исход дела, в котором главным вопросом является допустимость либо недопустимость разглашения информации, представляющей интерес для общества, а также пределы ограничения доступа к такой информации. Вероятно, в первом случае возможно было бы действия СМИ переквалифицировать на диффамацию и признать нарушение положений ст. 10 Конвенции.

Как отмечалось ранее, в рассмотрении ЕСПЧ часто бывают дела, в которых одним из основных вопросов становится вопрос о возможности доступа и разглашения той или иной «чувствительной информации». Однако критерии достаточности ограничения доступа слишком подвижны, чтобы служить четким показателем законности либо незаконности действий государственных органов.

Как отмечает Л. К. Терещенко, основным принципом ограничения доступа к информации является следующее правило: «открытость не может быть абсолютной, но она должна быть необходимой и достаточной»¹.

Несмотря на то, что Глобальные принципы национальной безопасности носят рекомендательный характер, они представляют немалый интерес для настоящего исследования. На наш взгляд, в российских юридических исследованиях им не было уделено должное внимание.

Указанный документ устанавливает 50 принципов, которые так или иначе призваны регулировать отношения в сфере ограничения доступа к «чувствительной» информации. Одним из основных показателей, который выступает в противовес национальной безопасности, является «общественный интерес». Именно соотношения интересов национальной безопасности и общественных интересов должно, по мнению авторов, определять

¹ Терещенко, Л. К. Доступ к информации: правовые гарантии / Л. К. Терещенко // Журнал российского права. – 2010. – №10 (166). – С. 46-53.

допустимость либо недопустимость ограничения доступа к информации. Безусловно, положения Принципов относятся в большей степени к ограничению доступа к информации в режиме государственной тайны, однако в рамках настоящего исследования они представляют особый интерес, поскольку в них определено, что и иные основания для ограничения доступа к информации в государственных органах должны соответствовать установленным в документе стандартам.

Документ основывается на положениях и принципах, установленных в двадцати международных документах, касающихся прав и свобод человека, прав на доступ к информации, свободе выражения и свободе средств массовой информации. Стоит отметить, что среди таких документов также учтено и специальное заявление ВикиЛикс.

Рассмотрим основные принципы в документах, указанных в Глобальных принципах национальной безопасности, которые устанавливаются применительно к ограничению доступа к правительственной информации, а не к свободе информации в целом.

Большинство международных документов, в том числе документов, содержащих рекомендации экспертов международных организаций и центров прав и свобод человека, содержат два основных принципа ограничения доступа к информации органов государственной власти:

1. Безопасность и персональная информация о жизни граждан.
2. Интересы национальной безопасности.

Как правило, в документах и рекомендациях сдерживающим фактором ограничения доступа к информации является «общественный интерес». Наиболее полно принципы ограничения доступа к информации описаны в Конвенции Совета Европы о доступе к официальным документам¹, поскольку в большей степени отражают именно те категории сведений, доступ к

¹ Конвенция Совета Европы о доступе к официальным документам (CETS № 205) (Заключена в г. Тромсе 18.06.2009). – (<https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/205>). – Дата обращения: 17.12.2017.

которым может быть ограничен. Так, в частности, Конвенция содержит 10 категорий сведений, доступ к которым может быть ограничен. Кроме того, в ряде международных документов прописана обязательность доказывания государственным органом обоснованности ограничения доступа к информации как безусловная гарантия права граждан на доступ к информации.

Именно на основании соотношения национальной безопасности и общественного интереса были выработаны 50 Глобальных принципов национальной безопасности. Все-таки, вопреки названию, на наш взгляд, указанный документ не состоит исключительно из принципов, а является по большей мере рамочным, устанавливающим основные права и обязанности в сфере доступа к информации, а также порядок рассмотрения дел в сфере нарушения права на доступ к информации.

Главными принципами ограничения доступа к информации названы следующие принципы: право на информацию; законность ограничения доступа к информации; обоснование ограничения доступа к информации государством; недопустимость освобождения любых органов от раскрытия информации; надзор за ограничением доступа к информации и доступ к информации органов надзора; обеспечение реального соблюдения принципов; возможность ограничения прав в режиме чрезвычайного положения только в необходимых пределах¹.

Вместе с тем, в самих принципах, как и в практике регулирования ограничения доступа к информации, в целях интересов национальной безопасности, одним из важнейших является вопрос определения пределов интересов национальной безопасности. Глобальные принципы национальной безопасности не дают определение «национальной безопасности», признавая при этом право каждого государства определять круг интересов, касающихся национальной безопасности. Все же Глобальные принципы национальной

¹ Отметим, что перевод принципов в данном случае не является дословным, а лишь передает их смысл в силу специфики изложения текста документа.

безопасности вводят такую важную категорию как «законный интерес национальной безопасности», устанавливая те цели, которым не может служить «национальная безопасность» – защите правительства или должностных лиц от позора или раскрытия проступка; сокрытие информации о нарушениях прав человека, любое другое нарушение закона, или функционирования государственных институтов; укрепление или увековечение частного политического интереса, партии, или идеологии; или подавление законных протестов.

Кроме того, установлены категории информации, доступ к которой может быть ограничен только в исключительных случаях, которые могут являться только единичными, а не обычной практикой.

Вместе с тем, Принципы достаточно подробно описывают необходимые условия для ограничения доступа к информации. Так, к примеру, в общих принципах установлено, что только органы государственной власти, чья деятельность непосредственно связана с обеспечением безопасности, могут ссылаться на «национальную безопасность» как на основание сокрытия информации. Также устанавливается необходимость доказывания правительством (либо соответствующими государственными органами) обоснованности ограничения доступа к информации, к тому же обязательным является обнародование классификации, применяемой для ограничения доступа к информации в органах государственной власти, а также необходимость создания независимого надзора за законностью ограничения доступа к информации. Важным, на наш взгляд, является также указание на возможность раскрытия в определенных случаях служащими информации (принцип 37), когда информация относится к правонарушениям либо угрозе жизни или здоровью населения с условием освобождения от ответственности за такое раскрытие.

Указанный документ обобщил большой объем существующего нормативного регулирования ограничения доступа к информации, а также правоприменительной практики и выработал основные требования к

регулированию ограничения доступа к информации о деятельности органов власти.

Обратимся к национальной правовой системе и к принципам и условиям ограничения доступа к информации, накапливаемой в государственных органах.

Важнейшим и первостепенным документом, устанавливающим право на доступ к информации и случаи ее ограничения, является Конституция Российской Федерации. Ст. 29 декларирует право граждан искать, получать, передавать, производить и распространять информацию любым законным способом. Также эта статья устанавливает, что перечень сведений, составляющих государственную тайну, определяется федеральным законом. Вместе с тем, Конституция Российской Федерации, как отмечает Э. В. Талапина, содержит четыре ограничения в обороте информации: использование незаконных способов ее производства и оборота; особый режим информации, отнесенной к государственной тайне; режим персональных данных; интеллектуальная собственность¹.

Несмотря на такое закрепление, указанный перечень оснований для ограничения доступа к информации не является исчерпывающим.

Для правового регулирования ограничения доступа к информации является базовым принцип ограничения любых прав и свобод, закрепленный в ч. 3 ст. 55 Конституции РФ: «права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства».

Этот принцип содержит сразу два условия ограничения прав и свобод человека, который также применим к праву на информацию:

¹ Талапина, Э. В. Модернизация государственного управления в информационном обществе: информационно-правовое исследование: дисс. докт. юрид. наук. / Э. В. Талапина. – М., 2015. – С. 38.

1. «Права могут ограничиваться исключительно федеральным законом».

2. Ограничение прав возможно только в той мере, «в какой это необходимо для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства»¹.

Именно эти условия составляют базу всей законодательной политики в сфере оборота информации, являются определяющими для поиска баланса интересов различных субъектов информационных отношений.

В Законе об информации в ст. 9 устанавливаются те интересы, для обеспечения которых может ограничиваться доступ к информации. К этим интересам относятся: защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В то же время, нетрудно заметить, что в отличие от рекомендаций, прописанных в Глобальных принципах национальной безопасности, в российском правовом порядке отсутствует какое-либо упоминание об «общественном интересе» как противовесе интересам «обороны страны и безопасности государства» в сфере ограничения доступа к информации, что, на наш взгляд, не способствует формированию взвешенного подхода к ограничению доступа к информации. При этом употребляются такие понятия как «интересы общества», «основы правового порядка и нравственности», но они используются в других сферах регулирования.

Вместе с тем, как отмечает Э. В. Талапина, принцип правовой определенности в сфере защиты ценной для государства информации, применяется ограниченно во всем мире, а не только в России². Так, к примеру,

¹ Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993. – 25 дек. – Ст. 55.

² Талапина, Э. В. Модернизация государственного управления в информационном обществе: информационно-правовое исследование: дисс. ... докт. юрид. наук. / Э. В. Талапина. – М., 2015. – С. 236.

в 2006 году в обзоре ПАСЕ отмечалось, что во многих европейских странах законодательство о государственной тайне содержит размытые и нечеткие формулировки.

Если же обратиться к принципам ограничения доступа к информации, охраняемой в режиме служебной тайны, то обнаружим, что как таковых принципов ограничения доступа к информации в этом режиме в законодательстве не предусмотрено. Кроме того, если принципом ограничения доступа к информации в режиме государственной тайны является «защита основ конституционного строя, нравственности, здоровья, обеспечения обороны страны и безопасности государства», то в режиме служебной тайны основанием для ограничения доступа к информации является «служебная необходимость», что фактически означает абсолютное усмотрение органов г.в. и м.с.у..

В свое время в проекте закона о служебной тайне от 2004 г. был предусмотрен ряд принципов ограничения доступа к информации в режиме служебной тайны. К ним, в частности, относились принципы законности, обоснованности, разумной достаточности и своевременности. В заключениях к проекту указывалось на то, что «использование принципов в качестве правовых ограничений в деятельности государственных органов в условиях достаточно общего их определения законопроектом может привести к злоупотреблениям в осуществлении последними своих полномочий» (Официальный отзыв Правительства Российской Федерации на Проект закона о служебной тайне). К сожалению, указанное замечание достаточно точно отражает ситуацию с использованием принципов правового регулирования, особенно в сфере публичного управления. Так, как мы отмечали ранее, если в сфере частного права подход к пониманию принципов формируется на основе судебной практики (поскольку принципы относятся именно к регулированию поведения самих участников, а не законодательному процессу), то для формирования подходов в органах власти необходим большой объем не только оспариваемых ненормативных предписаний, а, что важно, оспаривание

нормативных актов. Но даже при реализации такого подхода, большое количество оспариваний нормативных актов будет означать нестабильность всей системы управления. Вместе с тем, ограничение доступа к информации только на основании принципов должно сопровождаться усиленными мерами персональной ответственности должностных лиц за нарушение принципов и правил ограничения доступа к информации.

В проекте федерального закона, разработанном Минэкономразвития, были предусмотрены более подробные «принципы:

- законность отнесения сведений о деятельности государственных органов и органов местного самоуправления к сведениям, охраняемым в режиме служебной тайны;

- обоснованность отнесения сведений о деятельности государственных органов и органов местного самоуправления к сведениям, охраняемым в режиме служебной тайны;

- своевременность отнесения сведений о деятельности государственных органов и органов местного самоуправления к сведениям, охраняемым в режиме служебной тайны и снятия режима ограниченного доступа;

- приоритет прав и свобод человека и гражданина перед правами других субъектов правоотношений;

- защита прав пользователей (потребителей) информации на доступ к информации;

- открытость и общественный контроль за деятельностью государственных органов и органов местного самоуправления;

- защита права граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых телеграфных и иных сообщений;

– ответственность за нарушение права пользователей (потребителей) информации». ¹

И все же, несмотря на столь подробную регламентацию принципов, документ в остальной части оперирует лишь принципами законности, обоснованности и своевременности, причем давая повторное объяснение указанным принципам в тексте проекта (ст. 7). Таким образом, проект не был в достаточной мере внутренне согласованным, кроме того, некоторые из принципов были дублирующими по своему смыслу. Так, к примеру, установление принципов защиты прав граждан на неприкосновенность частной жизни и защиты правы на доступ к информации при наличии принципа приоритета прав и свобод человека и гражданина в данном случае было бы излишним.

В постановлении Правительства РФ № 1223 приводится перечень информации, распространение которой не может быть ограничено. Все же Положение не закрепляет ни основания ограничения доступа к информации, ни условия отнесения информации к категории информации ограниченного распространения.

Следует отметить всё же, что в одном из перечней сведений, относящихся к служебной информации ограниченного распространения, содержатся интересные критерии для отнесения сведений к указанной «категории:

– служебная информация должна создаваться за средства районного бюджета или пребывать во владении, пользовании или распоряжении районного совета;

– использоваться с целью обеспечения национальных интересов государства и интересов территориальной громады района;

– не относиться к государственной тайне.

¹ Проект Федерального закона «О служебной тайне». – (http://www.dzyalosh.ru/02-dostup/zakon/rub-02/Fedzak_o_sltaine_0.htm). – Дата обращения: 17.12.2017.

В случае разглашения такой информации возможно:

- нарушение конституционных прав и свобод человека и гражданина;
- наступление негативных последствий во внутривнутриполитической, внешнеполитической, экономической, социальной, гуманитарной, научно-технологической, экологической, информационной сферах и в сферах государственной безопасности и безопасности государственной границы;
- нанесение ущерба интересам территориальной громады района;
- создание препятствий в работе районного совета и его исполнительного аппарата»¹.

Считаем, что выделение таких критериев отнесения информации к информации ограниченного доступа в достаточной мере отражает основные требования, которым должна соответствовать информация, относящаяся к служебной тайне. Вместе с тем, эти критерии нельзя назвать бесспорными. Так, к примеру, вопросы вызывает критерий возможных негативных последствий в случае разглашения информации. Этот критерий носит весьма оценочный характер, что может привести, в отсутствие устоявшейся практики применения и понимания этого критерия, к злоупотреблениям при ограничении доступа к сведениям. Также в этом подходе к информации, охраняемой в режиме служебной тайны, относится исключительно внутренняя информация государственного органа. В нее не включена информация, составляющая тайну третьих лиц. Этот момент следует назвать недостатком, поскольку в соответствии с постановлением Правительства РФ №1233 в эту категорию информации должна включаться поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.

Стоит отметить, что во многих нормативных актах отсутствуют критерии отнесения документов к разряду служебной информации

¹ Перечень сведений, составляющих служебную информацию в Нижнегорском районном совете и его исполнительном аппарате: распоряжение председателя Нижнегорского районного совета от 20.06.2011 № 12.

ограниченного доступа. На основании чего можно сделать вывод о том, что наличие либо отсутствие служебной необходимости для защиты информации решается уполномоченным лицом самостоятельно, в силу внутренних убеждений. Отсутствие правил отнесения той или иной информации к категории «служебная информация/служебная тайна» может привести (и приводит в большинстве случаев, особенно в уголовно-исполнительной системе) к произвольному нормотворчеству в системе государственных органов.

В связи с этим, считаем, что необходимо закрепить принципы, в соответствии с которыми будет возможно ограничение доступа к информации в режиме служебной тайны, а также установить определенные категории сведений, которые должны быть отнесены к сведениям, охраняемым в режиме служебной тайны.

Следует отметить, что этот подход не нов. Аналогичный подход используется в Законе о государственной тайне. Однако в законе используются достаточно общие принципы законности, обоснованности и своевременности. На наш взгляд, такие принципы возможны только при четком закреплении перечня сведений, доступ к которым ограничивается. В таком случае принципы играют только роль общих начал.

Считаем, что необходимо закрепить принципы ограничения доступа к информации, охраняемой в режиме служебной тайны. К ним, в частности, необходимо отнести:

- ограничение доступа к информации только на основании и в соответствии с федеральным законом;
- обоснование ограничения доступа к информации. Данный принцип должен подразумевать необходимость обоснования ограничения доступа к той или иной информации государственным органом, а также возможность обжалования решения об ограничении доступа к информации как в административном, так и в судебном порядке;

- приоритет прав и свобод человека и гражданина. Этот принцип должен включать в себя помимо права на информацию также гарантии соблюдения баланса интересов «национальной безопасности» и «общественного интереса»¹;

- надзор за ограничением доступа к информации. Данный принцип означает введение контроля и надзора за порядком ограничения доступа к информации, периодический пересмотр документов, доступ к которым ограничен;

- временный характер ограничения. Этот принцип означает установление определенного максимального срока для охраны конфиденциальности сведений. При этом относительно конфиденциальных сведений третьих лиц срок должен соответствовать установленному законом сроку ограничения тех или иных сведений, если речь идет о персональных данных, то в таком случае они должны охраняться бессрочно либо в соответствии с положениями нормативных актов по истечении определенного времени могут быть уничтожены.

В качестве обоснования ограничения доступа к сведениям могут служить введение следующих категорий:

- интересы, для охраны которых осуществляется ограничение доступа к информации;

- возможные последствия, во избежание которых ограничивается доступ к информации.

2.2. Категории сведений, охраняемых в режиме служебной тайны

¹ Здесь следует особо отметить необходимость учета общественного интереса. Зачастую возникают ситуации, при которых затрагиваются права и свободы коллективных субъектов (общества, населения города, района), но не затрагиваются напрямую интересы субъекта. В этом случае необходимо также предусмотреть возможность соблюдения баланса общественного интереса в соотношении с интересами государства как неотъемлемое право граждан и общества на информацию.

Вопрос определения категорий сведений, охраняемых в режиме служебной тайны, является достаточно сложным. Как справедливо отмечает И. Ю. Павлов, проблемой служебной тайны, как и государственной, является то, что перечень сведений, которые относятся к категории «служебная тайна» устанавливается внутренними актами, либо ведомственными актами, которые, в свою очередь, также не подлежат разглашению. Фактически получается замкнутый круг: в нормативном акте предусмотрено, что доступ может ограничиваться к тем сведениям, перечень которых предусмотрен нормативным актом, в свою очередь акт, в котором предусмотрен такой перечень сведений, сам является служебной информацией ограниченного доступа. И поэтому проверить законность либо незаконность отнесения той или иной информации к служебной тайне не представляется возможным.

Для определения круга информации, которая может быть отнесена к сведениям, охраняемым в режиме служебной тайны, начнем с выявления категорий сведений, которые не могут быть отнесены к информации ограниченного доступа ни при каких обстоятельствах. Одним из главных нормативных правовых актов, который определяет такой перечень, является Закон об информации, в соответствии с п. 4 ст. 8 которого не может быть ограничен доступ к нормативным актам, которые так или иначе затрагивают права, свободы человека и гражданина, устанавливают обязанности, а также устанавливают правовое положение организаций и полномочия государственных органов или органов местного самоуправления. Не может быть ограничен доступ к информации о состоянии окружающей среды, информации о деятельности государственных органов и органов местного самоуправления, об использовании бюджетных средств, информации, накапливаемой в открытых фондах библиотек, музеев и архивов, в государственных и муниципальных информационных системах, созданных для обеспечения граждан и организаций информацией, а также установлен запрет на ограничение доступа к иной информации, недопустимость ограничения доступа к которой установлена другими федеральными

законами.

Стоит обратить внимание на соотношение обязательных «базовых» требований к открытой информации с установленными на законодательном уровне правовыми ограничениями. Так, к примеру, важнейшей гарантией обеспечения законности и защиты прав и свобод человека и гражданина является недопустимость ограничения доступа к нормативным правовым актам, затрагивающим права и свободы человека и гражданина, или устанавливающих статус (правовое положение) организаций. Вместе с тем, в практике правового регулирования встречаются случаи, когда документы, прямо затрагивающие права и свободы граждан, не публикуются официально, поскольку относятся к служебной тайне. Наиболее часто такая проблема встречается в системе Федеральной службы исполнения наказания.¹ При этом органы, принимающие указанные акты, обосновывают свою позицию тем, что акт был издан в пределах компетенции, установленной законодательством. При этом совершенно игнорируется содержательная сторона спора – установление норм, прямо затрагивающих права и свободы граждан подзаконными нормативными актами.

Обязательным требованием законодательства является требование запрета ограничения доступа к сведениям о состоянии окружающей среды. Однако иногда в нормативных актах встречаются упоминания «об отнесении к сведениям, охраняемым в режиме служебной тайны, сведений о наличии радиоактивных веществ, сведений о происшествиях, могущих вызвать панику, до официального завершения расследования»². Кроме того, в некоторых ведомственных нормативных актах встречается информация о том, что информация о чрезвычайных ситуациях, а также мерах по их устранению

¹ Решение Верховного суда от 18.06.2012 Дело № АКПИ12-543 // Сайт компании «Гарант». – (<http://www.garant.ru/products/ipo/prime/doc/70097054/>). – Дата обращения: 17.12.2017.

² Об утверждении временного перечня сведений, составляющих служебную информацию ограниченного распространения: постановление Администрации Кировской области от 18.06.1997 № 183 (ред. от 08.10.1997).

может быть также отнесена к разряду информации ограниченного доступа.¹ На наш взгляд, такой подход не всегда является корректным, поскольку зачастую именно какие-либо чрезвычайные ситуации техногенного характера являются причиной резкого ухудшения состояния окружающей среды. И именно немедленное информирование о таких чрезвычайных ситуациях необходимо для того, чтобы можно было избежать тяжелых последствий для жизни и здоровья населения. Кроме того, такая обязанность предусмотрена законом².

Еще одной важной гарантией права на информацию является запрет ограничения доступа к информации о деятельности органов г.в. и м.с.у.. Кроме указанной нормы, для повышения открытости органов государственной власти, а также снижения возможного риска злоупотребления правом на ограничения доступа к информации, Закон о государственной тайне устанавливает перечень информации, доступ к которой не может быть ограничен. Соответственно, если такая информация не может охраняться в режиме государственной тайны, считаем, что такая информация не может охраняться и в иных режимах. Такой вывод основан на общем смысле законодательства об информации, а также на исследованиях норм подзаконных актов. Так, к примеру, существуют ведомственные акты³ Следственного Комитета, которые закрепляют те категории сведений, доступ к которым не может быть ограничен. При этом указанные критерии дублируют те, что указаны в Законе о государственной тайне. Такое регулирование свидетельствует о недопустимости ограничения доступа к

¹ Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Государственном комитете Кабардино-Балкарской Республики по транспорту и связи: приказ Государственного комитета Кабардино-Балкарской Республики по транспорту и связи от 16.01.2015 года № 4-П.

² О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон от 21.12.1994 № 68-ФЗ (ред. от 23.06.2016).

³ Об утверждении Порядка отнесения служебной информации к разряду ограниченного распространения и обращения с документами, содержащими служебную информацию ограниченного распространения, в системе Следственного комитета Российской Федерации: приказ Следственного комитета России от 23 декабря 2014 г. № 109.

информации, доступ к которой не может быть ограничен в режиме государственной тайны, и в других режимах информации.

При обозначении круга сведений, доступ к которым не может быть ограничен, следует вспомнить, что существует также один нормативный акт, который устанавливает перечень информации, относимой к категории «открытые данные»¹. Сведения, относимые к данной категории, должны находиться в свободном доступе вне зависимости от наличия либо отсутствия запроса таких данных гражданами.

При первичном анализе нормативных актов получаем достаточно обширный перечень данных, доступ к которым не может быть ограничен. В том числе, это большой объем информации о деятельности органов власти и местного самоуправления. В то же время вызывает вопрос соотношение таких гарантий с нормативными предписаниями для государственных служащих: так, в Законе о государственной гражданской службе в пп. 7, п. 1, ст. 15 предусмотрена обязанность государственного служащего «не разглашать сведения, <...> ставшие ему известными в связи с исполнением должностных обязанностей». В свете принципа открытости государственной власти, представляется необоснованным такое требование к должностному служащему: как минимум те сведения, которые являются «открытыми данными», а также не могут быть ограничены в доступе или содержаться в режиме государственной тайны, должны быть изъяты из общего правила. Кроме того, возникает вопрос о том, должен ли хранить государственный служащий в тайне (не разглашать) абсолютно все сведения, которые стали ему известны в результате служебной деятельности? В таком случае даже обычный семейный разговор о том, как прошел день, превращается в разглашение служебной информации и, соответственно, нарушение требований, предъявляемых к государственному служащему. Именно такое

¹ Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 09.02.2009 г. №8-ФЗ (ред. от 09.03.2016).

требование, на наш взгляд, является тем основанием, согласно которому служебная тайна отождествляется со служебной информацией. На наш взгляд, такое отождествление является необоснованным.

Можно сравнить коммерческую тайну и тайну, которую должны хранить государственные служащие. В ФЗ «О коммерческой тайне» дается определение коммерческой тайны, в соответствии с которой под ней понимается режим конфиденциальности информации. Законом предусмотрено три признака информации, относящейся к коммерческой тайне, одним из которых является введение в отношении такой информации режима коммерческой тайны. В свою очередь, ст. 10 устанавливает целый ряд мер, которые должны быть приняты для охраны коммерческой тайны. Именно такая информация должна сохраняться работником в тайне. Соответственно, это строго определенный круг сведений, которые не могут быть разглашены. И только за разглашение конкретных сведений возможно привлечение работника к ответственности.

В то же время, зачастую на практике работодатели стремятся засекретить абсолютно всю информацию, которая может стать известна работнику в ходе исполнения им трудовых обязанностей, прописывая в трудовом договоре пункт об обязательности сохранения любой информации, связанной с деятельностью компании, в том числе и о размере заработной платы, об условиях трудового договора, а также условиях труда. Кроме того, иногда в положениях о конфиденциальности работодатели стремятся сделать указание на то, что вся информация о деятельности компании составляет коммерческую тайну за исключением тех сведений, отнесение которых к конфиденциальным запрещено ФЗ «О коммерческой тайне». Такое положение, хоть и законно, на первый взгляд, однако его соблюдение практически не является возможным в силу несоблюдения требований к режиму такой информации:

1. Отсутствует перечень информации, относимой к конфиденциальной информации. Некоторые авторы, анализируя судебную

практику и практику гражданского оборота, отмечают, что, как правило, «бесспорным доказательством волеизъявления правообладателя о наделении той или иной информации юридической характеристикой коммерческой тайны является указание на нее в гражданско-правовом договоре»¹. В свою очередь, на наш взгляд, попытка ограничить доступ к информации, которая может быть получена работником/иным лицом в процессе осуществления трудовой функции/исполнения обязательств по договору в общем, является несостоятельной. Такая позиция, в частности, была высказана еще 2012 г. В одном из дел² правообладатель попытался установить режим «коммерческой тайны» в отношении всех сведений о деятельности сторон, полученных ими при заключении, изменении (дополнении), исполнении и расторжении договора, а также сведений, вытекающих из содержания договора путем включения указанной формулировки в текст договора. Суд посчитал перечень информации, содержащий коммерческую тайну, недостаточно определенным и оформленным.

2. Необходим контроль за соблюдением порядка доступа и обращения с такой информацией. Для этого, как правило, используются технические средства либо организационные. Такие процедуры контроля и организации являются крайне затратными и значительно усложняют порядок работы с такой информацией (так, в частности, как правило, используются только защищенные каналы связи, запрещается работа со сведениями вне помещения работодателя, либо ведется строгий учет сведений и лиц, которые получили к ним доступ и т.д.). Если же применять такой порядок работы ко всей информации компании, работа значительно усложнится и повысятся издержки на охрану информации и обеспечение технических мер для ее сохранения в тайне.

¹ Осокина Е. Ю. О некоторых проблемах применения новых положений ГК РФ о промышленной собственности / Е. Ю. Осокина // Право и экономика. – 2015. – №2.

² Определение ВАС РФ от 23.08.2012 № ВАС-10500/12 по делу № А27-12862/2011. – (<http://kad.arbitr.ru/Card/1d23db0f-f4d2-4e54-9fed-e0808b97e6f4>). – Дата обращения: 17.12.2017.

По факту же, та информация, которая не обеспечена организационными и технологическими методами защиты, охраняется только совестью работника, поскольку в соответствии с подпунктом 3 п. 1 ст. 11 указанного ФЗ «О коммерческой тайне» работодатель обязан «создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны». Если же такие условия не соблюдены, работодателю может быть отказано в иске на основании п. 5 ст. 11 указанного закона.

Итак, проводя аналогию между режимами коммерческой тайны и служебной информации, можем сделать вывод о том, что ко всей информации, существующей и образующейся в результате деятельности органов государственной власти, не может применяться требование о неразглашении. Такой же вывод следует и при изучении требований к ограничению доступа к информации в режиме государственной тайны. Требование о неразглашении всей существующей информации в органах государственной власти прямо противоречит Закону об информации, а также принципу открытости деятельности органов г.в. и м.с.у..

Такой подход к ограничению распространения служебной информации критикуется исследователями: так, к примеру, Е. К. Волчинская отмечает, что в таком случае «требование в части установления условий отнесения информации к сведениям, составляющим служебную тайну, обязательности соблюдения конфиденциальности такой информации, на законодательном уровне не выполнено»¹. И мы согласны с этим мнением.

На основе анализа многочисленных постановлений и приказов различных органов власти о порядке обращения со служебной информацией, можем сделать вывод о том, что в изученных документах отсутствует единообразие понимания служебной информации и служебной тайны. Об этом свидетельствует тот момент, что в некоторых нормативных актах

¹ Волчинская, Е. К. Ограничение доступа к служебной информации: административно-правовые аспекты // магистерская диссертация. – Челябинск, 2014. – С.24.

встречается упоминание об ограничении доступа и распространения служебной информации как таковой¹, за исключением той информации, доступ к которой не может быть ограничен. В других же нормативных актах указывается порядок работы с конкретными категориями служебной информацией ограниченного доступа. Таким образом, в нормативных актах очерчивается круг сведений, в отношении которых применяется установленный порядок.

Еще одним требованием законодателя является запрет на ограничение доступа к информации, накапливаемой в открытых фондах библиотек. Такое требование получило свое развитие в Законе о библиотечном деле.

Проблема содержания архивов, библиотек и прочих хранилищ является одной из актуальнейших проблем информационного права². Вместе с тем, несмотря на указанный принцип, и в библиотеках существуют определенные ограничения доступа к информации: так, к примеру, во многих библиотеках существует отдел «ДСП», куда в 1988 году были переведены множество книг и документов ограниченного доступа. К документам из указанного фонда можно получить доступ лишь по письму-отношению, которое выдает организация, от лица которой обращается человек в библиотеку. Кроме того, существует также раздел экстремистской литературы, доступ к которой является ограниченным (к такой литературе относится, например, *Mein Kampf* А. Гитлера), то есть доступ к такой литературе можно также получить только при наличии письма-отношения (такое правило действует в ряде крупнейших библиотек страны (Российская государственная библиотека, Российская национальная библиотека и т.д.). При этом работники библиотеки³

¹ О работе со служебной информацией в Совете депутатов муниципального образования «Пироговское»: решение Совета депутатов муниципального образования «Пироговское» от 28.08.2014 № 89. Обратим внимание на то, что указанное решение регулирует работу депутатов, а не государственных либо муниципальных служащих, однако позволяет понять принятую концепцию работы со служебными сведениями в целом.

² Ее важность подчеркивает Тедеев А. А.: Тедеев, А. А. Предмет информационного права в условиях Интернета / Тедеев А. А. // Информационное право. – 2006. – №3. – С. 3-5.

³ Диссертант беседовал с работниками Российской Государственной библиотеки, Российской Национальной библиотеки, Челябинской областной научной библиотеки.

признаются, что никаких нормативных оснований, либо же даже внутренних документов для того, чтобы отказать в выдаче запрашиваемой литературы при наличии письма-отношения (практически вне зависимости от указанной там организации, цели получения информации), у библиотеки нет. В одной из работ¹, посвященной проблеме размещения информации ограниченного доступа в библиотеках, отмечается, что единственным актом, который может на настоящий момент регулировать порядок работы с литературой ограниченного доступа является Инструкция о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения. Указанного документа ни в сети Интернет, ни в библиотеках обнаружить не удалось.

Стоит отметить, что в библиотеках для обоснования ограничения доступа к информации и регулирования такого доступа применяется один акт, юридическая сила и основание принятия которого вызывает вопросы. Работники библиотеки ссылаются на такой акт, как «Инструкция о порядке обращения с документированной служебной информацией ограниченного распространения в организациях, учреждениях, предприятиях и т.д.», принятую в Москве в 2000 г. Госглавэкспертизой. При этом документ можно найти в Интернете без каких-либо реквизитов: даты принятия, номера, источника опубликования, а также фамилии должностного лица, утвердившего эту инструкцию. Кроме того, информация, имеющаяся в сети Интернет о Госглавэкспертизе свидетельствует о крайне ограниченных полномочиях и компетенции данного органа. В лучшем случае этот акт мог действовать только в рамках этого органа, регулирующего деятельность в сфере строительства.

¹ Махотина, Н. В. Фонд литературы ограниченного распространения в научных библиотеках: базовые аспекты функционирования: автореф. дисс. ... канд. пед. наук. // Н. В. Махотина. – Новосибирск, 2011. – 20 с.

Таков результат перестроения системы информации ограниченного доступа без применения адаптирующих моделей для всех участников производства, накопления, хранения и распространения информации.

Кроме указанных исключений отнесения сведений к информации ограниченного доступа в ведомственных актах регулирование, как правило, строится на основе выделения круга той информации, доступ к которой не может быть ограничен в режиме служебной тайны.

Как правило, акты выделяют семь категорий сведений, доступ к которым не может быть ограничен:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Многие подзаконные акты дублируют перечень сведений, установленный постановлением Правительства РФ №1233¹.

Большая часть нормативных актов построены по модели утверждения перечня сведений, которые не могут быть отнесены к сведениям, охраняемым в режиме служебной тайны. При этом не устанавливаются перечни сведений, доступ к которым должен быть ограничен либо может быть ограничен.

Считаем, что такая модель регулирования повышает риски злоупотребления правом на ограничение доступа к информации в органах власти.

В данном случае напрашиваются аналогии с иными федеральными законами, которые устанавливают режим информации ограниченного доступа. Законов, которые устанавливают режим информации ограниченного доступа в отношении широкого круга сведений, для которого необходимо определение, не так много: это Закон о государственной тайне и ФЗ «О коммерческой тайне». Остальные нормативные акты устанавливают ограничение в отношении распространения узкой категории сведений. К примеру, налоговая тайна подразумевает вполне конкретный перечень сведений о налогоплательщике, который должны охраняться. И если рассмотреть модель регулирования налоговой тайны, можно сказать, что она построена также на принципе «изъятия», то есть установления ограничения определенного круга информации о налогоплательщике, которая не может

¹ Об утверждении Инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации: приказ Министерства образования и науки Российской Федерации от 30.12.2010 г. № 2233 (ред. от 10.08.2012).

Инструкция о порядке обращения со служебной информацией ограниченного распространения в исполнительных органах государственной власти Ямало-Ненецкого автономного округа: постановление Администрации Ямало-Ненецкого автономного округа от 28.01.2010 г. № 49-А

Об утверждении Положения о порядке работы со служебной информацией ограниченного распространения в администрации Волжского муниципального района: Распоряжение администрации Волжского муниципального района от 18.04.2012 г. № 71.

Об утверждении инструкции по делопроизводству в вооруженных силах Российской Федерации: Приказ Министра обороны Российской Федерации от 23.05.1999 № 170 (ред. от 27.05.2004).

охраняться налоговым органом, однако вся иная информация, которая не указана в исключении, не должна быть распространена (ст.ст. 102,113 Налогового кодекса Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ). В то время как под категорию коммерческой либо государственной тайны сведения могут попадать либо не попадать в зависимости от волеизъявления правообладателя такой информации.

Если рассмотреть модель регулирования государственной тайны, то здесь можно обнаружить, что помимо установления круга сведений, доступ к которым не может быть ограничен, Закон о государственной тайне закрепляет перечень сведений, охраняемых в таком режиме. Кроме того, данный перечень детализируется в Указе Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» (Далее – Указ Президента РФ №1203), а также закрепляет те органы государственной власти, которые имеют право распоряжаться такой информацией. Таким образом, сведения, доступ к которым ограничивается, строго регламентирован в нормативных актах, являющихся официально опубликованными.

Если изучить модель регулирования коммерческой тайны, то здесь можно обнаружить, что ФЗ «О коммерческой тайне» дает только тот перечень сведений, доступ к которым не может быть ограниченным. Остальные же сведения могут быть отнесены к коммерческой тайне в случае, если перечень будет прописан в локальных нормативных актах правообладателя. Расширительное толкование коммерческой тайны в данном случае не допускается. Таким образом, в указанном нормативном акте происходит рамочное регулирование отношений, но подробное регулирование должно быть в обязательном порядке в локальных актах организации с четким указанием категорий сведений, относящихся к коммерческой тайне предприятия.

В то же время, такая модель, хоть и является близкой по способу правового регулирования к служебной тайне, все же существенно отличается от нее требованием законодательства о строгом закреплении перечня

сведений в актах правообладателя. В то время как в отношении служебной тайны зачастую единственным критерием отнесения информации к сведениям, охраняемым в режиме служебной тайны, является служебная необходимость. На основе анализа нормативных актов, устанавливающих порядок отнесения сведений к служебной тайне, работы с ними, а также перечней сведений, охраняемых в режиме служебной тайны, выявим тот круг информации, которая чаще всего подпадает под критерии «служебной тайны».

Исследуем ряд перечней сведений, к которым удалось получить доступ¹.

В основном доступны перечни администраций муниципальных районов, администраций областей. Начиная с 2015 года, появился большой массив нормативных актов, утверждающих положения/инструкции о порядке работы со служебной информацией ограниченного доступа, что, на наш взгляд, «является несомненным шагом вперед на пути к прозрачности и открытости системы государственного управления. Стоит отметить, что большинство инструкций и положений не устанавливают перечень сведений, доступ к которым может быть ограничен в режиме *служебной тайны*.

Рассмотрим ряд нормативных актов, которые все же устанавливают категории сведений, которые могут быть отнесены к режиму служебной тайны. В ряде перечней под служебной информацией понимаются «сведения об информационно-аналитической системе; аналитические прогнозы; заключения, вследствие разглашения которых возможно нарушение конституционных прав и свобод человека и гражданина, наступление негативных последствий в государстве и районе, создание препятствий в работе райсовета и его исполнительного аппарата; сведения о технических возможностях программного обеспечения, компьютерной техники, которые

¹ Сразу оговоримся, что проверить, являются ли эти документы действующими, не представляется возможным в силу их особого характера.

используются; служебная корреспонденция; сведения об экономическом положении крупнейших предприятий, о научно-технических разработках; сведения о структуре, составе, объеме автопарка, маршруте передвижения главного должностного лица области; сведения о местах хранения вооружений; сведения о предстоящих международных визитах, содержании экономических договоренностей, программах пребывания, также персональные данные, сведения, составляющие тайну судопроизводства; сведения, связанные с профессиональной деятельностью (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений)»¹.

В некоторых нормативных актах встречается разделение служебной информации на служебную тайну и информацию о частной жизни лица («чужая» тайна). Так, например, приказ Государственного комитета Кабардино-балкарской республики по транспорту и связи от 16 января 2015 г. № 4-П «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Государственном комитете Кабардино-Балкарской Республики по транспорту и связи» устанавливает перечень сведений, отнесенных к конфиденциальной (служебной) информации. В перечне указывается отдельно такая категория как «служебная тайна» (п. 2), при этом, помимо прочих категорий, перечисленных в перечне, отдельно выделяется категория сведений, ограничение доступа к которым диктуется служебной необходимостью, что фактически означает открытый характер перечня и позволяет его трактовать предельно широко.

¹ Составлено в результате изучения следующих нормативных актов:

Об организации работы со служебной информацией ограниченного доступа в исполнительных органах государственной власти Архангельской области: указ Губернатора Архангельской области от 25.08.2011 № 125-у;

Перечень сведений, составляющих служебную информацию в Нижегородском районном совете и его исполнительном аппарате: распоряжение председателя Нижегородского районного совета от 20.06.2011 №12.

И др.

По результатам анализа различных ведомственных нормативных актов, а также актов органов власти субъектов и местного самоуправления, мы можем сделать вывод о том, что в нормативных актах под служебной информацией ограниченного доступа понимается внутренняя информация государственных органов (заметим, что именно эта классификация приведена в таблице) и конфиденциальная информация третьих лиц – информация, ставшая известной государственным органам, органам местного самоуправления и относящаяся к категории конфиденциальной (персональные данные, профессиональная тайна, тайна следствия и т.д.). Можно выделить определенные категории сведений (хотя иногда весьма условно), отнесенных к информации ограниченного доступа, которые чаще всего указываются в таких перечнях:

1. Сведения, касающиеся информационной безопасности государственных органов, к которым относятся информация о порядке защиты информации, логины, пароли для входа в информационную систему и другая информация, обеспечивающая работу с информационными системами и их функционирование.

2. Сведения в области физической безопасности субъектов. Указанные сведения можно подразделить на:

а. сведения, в области безопасности органа государственной власти/местного самоуправления;

б. сведения в области безопасности населения, в том числе мобилизационные сведения, сведения о безопасности систем жизнедеятельности и гражданской обороне.

3. Сведения в сфере административно-хозяйственной деятельности, к которым относятся те сведения, которые касаются организационного технического и хозяйственного обеспечения деятельности, в том числе протоколы заседания комиссий по замещению вакантных должностей, инструкции по делопроизводству, информация по кадровому составу,

штатному расписанию и количественному составу государственного органа и т.д.

4. Информация о непосредственной работе государственного органа. Эта группа выделена достаточно условно, однако является одной из наиболее крупных. К ней относятся сведения о внешнеэкономических связях, информация и протоколы закрытых заседаний, проекты нормативных документов, аналитические материалы об экономическом состоянии той или иной отрасли, переписка и корреспонденция¹.

5. Информация в сфере научно-технических разработок. Такая категория сведений выделяется в нормативных документах крайне редко, однако именно для специализированных учреждений это является очень важной категорией сведений.

6. Сведения в геодезии, картографии и проектировании.

7. Конфиденциальная информация третьих лиц.

8. Иные сведения.

Пожалуй, это та группа, которая вызывает больше всего нареканий. Как правило, к ней относится, помимо прочего (обычно, кадровых вопросов), такая формулировка: «Сведения, содержащиеся в документах с пометкой «Для служебного пользования», в части, не содержащей сведения, составляющих государственную тайну, <...> образующиеся в деятельности государственного органа, ограничение на распространение которых диктуется служебной необходимостью, за исключением сведений, которые не могут быть отнесены к служебной информации ограниченного распространения»².

¹ Стоит отметить, что именно в этой категории сведений очень часто встречаются положения, противоречащие федеральному законодательству.

² См. к примеру:

Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации и организаций, находящихся в его ведении: приказ Министерства финансов России от 17.06.2014 № 162 (ред. от 16.11.2015);

Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Государственном комитете Кабардино-Балкарской Республики по транспорту и связи: приказ Государственного комитета Кабардино-

Такая формулировка делает возможным отнесение неограниченных массивов информации к служебной информации ограниченного распространения. В одном из нормативных правовых актов к этой категории сведений были отнесены «сведения о происшествиях, могущие вызвать панику, межнациональные конфликты, до официального завершения расследования, сведения о наличии радиоактивных веществ»¹. Такое ограничение к доступу информации просто недопустимо, так как напрямую противоречит положению Закона об информации.

Следует отметить, что указанный перечень утратил свою силу, в 1997 году определением Верховного Суда РФ ряд положений указанного перечня были признаны недействительными².

А. А. Антопольский отмечает, что отсутствие единой нормативной базы для регулирования служебной информации вынуждает региональные органы г.в. и м.с.у. самостоятельно регулировать такие отношения. И такие региональные нормы, если только они не формально копируют положения постановления Правительства РФ № 1223 или Указ Президента РФ № 188, часто вступают в прямое или косвенное противоречие с нормами Конституции Российской Федерации и федерального законодательства³.

Считаем, что необходимо в законодательном порядке определить те категории сведений (сферы, в которых может ограничиваться доступ к сведениям), кроме того, необходимо утверждение перечней информации каждым государственным или муниципальным органом, в котором есть потребность для ограничения доступа к определенным категориям сведениям.

Балкарской Республики по транспорту и связи от 16.01.2015 года № 4-П (ред. от 03.08.2016).

¹ Об утверждении временного перечня сведений, составляющих служебную информацию ограниченного распространения: постановление администрации Кировской области от 18.06.1997 № 183 (ред. от 08.10.1997).

² Определение Верховного Суда РФ от 10.11.1997 № 10-Г97-4 // Сайт компании «Консультант Плюс».

³ Антопольский, А. А. Региональное законодательство о конфиденциальной служебной информации / А. А. Антопольский // Информационные ресурсы России. – 2005. – № 3. – С. 28-31.

Следует отметить, что в Республике Беларусь в 2014 году было принято Положение¹ о порядке проставления ограничительного грифа «Для служебного пользования» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения. Указанное положение обязательно для исполнения всеми государственными органами. Вспомним, что в Республике Беларусь служебная тайна включена в систему государственных секретов. В положении установлены категории сведений, которые должны быть отнесены к служебной тайне. В положении насчитывается 114 позиций. К ним относятся 18 групп сведений: мобилизационные вопросы; наука и техника, научно-техническая информация; оборона и государственная безопасность; вопросы гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций, заимствования материальных ценностей; военно-техническое сотрудничество; правоохранительная деятельность; промышленность; энергетика; геология; полезные ископаемые, их добыча и переработка; транспорт; связь; внешнеэкономическая деятельность, финансы; банковская деятельность; геодезия, картография; гидрометеорология; медико-санитарные вопросы; иные сведения.

Вместе с тем, перечень не является закрытым, так как последняя группа «иные сведения» сформулирована следующим образом: «Иные сведения, касающиеся деятельности государственного органа, государственной организации, иного юридического лица, организации, не являющейся юридическим лицом, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц, организаций, не являющихся юридическими лицами».

¹ О служебной информации ограниченного распространения: Постановление Совета Министров Республики Беларусь от 12 августа 2014 г. № 783.

регламентирование, по сути, сводит к нулю установление конкретных категорий сведений, поскольку размытая формулировка позволяет государственным органам относить к сведениям, охраняемым в режиме служебной тайны практически любые сведения. Что же касается указанного перечня, то он будет служить скорее ориентиром для государственных органов, но не гарантией информационных прав граждан. Саму же проблематику критерия «национальная безопасность» мы рассматривали ранее в работе.

Ранее были разработаны и предложены два проекта Федерального закона «О служебной тайне», которые предлагали ввести следующий перечень сведений, доступ к которым должен быть ограничен:

1. В перечне, предлагаемом Минэкономразвития установлены два типа перечней – сведения, доступ к которым должен быть ограничен, и сведения, доступ к которым может быть ограничен. К первому перечню относились «сведения, добровольно передаваемые в установленном порядке в государственные органы и органы местного самоуправления физическими лицами или организациями на условии сохранения их конфиденциальности, если требование сохранения их конфиденциальности является законным и обоснованным; сведения, связанные с условиями для поставки товаров для государственных (муниципальных) нужд предложенными организациями, допущенными в установленном порядке к участию в конкурсах (тендерах) на поставку товаров для государственных (муниципальных) нужд; персональные данные физических лиц, находящиеся в распоряжении государственного органа или органов местного самоуправления в связи с выполнением им своих полномочий; сведения о деятельности государственных органов и органов местного самоуправления, отнесенные к конфиденциальной информации в соответствии с федеральными законами»¹.

¹ Проект Федерального закона «О служебной тайне» - (<https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiHqer575DXAhVoDZoKHUrJDCoQFggxMAI&url=http%3A%2F%2Fwww.sibirp.ru%2Fattachments%2>)

Ко второму перечню относились «сведения, связанные с подготовкой проектов индивидуальных правовых и нормативных правовых актов, включая тексты проектов таких актов, если их преждевременное распространение и (или) разглашение нанесет ущерб балансу жизненно важных интересов личности, общества и государства либо приведет к созданию односторонних преимуществ для субъектов, получивших доступ к указанным сведениям; сведения о запланированных, готовящихся и проводимых проверках за соблюдением законодательства Российской Федерации; сведения о кандидатах на замещение должностей государственной службы, должностей муниципальной службы, если иное не предусмотрено федеральным законом; сведения об авторстве предложений и личных позициях, изложенных в ходе обсуждений, консультаций в процессе работы государственного органа, органа местного самоуправления, за исключением случаев, когда автор публично оглашает данные сведения либо не возражает против раскрытия сведений о своем авторстве; сведения о внутриведомственных и межведомственных обсуждениях, консультациях рабочего и подготовительного характера, включая протоколы совещаний, служебные записки, справочные и иные материалы, имеющие подготовительный характер, если иное не предусмотрено федеральными законами»¹.

2. В проекте, предложенном депутатами Государственной Думы, перечень сведений не был предусмотрен. Его разработка должна была проводиться комиссиями, формируемыми в органах государственной власти.

Как следует из приведенного анализа нормативных правовых актов, установление объектов режима служебной информации возможно двумя путями: с одной стороны, очерчивается круг тех сведений, доступ к которым не может быть ограничен (в условиях правового регулирования Российской

Feditor%2Ffiles%2Fmod_structure%2F13%2Fseminar1_13.doc&usg=AOvVaw1cTvzbzgfUhIOChEdKVPf62). – Дата обращения: 17.12.2017.

¹ Публикуется по монографии Прокопенко, А. А., Дрога, А. А. Правовое регулирование оборота информации, относящейся к служебной и профессиональной тайне в органах внутренних дел: монография / А. А. Прокопенко, А. А. Дрога. – Белгород: БелЮИ МВД России, 2011. – 97 с.

Федерации эти ограничения обуславливаются наличием обязательной для раскрытия информации – открытых данных и перечней категорий сведений, доступ к которым не может быть ограничен); с другой стороны, может быть установлен непосредственно перечень той информации, доступ к которой может быть ограничен в режиме служебной тайны. Считаем, что поскольку в регулировании деятельности органов государственной власти преобладает административистский подход, необходимо разработать перечень категорий сведений, доступ к которым может быть ограничен с учетом требований законодательства к информационной открытости власти по аналогии с порядком установления перечня сведений в области государственной тайны.

Вместе с тем, вопрос об установлении конкретного закрытого перечня сведений, доступ к которым должен быть ограничен, является одним из наиболее спорных, поскольку многие отмечают крайне широкий спектр сведений, существующих в системе государственного управления, доступ к которым не может быть открыт. Все же полагаем, что необходимо обозначить четкий перечень не самих сведений, а категорий сведений, доступ к которым может быть ограничен. Этот перечень должен быть закрытым. Его составление возможно в результате детального изучения ведомственных перечней, доступ к которым в настоящий момент является закрытым.

Считаем, что помимо определения сведений, охраняемых в режиме служебной тайны, необходимо сделать перечень таких сведений открытым в соответствии с общим принципом законности, так как даже в открытых перечнях можно обнаружить нарушения законодательства (стоит вспомнить о том, что долгое время постановление №1233 не было официально опубликовано и относилось к служебной тайне).

Возвращаясь к вопросу о возможности отнесения иных видов информации ограниченного доступа, затронутым в третьем параграфе первой главы, отметим, что, исходя из сходности базовых элементов правового режима (принципы, объект, субъект), важно говорить о теоретической возможности объединения в режим служебной тайны достаточно большого

массива информации, доступ к которой ограничивается. Вместе с тем, нерешенным остается вопрос о возможности соотношения мер, принимающихся для защиты информации, а также ответственности за ее разглашение. В случае унификации последних двух элементов возможно объединение в режим служебной тайны многих видов информации ограниченного доступа. Так, к примеру, по сходности объектов (информации, образующейся в государственных органах или органах местного самоуправления либо поступающей туда и являющейся тайной третьих лиц), так и по кругу субъектов (государственные и муниципальные служащие), могли бы быть объединены многие виды информации ограниченного доступа.

В приложении к настоящей диссертации приведена сравнительная таблица различных видов информации ограниченного доступа, в отношении которой предусмотрено условие соблюдения ее конфиденциальности в соответствии с требованиями Федеральных законов и приведена характеристика информации по четырем пунктам: нормативный акт, которым установлено требование соблюдения конфиденциальности информации; субъекты, на которых возложена обязанность по соблюдению конфиденциальности информации; порядок работы с информацией (пункт предусматривает нормативное регулирование порядка работы с информацией), а также меры ответственности, предусмотренные в случае нарушения защиты информации.

Указанный анализ проводился с целью выявления возможности отнесения некоторых видов сведений к информации, которая может охраняться в режиме служебной тайны и создания системы объектов служебной тайны. При этом 15 из 27 видов информации так или иначе представляют собой персональные данные и/или информацию о личной жизни граждан, ряд сведений образуется в результате деятельности государственных органов (проведении проверок, участии организаций в госзакупках, осуществлении иных функций государственных органов).

Субъектами, на которые возложена обязанность по обеспечению конфиденциальности информации, как правило, являются органы государственной власти, местного самоуправления, должностные лица либо государственные служащие. Однако во многих случаях субъектами также становятся подведомственные организации, либо организации, граждане, выполняющие работу на основании договора с государственными либо муниципальными органами.

Отдельно стоит поговорить о регламентации мер защиты информации, применяемых в каждом конкретном случае. В большинстве рассмотренных случаев осуществляется как автоматизированная, так и неавтоматизированная обработка информации. При этом автоматизированная обработка данных во многих случаях происходит в государственных автоматизированных информационных системах (ГИСах/ГАСах) либо в автоматизированных информационных системах (АИСах).

При этом в государственных информационных системах могут существовать открытые и закрытые части, в которых представлена общедоступная информация и конфиденциальная информация соответственно. Основные правила, регулирующие государственные информационные системы установлены ст. 14 Закона об информации, а также постановлением Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации». Существуют отдельные ведомственные приказы, как правило, в правоохранительных органах, в отношении ведения информационных систем.

Стоит отметить, что, как правило, ответственность за разглашение видов информации ограниченного доступа не конкретизируется (за исключением уголовной ответственности) и является общей для нарушения режима конфиденциальности.

Вместе с тем, в приведенной таблице указан ряд различий в регулировании и обеспечении ограничения доступа к различной информации. Указанные различия, а также их степень, на наш взгляд, позволяют понять возможность защиты информации в режиме служебной тайны.

Так, в частности, по признаку субъектного состава и мерам ответственности к сведениям, охраняемым в режиме служебной тайны, не могут быть отнесены следующие сведения:

- Факт передачи в федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма информации, поскольку субъектами, которые обязаны соблюдать конфиденциальность указанной информации, являются организатор торговли, клиринговая организация и центральный контрагент. Таким образом, указанная информация не соответствует существенным характеристикам информации, охраняемой в правовом режиме служебной тайны, поскольку в этом случае охраняется сам факт передачи информации передающими лицами, а не ее содержание.

За разглашение этой информации лица могут быть привлечены к административной ответственности за неисполнение требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ст. 15.27 КоАП, а также к уголовной ответственности по ст. 174, 205.1 УК РФ).

Тайна усыновления также не может быть отнесена к сведениям, охраняемым в режиме служебной тайны, в полной мере, поскольку субъектами, на которые возложена обязанность сохранения тайны, являются не только Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, но также и иные лица, которым стала известна указанная информация. Таким образом, круг субъектов так или иначе может быть достаточно широк, а субъекты, которым стало известно об указанном факте,

не связаны договорными отношениями или отношениями государственной службы. Соответственно, субъектный состав не позволяет отнести тайну усыновления к категории информации, охраняемой в режиме служебной тайны.

Также стоит отметить, что в отношении разглашения тайны усыновления в Уголовном кодексе статьей 155 предусмотрен специальный состав преступления, при этом круг субъектов определен в общем виде: к ответственности может быть привлечено лицо, обязанное хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иное лицо, разгласившее тайну из корыстных или иных низменных побуждений.

- Сведения, содержащиеся в заявках на участие в конкурсе на право заключить контракт на проведение лотерей.

Указанные сведения также не могут охраняться в режиме служебной тайны, поскольку субъектами, обязанными сохранять конфиденциальность сведений являются участники размещения заказа, подавшие заявки на участие в конкурсе, организатор лотереи, лица, осуществляющие хранение конвертов с заявками на участие в конкурсе и заявок на участие в конкурсе, поданных в форме электронных документов.

- Отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. К таким сведениям относятся сведения об участниках аукциона, а также сведения, содержащиеся в конвертах с заявками на участие в открытом конкурсе, в форме электронных документов заявок на участие в открытом конкурсе до момента проведения аукциона. Также не могут быть признаны информацией, охраняемой в режиме служебной тайны, поскольку сохранность указанных сведений обеспечивается оператором электронной площадки, который не является государственным органом, подведомственной организацией, а также порядок защиты сведений определяется отдельным нормативным актом (Приказ Минэкономразвития России от 23.07.2015 № 495 «Об утверждении

Порядка проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, Требований к операторам электронных площадок, к электронным площадкам, в том числе технологическим, программным, лингвистическим, правовым и организационным средствам, необходимым для проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве»).

Также в этом случае предусмотрен специальный вид ответственности: нарушение порядка и (или) сроков возврата денежных средств, внесенных в качестве обеспечения заявок на участие в определении поставщика (подрядчика, исполнителя), порядка и (или) сроков блокирования операций по счету участника закупки, порядка ведения реестра участников электронного аукциона, получивших аккредитацию на электронной площадке, правил документооборота при проведении электронного аукциона, разглашение оператором электронной площадки, должностным лицом оператора электронной площадки информации об участнике закупки до подведения результатов электронного аукциона (ст. 7.31.1 КоАП РФ).

Таким образом, меры по охране указанной информации, а также круг субъектов не подпадают под условия правового режима служебной тайны.

Еще одним спорным моментом в определении категорий сведений, которые могут быть включены в сведения, охраняемые в режиме служебной тайны, является тайна следствия. На наш взгляд, тайна следствия сама по себе гораздо шире чем понятие служебной тайны. Во-первых, потому, что субъектами, обязанными хранить тайну следствия (данные предварительного расследования) являются помимо органов, проводящих расследования, также лица, участвующие в уголовном судопроизводстве, которые не связаны с договорными либо служебными отношениями с соответствующими органами. Кроме того, за разглашение указанной информации предусмотрен отдельный вид уголовной ответственности для лиц, которые не являются сотрудниками соответствующих органов, проводящих расследование – ст. 310 УК РФ.

Вместе с тем, следуя концепции, в соответствии с которой правовой режим и сведения представляют собой различные категории, можно говорить о том, что сами по себе данные предварительного расследования могут составлять служебную тайну в рамках органов, производящих расследование, в то время как такая информация, ставшая известной иным участникам уголовного судопроизводства, будет попадать уже под иной правовой режим защиты информации. Однако в этом случае считаем такое разделение правового режима искусственным и необоснованным, поскольку он будет предполагать различное регулирование указанной информации. Также данные предварительного расследования отличает от иной информации ограниченного доступа достаточно серьезный перечень исключений для разглашения такой информации, что не позволит в достаточной мере интегрировать указанные данные в общий массив информации, защищаемый в режиме служебной тайны.

Таким образом, на основе представленного анализа, можно сделать вывод о существенном сходстве правового регулирования многих видов информации, содержащейся в органах г.в. и м.с.у., а также публичных акционерных обществ, корпораций, иных организаций, создаваемых Российской Федерацией на основании федерального закона, организаций, создаваемых для выполнения задач, поставленных перед федеральными государственными органами. Так, в частности, есть сходство в регулировании порядка работы с информацией, особенно если обработка такой информации осуществляется в государственных информационных системах. Так или иначе, все информационные системы в органах г.в. и м.с.у. должны отвечать техническим требованиям ФСТЭК, утвержденным Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Далее – Приказ ФСТЭК №17)

Также сходен состав мер ответственности, предусмотренных за разглашение информации ограниченного доступа, который приведен ранее.

Вместе с тем, стоит отметить, что лишь в отношении первичных статистических данных, а также данных о переписи населения, объектах сельскохозяйственной переписи предусмотрена ответственность не только за разглашение информации, но также за утрату, фальсификацию, содействие фальсификации указанных сведений. Полагаем, что ответственность за такой перечень действий более полно отвечает целям охраны информации ограниченного доступа и должна применяться в отношении всей информации, которая может охраняться в режиме служебной тайны.

Исходя из изложенного, можно сделать вывод о возможной защите в режиме служебной тайны, по крайней мере, 20 видов сведений ограниченного доступа, предусмотренных в указанной таблице. Вместе с тем, стоит отметить, что при принятии решения об объединении различных видов информации ограниченного доступа, необходимо детально проанализировать технические и организационные меры защиты информации. В рамках настоящего исследования это не представляется возможным.

Важным моментом обеспечения эффективности и законности ограничения доступа к информации является установление надзора за деятельностью в сфере ограничения доступа к информации государственными органами, которая должна быть подотчетна. В настоящее время, как правило, к перечням информации, а также к служебной тайне государственного органа доступ является закрытым, проверка на соответствие указанных сведений законодательству отсутствует. Справедливо будет отметить, что в настоящее время отсутствуют условия и правила ограничения доступа к информации в режиме служебной тайны, на соответствие которым можно было бы проверять защищаемую в режиме служебной тайны информацию. Вместе с тем, в состав основных разделов данной классификации необходимо включать сведения об информационной и физической безопасности, информацию о непосредственной деятельности, связанной с реализацией властных полномочий, сведения в области геодезии, картографии и проектировании, информацию о научно-технических разработках, сведения об

административно-хозяйственной деятельности, а также информацию, составляющую тайну третьих лиц. Такая категория как «сведения об административно-хозяйственной деятельности» нуждаются в существенной законодательной проработке, не должны быть открытыми и должны соответствовать требованиям законодательства об обеспечении информации о деятельности органов г.в. и м.с.у..

Следует также отметить, что проведенный анализ позволяет говорить о возможности объединения многих видов информации ограниченного доступа в режиме служебной тайны.

2.3 Субъекты правоотношений, возникающих в сфере охраны и оборота сведений, охраняемых в режиме служебной тайны.

Субъектный состав отношений в сфере оборота служебной тайны является еще одним малоизученным вопросом. В литературе, как правило, этому вопросу уделяется недостаточное внимание. Как правило, когда рассматривают субъекты служебной тайны, речь идет об ответственности государственных служащих за разглашение информации, либо о полномочиях должностных лиц, которые имеют право относить информацию к сведениям, охраняемым в режиме служебной тайны. В то же время, круг субъектов отношений достаточно разнообразен и разнороден.

Служебную тайну можно рассматривать как с позиции информационного права, так и с позиций права административного. В теории информационного права, как правило, субъекты подразделяются на производителя, обладателя и потребителя информации¹.

¹ Копылов, В. А. Информационное право / В. А. Копылов. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – 512 с.

У. М. Станскова¹ высказывает позицию, в соответствии с которой в рамках трудовых отношений субъектами информационных правонарушений может стать как работник, виновный в неисполнении или в ненадлежащем исполнении обязанностей по охране информации ограниченного доступа, так и работодатель, не принявший надлежащих мер для охраны конфиденциальной информации. Кроме того, субъектами в данном случае могут выступать и третьи лица – участники иных непосредственно связанных с трудовыми отношений, которые нарушили требования по обеспечению конфиденциальности. На наш взгляд, допустимо применить аналогию такой модели субъектного состава отчасти и к отношениям в области гражданской службы.

В то же время, под субъектом административного права понимаются «физические или юридические лица, которые в соответствии с установленными административным законодательством нормами участвуют в осуществлении публичного управления, реализации функций исполнительной власти»². Субъект в понимании административного права это «одна из сторон публичной управленческой деятельности, участник управленческих отношений, наделенный законодательством правами, обязанностями, полномочиями, компетенцией, ответственностью, способностью вступать в административно-правовые отношения»³. В таком случае, речь, как правило, идет именно о публичных субъектах правоотношений.

О. А. Ястребов приводит следующую классификацию публичных субъектов:

1. Органы исполнительной власти.
2. Государственные учреждения.
3. Государственные корпорации.

¹ Станскова, У. М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореф. дис. ... канд. юрид. наук: 12.00.05 / У. М. Станскова. – Екатеринбург, 2014. – 22с.

² Бахрах, Д. Н. Административное право России. Учебник для Вузов. / Д. Н. Бахрах. – М.: Издательство «Норма». – 2000. – С. 123.

³ Там же. С. 124

4. Государственные унитарные предприятия¹.

В данном случае она представляет для нас особый интерес, поскольку является более широкой, чем традиционная классификация, и включает в себя, в том числе, и такие субъекты как государственные корпорации. Другие же субъекты не могут отвечать основным требованиям самостоятельного отнесения информации к сведениям, охраняемым в режиме служебной тайны, поскольку не наделены в полной мере государственно-властными полномочиями.

В то время как государственные корпорации, юридический статус которых до сих пор в науке права и правового регулирования до конца не определен и часто отмечается схожесть его со статусом органа государственной власти, вполне может быть субъектом отношений в сфере служебной тайны².

К примеру, такая государственная корпорация как «Росатом» является, пожалуй, одним из наиболее крупных субъектов отношений, возникающих как в сфере служебной, так и в сфере государственной тайны. Так, в соответствии с п. 11 ст. 27 Федерального закона от 01.12.2007 № 317-ФЗ «О государственной корпорации по атомной энергии «Росатом», указанная корпорация наделяется полномочиями по отнесению сведений к государственной тайне и утверждает перечень сведений, подлежащих засекречиванию в соответствии с законодательством Российской Федерации. Кроме того, Росатом обладает достаточно серьезной системой защиты не только государственной, но и служебной тайны. Об этом свидетельствует ряд нормативных актов, изданных непосредственно Росатомом. К примеру, в корпорации действует достаточно обширная информационная система,

¹ Ястребов, О. А. Публичные субъекты административного права. Учебное пособие / О. А. Ястребов. – М.: РУДН, 2009. – 144 с.

² Подробнее о статусе госкорпорации см.: там же; Каплин, С. Ю. Государственная корпорация как субъект права: монография / Каплин С. Ю.; Науч. ред Павлушина А. А. – Самара: Инсома-пресс, 2011. – 98 с.

получение доступа к которой фактически означает доступ к служебной тайне¹. Наличие такой системы служебной тайны в государственной корпорации, которая тесно и непосредственно связана с тайной государственной, охраняемой в госкорпорации, свидетельствует о необходимости распространения регулирования служебной тайны также и на такие квазипубличные органы как госкорпорации, фонды (Фонд обязательного медицинского страхования, Пенсионный фонд, Фонд социального страхования).

Обратимся к вопросу о том, какие субъекты служебной тайны указаны непосредственно в нормативных актах.

При этом при обсуждении Проекта закона о служебной тайне, а также в литературе (как отмечалось ранее) неоднократно возникал вопрос относительно круга субъектов, на которые будут распространяться требования о защите служебной тайны. При этом стоит различать субъектов, в которых может образоваться информация ограниченного доступа, и субъектов, которым такая информация может передаваться. Немаловажным аспектом является и вопрос наделения должностных лиц полномочиями установления ограничения доступа к информации в режиме служебной тайны.

Исходя из того, что служебная и государственная тайна являются смежными институтами, исследуем субъектный состав в законе о государственной тайне.

Так в законе о государственной тайне предусмотрен достаточно широкий круг субъектов, на которых может быть возложена обязанность по

¹ О предоставлении доступа пользователей к информационному фонду и сервисам центрального узла информационно-коммуникационной системы Росатома: Приказ Росатома от 17.12.2007 № 651.

Об организации доступа пользователей к информационному фонду и сервисам центрального узла информационно-коммуникационной системы Росатома (вместе с «Порядком подключения пользователей к системе электронного документооборота Росатома», «Инструкцией по обеспечению информационной безопасности при организации доступа пользователей к информационным ресурсам и сервисам центрального узла информационно-коммуникационной системы Росатома»): Приказ Росатома от 22.10.2007 № 544.

защите государственной тайны. Он прямо не обозначен, но исходя из смысла норм, можно сделать вывод, что субъектами, на которые может быть возложена обязанность по защите государственной тайны, могут быть органы государственной власти, органы местного самоуправления, учреждения и организации, должностные лица и граждане, имеющие доступ к государственной тайне и осуществляющие работу с указанными сведениями. Вместе с тем, право на разработку развернутых перечней сведений, подлежащих засекречиванию, предоставлено только должностным лицам (руководителям) федеральных органов государственной власти и некоторых квазипубличных образований (корпорация «Росатом», «Роскосмос», Банк России и т. д.). Перечень этих должностных лиц строго ограничен и указан в Распоряжении Президента РФ от 16.04.2005 № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».

На наш взгляд, аналогичная модель регулирования ограничения доступа к информации, охраняемой в режиме служебной тайны, могла быть вполне приемлемой. Вместе с тем, считаем, что перечень должностных лиц, которым предоставляется право ограничивать доступа к информации в режиме служебной тайны, мог бы быть несколько шире: так, в частности, к указанной группе могли бы быть добавлены руководители ФСС, ПФР и ФОМС.

Стоит отметить одну очень важную деталь: в законе о государственной тайне не предусматривается возможность наличия «самостоятельных» сведений, составляющих в органах судебной власти государственную тайну вне рамок материалов дел, рассматриваемых в судах. Вместе с тем полагаем, что в органах судебной власти существует потребность в ограничении доступа к некоторой информации в режиме служебной тайны. Об этом, в частности, свидетельствуют инструкции по делопроизводству, утвержденные Верховным Судом Российской Федерации, в которых присутствуют указания

на запрет на разглашения сведений, содержащихся в служебных документах¹. Например, те же сведения об обеспечении информационной безопасности суда могут также относиться к служебной тайне. Таким образом, полагаем, что круг субъектов, которым может быть предоставлено право на установление перечней информации, доступ к которой может быть ограничен в режиме служебной тайны, будет шире по сравнению с составом субъектов государственной тайны.

Еще одним нерешенным вопросом остается возможность ограничения доступа к информации органами местного самоуправления. На наш взгляд, в органах местного самоуправления также может образовываться информация, охраняемая в режиме служебной тайны, однако предоставление права устанавливать самостоятельно категории сведений, доступ к которым ограничивается, может привести к отсутствию единообразия регулирования. Вместе с тем, полагаем, что можно было бы предоставить право определять перечни сведений, относимых к служебной тайне, должностным лицам субъектов, что позволило бы достичь определенного баланса интересов при формировании таких перечней, позволив с большей оперативностью принимать решения об ограничении доступа к той или иной информации, но обеспечив единообразие и прозрачность ограничения доступа к информации в рамках одного субъекта.

В Указе Президента РФ №188 в отношении режима служебной тайны речь идет о таком субъекте как государственные органы. В постановлении Правительства РФ № 1233 также субъектом являются государственные органы, но такой вывод можно сделать только исходя из контекстного толкования определения «служебной тайны», которое дается в этом постановлении.

Вместе с тем, нельзя не отметить, что в институте государственной тайны государственным органам отдается первостепенное значение, которое

¹ Об утверждении Инструкции по судебному делопроизводству в районном суде: приказ Судебного департамента при Верховном Суде РФ от 29.04.2003 № 36.

предопределяется также и тем, что полномочия по утверждению перечней сведений, охраняющихся в режиме государственной тайны, предоставлены должностным лицам государственных органов или квазипубличных образований.

Следует учесть, что аналогичное понимание субъектов по охране служебной тайны является доминирующим в законодательстве и в различных ведомственных актах, однако не единственным. Так, Федеральный закон «О страховании вкладов физических лиц в банках Российской Федерации» от 23.12.2003 № 177-ФЗ содержит положение в ст. 31, согласно которому «Агентство вправе получать информацию, составляющую служебную, коммерческую и банковскую тайну банка, в отношении которого наступил страховой случай»¹. Концепция указанного нормативного акта предполагают существование служебной тайны не только в органах власти, но и в коммерческих банках в данном случае. Кроме того, аналогичная позиция существует в Федеральный Закон «О рекламе». В ст. 34 указанного закона содержится положение о том, что «Юридические лица, индивидуальные предприниматели обязаны представлять в антимонопольный орган (его должностным лицам) по его мотивированному требованию в установленный срок необходимые документы, материалы, объяснения, информацию в письменной и (или) устной форме (в том числе информацию, составляющую коммерческую, служебную и иную охраняемую законом тайну)»². Опять в данном случае очевидно, что законодатель допускает возможность наличия служебной тайны у юридических лиц.

Полагаем, что такое противоречивое понимание в законодательстве понятия «служебная тайна» связано с позицией, ранее закреплявшейся в ст. 139 ГК РФ. Статья утратила силу 1 января 2008 года, но во весь массив нормативных актов соответствующие изменения внесены так и не были.

¹ О страховании вкладов физических лиц в банках Российской Федерации: федер. закон от 23.12.2003 № 177-ФЗ (ред. от 29.07.2017).

² О рекламе: федер. закон от 13.03.2006 № 38-ФЗ (ред. от 29.07.2017).

Из-за этого и сложилось до сих пор распространенное мнение о том, что режим служебной тайны может устанавливаться также в негосударственных организациях.

На данный момент, по нашему мнению, субъектами отношений по обороту и охране сведений, охраняемых в режиме служебной тайны, являются государственные органы и должностные лица, и нет оснований полагать, что служебная тайна может образовываться в негосударственных организациях за исключением тех, которые исполняют роль квазипубличных органов либо осуществляют работы на основании государственных контрактов.

Необходимо понимать, для чего нужно четко обозначать тот круг субъектов, которые участвуют в процессе производства и оборота информации, охраняемой в режиме служебной тайны.

Прежде всего, определение субъектного состава необходимо для решения вопроса о круге лиц, уполномоченных относить информацию к сведениям, охраняемым в режиме служебной тайны. Заметим, что это очень важный вопрос для определения законности введения режима служебной тайны в том либо ином государственном органе, учреждении, предприятии.

Еще одним немаловажным вопросом является вопрос об определении тех лиц, на которых распространяются обязанности и требования охраны информации, охраняемой в режиме служебной тайны. Именно от решения этого вопроса напрямую зависит и разрешение вопроса о возможности либо невозможности применения мер ответственности за нарушения требований правового режима служебной тайны. Следует особо отметить, что мы осознанно не говорим о разглашении служебной тайны в данном случае, поскольку считаем, что круг правонарушений в сфере соблюдения режима служебной тайны значительно шире, чем только разглашение соответствующей информации.

При этом классификация субъектов может происходить по различным основаниям.

Первым классификационным основанием можно назвать функциональный признак – какую функциональную роль в правоотношениях, возникающих в сфере охраны служебной тайны, играет тот либо иной субъект:

1. Субъекты, уполномоченные устанавливать правила оборота и основания отнесения информации к категории служебной тайны. Пожалуй, самая малочисленная категория субъектов, но наиболее важная. Поскольку, в соответствии с Законом об информации, ограничения доступа к информации могут устанавливаться только на основании Федеральных законов, соответственно, такими субъектами являются именно органы законодательной власти федерального уровня.

2. Субъекты, уполномоченные устанавливать конкретный перечень категорий сведений, доступ к которым может быть ограничен. В данном случае мы особо выделяем эту категорию субъектов, поскольку считаем, что служебная тайна как таковая должна представлять собой стройную систему в каждом конкретном государственном органе и его подразделениях. Именно поэтому, перечень конкретных сведений, которые могут охраняться в режиме служебной тайны, должны определяться относительно всех подведомственных органов непосредственно на уровне министерства. Только такая системность позволит избежать злоупотреблений в сфере ограничения доступа к информации и обеспечит унификацию системы информации.

3. Субъекты, которые уполномочены относить ту или иную информацию к сведениям, охраняемым в режиме служебной тайны. К ним, как правило, относятся руководители государственных органов или структурных подразделений. Именно они принимают решение и должны нести ответственность за правомерность и обоснованность отнесения либо не отнесения той или иной информации к сведениям, охраняемым в режиме служебной тайны. Как правило, эти же субъекты уполномочены допускать государственных/муниципальных служащих до работы с определенными сведениями, охраняемыми в режиме служебной тайны, и уполномочены

принимать решение о передаче сведений иным государственным органам или должностным лицам.

4. Субъекты, обеспечивающие соблюдение режима охраны информации, охраняемой в режиме служебной тайны. Как правило, субъектом, который обеспечивает оборот бумажных носителей, содержащих сведения, охраняемых в режиме служебной тайны, является служба делопроизводства о.г.в. или м.с.у., либо служба безопасности о.г.в., которая, помимо прочего, занимается и обеспечением безопасности электронного оборота документов.

5. Субъекты, осуществляющие работу с документами, охраняемыми в режиме служебной тайны. Это одна из наиболее многочисленных категорий субъектов. К ним относятся те государственные и муниципальные лица, которые напрямую работают с указанной информацией и несут ответственность за ее разглашение.

Данная классификация позволит в дальнейшем гораздо подробнее рассмотреть меры ответственности относительно каждой из категорий субъектов отношений, возникающих в сфере производства, охраны и оборота сведений, охраняемых в режиме служебной тайны. Следует отметить, что ответственность и меры контроля должны быть предприняты для всех субъектов-участников отношений в сфере оборота служебной тайны.

В настоящее время нельзя выявить иную классификацию с классификационным основанием субъектов «от обратного» – то есть по мерам применимой ответственности. Данное основание является недостаточно разработанным в силу слабого регламентирования ответственности за разглашение служебной тайны на законодательном уровне. Проблемы ответственности мы рассмотрим в пятом параграфе данной главы. Сейчас же стоит отметить, что, несмотря на установление во многих подзаконных актах ответственности за разглашение информации, охраняемой в режиме служебной тайны, такую как уголовную, административную, дисциплинарную и иную, на практике же применение иной ответственности,

кроме как дисциплинарной, встречается крайне редко. Именно поэтому классифицировать субъектов по мерам ответственности крайне сложно.

Еще одной классификацией, которая встречается в литературе, является классификация по признаку организационной формы субъекта служебной тайны.

Как отмечает Г. Г. Камалова, условно субъектов служебной тайны можно разделить на четыре категории:

1. «органы государственной власти;
2. органы местного самоуправления;
3. государственные корпорации;
4. подведомственные организации, осуществляющие государственные функции и оказывающие государственные услуги»¹.

В то же время, на наш взгляд, даже такая классификация субъектов недостаточно отражает многообразие состава участников возникающих правоотношений.

Существуют организации, которые, являясь коммерческими, все же оказывают услуги/ведут работы в рамках осуществления своих обязанностей по государственному либо муниципальному контракту. В этом случае государственные органы также могут передавать информацию, составляющую государственную либо служебную тайну таким организациям. При этом, если в случае предоставления государственной тайны таким организациям существуют нормативные предписания и определенные технические требования, которым должна отвечать система охраны информации на конкретном предприятии, то выятные требования к обороту и охране служебной тайны на нормативном уровне отсутствует. В дальнейшем мы будем рассматривать систему технологических требований к обороту сведений, однако такие требования не являются обязательными для

¹ Камалова, Г. Г. О субъектах правоотношений в области защиты служебной тайны / Г. Г. Камалова // колл. монография / под общ.ред. И. Л. Бачило. – М.: Издательство Юрайт, 2009. – 530 с.

организаций, которым доверяются те или иные сведения, охраняемые в режиме служебной тайны, такие требования могут предъявляться, однако, теми государственными и муниципальными органами, которые предоставляют информацию, охраняемую в режиме служебной тайны.

В то же время нигде, даже на подзаконном уровне, не встречается упоминание организаций, которым, в качестве субъектов служебной тайны, государственными или муниципальными органами предоставляется информация, охраняемая в режиме служебной тайны.

Следует также отметить, что в отзывах на Проект Закона о служебной тайне были отражены такие вопросы, как возможность отнесения органов местного самоуправления к кругу субъектов отношений в сфере служебной тайны. На наш взгляд, органы местного самоуправления также могут аккумулировать информацию, доступ к которой необходимо ограничивать. Так, к примеру, к такой информации могут относиться сведения о системах жизнеобеспечения; сведения о физической и информационной безопасности органа местного самоуправления. Кроме того, так или иначе, органы местного самоуправления также накапливают информацию, составляющую «чужую» тайну.

На основании изложенного, приходим к выводу о том, что круг субъектов отношений в сфере охраны служебной тайны выходит за пределы двоичной системы «государственный орган – государственный служащий».

Считаем возможным выделять также следующие категории субъектов служебной тайны в зависимости от того, на каком основании они работают с информацией:

1. Субъекты, которые получают доступ к служебной тайне в силу закона.
2. Субъекты, которые получают доступ к служебной тайне в силу договора.

На наш взгляд, нормативное определение круга субъектов, а также их статуса, необходимо для совершенствования механизмов защиты информации, охраняемой в режиме служебной тайны.

2.4. Меры защиты информации в режиме служебной тайны

Обеспечение охраны информации, охраняемой в режиме служебной тайны, является одним из необходимых требований для обеспечения информационной безопасности в целом. Как отмечала профессор И. Л. Бачило, обеспечение информационной безопасности – самый важный вопрос, решение которого происходит во многом на уровне инфраструктуры¹. При этом информация должна быть защищена как от внутренних, так и от внешних угроз. Ю. И. Коваленко выделяет два вида угроз:

1. Несанкционированный доступ.
2. Санкционированный доступ.²

В случае санкционированного доступа, доступ к информации происходит уполномоченным лицом, но с противоправными целями (нарушение целостности, изменение и (или) разглашение информации).

Именно обеспечение защиты информации, охраняемой в режиме служебной тайны, и является содержанием самого правового режима служебной тайны. Вместе с тем, содержание правового режима служебной тайны составляют те методы правового регулирования, которые опосредуют порядок оборота информации, охраняемой в режиме служебной тайны. Под методом правового регулирования понимаются определенные приемы,

¹ Бачило, И. Л. Правовые проблемы развития информационного общества // Информационное право: актуальные проблемы теории и практики: сб. докладов науч.-практ. Конференции, Москва, 3.04.2015 / ред. совет: Ю. Л. Васильченко, И. М. Рассолов, С. Г. Чубукова. – М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2015. – С. 6-14.

² Коваленко, Ю. И. Организационно-правовое обеспечение информационной безопасности: Учебно-методическое пособие / Ю. И. Коваленко. – М.: МИНИТ ФСБ России, 2003. – С. 41.

способы, средства воздействия права на общественные отношения, к которым относятся различные стимулы, запреты и ограничения. В регулировании института служебной тайны превалирует императивный метод правового регулирования, основанный во многом на различных запретах и ограничениях, вводимых в отношении охраняемых сведений. Причем запреты и ограничения в данном случае существуют как на организационном, так и на технологическом уровнях.

Для нас представляет интерес вопрос регулирования защиты информации, передающейся в рамках международного межправительственного обмена.

Регулированию международного межправительственного обмена информации ограниченного доступа посвящены ряд соглашений, которые вводят условную классификацию степеней секретности без регулирования подробного порядка обращения с такой информацией, либо регламентируют возложение обязанностей на службы специальной связи¹ без указания классификации информации и разграничения степени доступа и защиты передаваемых сведений.

Так, например, на уровне стран Большой восьмерки принят протокол TLP², который унифицирует на международном уровне степени доступности передаваемой информации и вводит четыре степени доступности информации в зависимости от того, каким цветом³ она обозначена:

¹ Соглашение о сотрудничестве в межгосударственном обмене отправлениями специальной связи (Ашхабад, 23.12.1993 года) с изменениями, внесенными Протоколом от 16.03.01г. – (http://base.spinform.ru/show_doc.fwx?rgn=4685). – Дата обращения 17.12.2017; Положение о межгосударственном обмене отправлениями специальной связи. Утверждено Соглашением Совета глав правительств Содружества Независимых Государств о межгосударственном обмене отправлениями специальной связи от 23.12.1993 года. (ред. от 15.03.2001). – (https://base.spinform.ru/show_doc.fwx?rgn=4686). – Дата обращения: 17.12.2017.

² CPNI information exchange membership guidelines. – (<http://webarchive.nationalarchives.gov.uk/20100815133302/http://www.cpn.gov.uk/Docs/ie-membership-guidelines.pdf>). – Дата обращения: 17.12.2017.

³ TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance – Version 1.0. – (<https://www.us-cert.gov/sites/default/files/tlp/tlp-v1.pdf>). – Дата обращения: 17.12.2017.

1. Красным обозначается строго конфиденциальная информация, предназначенная только для конечного получателя. Как правило, информация должна быть доступна только участникам встречи или заседания. В большинстве случаев информация передается лично.

2. Желтым обозначается информация ограниченного распространения. Получатель может поделиться такой информацией только в рамках своей организации, при условии, что это необходимо. Автор конкретной информации может установить пределы, в которых разрешается ею делиться.

3. Зеленым обозначается информация широкого распространения. Информация этой категории может быть широко распространена в пределах определенного сообщества. Тем не менее, информация не может быть опубликована в СМИ, Интернете или где бы то ни было за пределами сообщества.

4. Белым обозначается информация для неограниченного распространения, которая может распространяться свободно, но не должна нарушать авторские права.

В то же время, данный протокол не регламентирует порядок передачи, обработки и хранения такой информации, что в свою очередь не создает полноценного механизма обращения информации ограниченного доступа. Кроме того, отсутствует какая-либо ответственность договаривающихся организаций в случае разглашения той или иной информации.

Как правило, при международном межправительственном обмене, для разрешения вопросов охраны секретной информации заключается соглашение между обменивающимися странами, в котором сопоставляются используемые в странах грифы секретности и меры, применяемые к их защите. Так, к примеру, в соглашении между Правительством Российской Федерации и Кабинетом Министров Украины о взаимной охране секретной информации (Заключено в г. Москве 02.12.2000) описаны не только грифы секретности, но также меры защиты информации и порядок привлечения к ответственности виновных за разглашение секретной информации лиц. Такое регулирование

наилучшим образом отвечает требованиям организации оборота информации ограниченного доступа, однако, вместе с тем, стоит отметить, что в указанных документах отсутствует как таковое регулирование служебной информации, к которой, в том числе, относится и дипломатическая переписка, а также информация, образующаяся в результате межправительственного взаимодействия различных стран.

В связи с этим особый интерес представляет документ, который регулирует охрану служебной тайны в такой межправительственной организации как Евразийская экономическая комиссия¹. Пожалуй, это один из редких примеров нормативных актов такого уровня, который посвящен непосредственно подробному регулированию обращения с информацией ограниченного доступа. Следует отметить логичность и системность построения нормативного акта, в котором подробно определена терминологическая база, которая используется при охране информации ограниченного доступа². Также в нормативном акте приведен примерный перечень сведений, которые могут быть отнесены к служебной тайне (информации для служебного пользования). Перечень все же не является закрытым, что предоставляет возможность регулировать степень ограничения доступа к определенной информации. При этом можно сказать, что перечень выполняет больше не функцию недопущения злоупотребления правом на ограничение доступа к информации, а определяет ту информацию, доступ к которой должен быть ограничен в любом случае.

¹ О Порядке работы с документами ограниченного распространения (конфиденциальными и для служебного пользования) в Евразийской экономической комиссии: решение Совета Евразийской экономической комиссии от 18.09.2014 № 71.

² Все же стоит отметить, что, несмотря на стройность и логичность используемого понятийно-категориального аппарата, указанный акт во многом не согласуется с терминологией, используемой не только в национальных законодательствах некоторых стран, но и в рамочных законах СНГ. Само по себе терминологическое расхождение не может породить серьезных практических проблем из-за различия в сферах применения, однако унификация понятийно-категориального аппарата в рамках одной наднациональной правовой системы хотя бы с теоретической точки зрения должна присутствовать.

При изучении механизмов защиты информации, охраняемой в режиме служебной тайны, мы будем опираться на те нормативные акты, которые регулируют обращение с информацией ограниченного доступа в органах государственной власти. «Информация ограниченного доступа в органах государственной власти» – это категория куда более широкая, чем понятие «служебная тайна», особенно если рассматривается она в рамках технологической защиты информации. Как правило, во внутренних и ведомственных приказах под «информацией ограниченного доступа», обозначенной грифом «ДСП», подразумевается та информация, которая охватывается понятием «служебная тайна». Как правило, исключениями в этом случае является профессиональная тайна, которая также может охраняться под общим обозначением «информация ограниченного доступа» в правоохранительных органах (к примеру, тайна следствия). Стоит все же отметить, что ввиду неопределенности понятийно-категориального аппарата, под «информацией ограниченного доступа» понимают часто весь массив конфиденциальной информации, охрана которой прописана в законодательстве либо ее охрана вызвана служебной необходимостью.

В любом случае, используется, как правило, одна система информационной безопасности.

Для обеспечения информационной безопасности применяется ряд мер, к которым можно отнести меры организационного и меры технологического характера. Некоторые исследователи говорят также о мерах ответственности как об одном из механизмов защиты и охраны информации¹. К организационным мерам можно отнести меры «индивидуального» и общего характера. К организационным мерам индивидуального характера можно отнести порядок закрепления обязанности сохранения служебной тайны в

¹ Швецов, А. В. Защита информации в сфере служебной тайны в деятельности ОВД: Правовой аспект: дисс... канд.юрид. наук. 05.13.19 / А. В. Швецов. – Воронеж, 2005. – 189с.;

Дворников, А. А. Уголовно-правовая охрана государственной и служебной тайны в органах внутренних дел: автореф. дис.... канд. юрид. наук / А. А. Дворников. – Тюмень, 2007. – 22с.

трудовом договоре/контракте с государственным служащим¹. К организационным мерам общего характера можно отнести установление порядка работы со сведениями, охраняемыми в режиме служебной тайны. К мерам технологического характера относятся те меры, которые применяются в отношении информационных систем государственного органа, содержащих сведения, охраняемые в режиме служебной тайны. К ним, в частности, относятся требования, предъявляемые при сертификации и аттестации рабочих мест, а также требования, предъявляемые к оборудованию и программному обеспечению, позволяющему охранять сведения от несанкционированного доступа, изменения и уничтожения.

Меры ответственности, на наш взгляд, нельзя полностью отнести к мерам охраны сведений, так как ответственность наступает именно вследствие нарушения требований и правил работы с информацией и носит превентивный характер лишь отчасти. О мерах ответственности подробнее поговорим в параграфе 5 настоящей главы.

Начнем с анализа организационных мер общего характера. Эти меры содержатся во многих ведомственных нормативных актах. Стоит отметить тенденцию повышения прозрачности при принятии таких актов, поскольку ранее такие акты принимались и обозначались пометкой «ДСП», открытый доступ к ним не был возможен.

В 2014 и в 2015 годах приняты новые ведомственные акты, которые регулируют порядок обращения с информацией ограниченного доступа и распространения. Интересно рассмотреть указанные нормативные акты с точки зрения развития нормативного понимания института служебной тайны. Так, к примеру, Приказ Росалкогольрегулирования от 29.01.2015 № 20 «Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральной службе по регулированию алкогольного

¹ Изучение данной проблемы представлено в работе Стансковой, У. М. Трудовые средства обеспечения конфиденциальности информации ограниченного доступа: автореф. дис. ... канд. юрид. наук: 12.00.05 / У. М. Станскова. – Екатеринбург, 2014. – 22 с.

рынка»¹ описывает порядок передачи служебной информации ограниченного распространения другим государственным органам власти и организациям, порядок снятия пометки «для служебного пользования» с носителей информации ограниченного распространения, организацию защиты служебной информации ограниченного распространения. Также определяет категории должностных лиц центрального аппарата Росалкогольрегулирования и его территориальных органов, уполномоченных относить служебную информацию к разряду ограниченного распространения. Это положение по своей структуре и по своему содержанию во многом повторяет другие аналогичные положения различных государственных органов.

Это положение по своей структуре и по своему содержанию во многом повторяет другие аналогичные положения различных государственных органов. Вместе с тем, сложно не заметить, что указанное положение не обладает полнотой регулирования заявленных отношений, не описывает в достаточной мере эффективный механизм охраны информации и хотя бы минимальной системы сдержек и противовесов в вопросе раскрытия информации и снятия/пересмотра грифа. Так указанное положение регламентирует порядок снятия грифа «ДСП», однако не предусматривает возможности инициировать проведение проверки и снятия грифа «ДСП» каким-либо лицом, также не предусмотрены принципы и порядок формирования экспертных комиссий, в полномочия которых входит снятие грифа с документов. Также положением не предусмотрен порядок проставления пометки «ДСП» на документах уполномоченными должностными лицами.

¹ Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральной службе по регулированию алкогольного рынка» (вместе с «Порядком передачи служебной информации ограниченного распространения другим государственным органам власти и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения»): приказ Росалкогольрегулирования от 29.01.2015 № 20.

Правила, устанавливаемые в таких внутренних актах, могут противоречить законодательству, а также ущемлять права и законные интересы граждан. Кроме того, оспаривание таких актов представляется крайне затруднительным по причине отсутствия доступа к этим актам, а также по причине отсутствия эффективного механизма оспаривания таких документов. Кроме того, как показывает практика, в абсолютном большинстве случаев суды отказывают в исках о снятии с документов грифа «ДСП» или признании норм, содержащихся в документе, незаконными.

Если мы обратимся к прописанному механизму защиты данных документов, обозначенных пометкой «ДСП», то обнаружим, что и он не является в полной мере эффективным и самодостаточным для обеспечения безопасности информации. Так, к примеру, указанный документ содержит следующее положение: «Выданные из архива гражданским служащим для работы дела с пометкой «ДСП» подлежат возврату в тот же день». Также содержится положение о том, что копирование таких документов без соответствующего разрешения запрещено. Однако возникает резонный вопрос, каким образом обеспечивается соблюдение указанной нормы, если в данном пункте отсутствует какое-либо указание на то, в каком режиме ведется работа с указанным документом, допускается ли вынос указанных документов работником из организации, каким образом обеспечивается его сохранность. Отдельные нарекания вызывает терминология нормы: обозначая выдаваемые работникам документы как «дела с пометкой «ДСП», указанный государственный орган сужает значение термина и ответственность гражданского служащего только до сохранения фактически определенной папки с указанным грифом, а не всей документации, содержащей соответствующий гриф в целом.

В положении присутствует указание на то, что документы могут быть переданы другим государственным органам и организациям. Когда речь идет об организациях, невозможно определить, идет ли речь исключительно о государственных организациях. В случае, если указанная норма не

ограничивает круг получателей только государственными органами и государственными организациями, возникает вопрос о том, каким образом в организации-получателе будет соблюдаться режим информации ограниченного доступа, и должен ли соблюдаться такой режим вообще?

В 2014 году был принят документ, повторяющий по большей части рассматриваемый Приказ Росалкогольрегулирования: Приказ Росрыболовства от 11.12.2014 № 986 «Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральном агентстве по рыболовству и его территориальных органах»¹. Он также не отвечает на поставленные ранее вопросы, имеет аналогичные проблемы в механизме правового регулирования.

Одним из наиболее подробных документов, регулирующих порядок обращения с документами, относящихся к категории информация «Для служебного пользования», является Приказ Минрегиона России от 20.05.2014 № 148 «Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве регионального развития Российской Федерации и его территориальных органах»². В этом документе прописан особый порядок допуска к работе со служебной информацией – решение руководителя структурного подразделения. В других приказах допуск, как правило, отдельно не оформляется и чаще всего работа с такими документами предусмотрена должностными регламентами. Таким образом, ответственность служащих, допущенных к работе с документами «ДСП»

¹ Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральном агентстве по рыболовству и его территориальных органах» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения»): Приказ Росрыболовства от 11.12.2014 № 986.

² «Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве регионального развития Российской Федерации и его территориальных органах» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения», «Порядком организации защиты служебной информации ограниченного распространения»): Приказ Минрегиона России от 20.05.2014 № 148.

персонализируется, а не «размывается», как в других приказах. Кроме того, в пункте 13 выше обозначенного приказа подробно описан порядок создания документов для служебного пользования: «Создание документов, относящихся к служебной информации ограниченного распространения, в структурных подразделениях Минрегиона России осуществляется на специально выделенном автоматизированном рабочем месте с закрытым доступом в общую информационную систему Минрегиона России, определенном решением руководителя структурного подразделения Минрегиона России». Такое указание на техническое обеспечение создания документов ограниченного доступа значительно повышает степень защиты информации ограниченного доступа. Кроме того, в приказе устанавливается порядок действия должностных лиц в случае получения информации об утере документов.

Как видим, порядок охраны сведений, защищаемых в режиме служебной тайны, в различных нормативных правовых актах не унифицирован. В то же время, стоит отметить, что в Проекте Закона о служебной тайне предусматривались базовые требования к охране сведений, охраняемых в режиме служебной тайны, порядку допуска к этим сведениям государственных служащих, граждан и передачи их в рамках межведомственного взаимодействия, а также иным организациям в рамках исполнения обязательств по государственному/муниципальному контракту.

Считаем, что на федеральном уровне необходима хотя бы минимальная унификация правил работы с такой информацией. Так, к примеру, Т. М. Занина предлагает вводить систему защиты служебной тайны, которая будет рамочно схожа с системой обращения с информацией, составляющей государственную тайну, в том числе в организационно-правовом и технологическом плане¹.

¹ Занина, Т. М., Кораблев, П. Н. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России. – 2008. – №1 – С. 31-34.

Во многих приказах есть положение о том, что документы с пометкой «ДСП» запрещено пересылать в электронном виде, передача их возможна только в печатном виде фельдъегерской связью¹. В то же время некоторые специалисты в области документооборота отмечают, что «если действительно соблюдать все требования морально устаревшего нормативного документа, то работать в современных условиях будет невозможно»². И это действительно нельзя отрицать. Многие положения по работе с информацией ограниченного доступа практически не отражают проблематику электронного документооборота. И, если строго следовать положениям, его будто и нет в системе документов с грифом «ДСП», однако это не так. Стоит отметить, что одним из положительных примеров установления унифицированного порядка работы со сведениями, охраняемыми в режиме служебной тайны, включающего себя и порядок электронного документооборота, и порядок бумажного документооборота, является постановление Совета Министров Республики Беларусь от 12 августа 2014 года №783 «О служебной информации ограниченного распространения».

Нельзя отрицать, что помимо организационного аспекта охраны служебной тайны, немаловажную роль играет и технологические вопросы обеспечения защиты информации. Интересно отметить, что в 2011 году был издан приказ Минкомсвязи³, который установил технологические требования к системам внутреннего документооборота. При этом важным моментом этого документа является также указание на использование информационных систем государственных органов в МЭДО (межведомственный электронный

¹ К примеру: Об утверждении Инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации: Приказ Министерства образования и науки Российской Федерации от 30.12.2010 г. № 2233 (ред. от 10.08.2012).

² Храмцовская, Н. Документы «Для служебного пользования» в электронном документообороте государственных органов / Н. Храмцовская // Делопроизводство и документооборот на предприятии. – 2011. – № 3. – С.45-53.

³ Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения: приказ Минкомсвязи РФ от 02.09.2011 № 221.

документооборот). При этом в документе дается прямая отсылка к стандартам ГОСТ и требованиям ФСТЭК при установлении соответствия системы электронного документооборота нормативным требованиям. Во исполнение единства мер по охране служебной тайны, точнее, информации, находящейся в распоряжении государственных органов власти, но не являющейся секретной, был издан Приказ ФСТЭК №17. Отдельно были изданы правила обработки и хранения персональных данных¹.

Ранее технологические требования содержались в методических рекомендациях ФСТЭК «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее – СТР-К) и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования о защите информации»². В соответствии с разъяснениями, содержащимися в Информационном письме ФСТЭК³, указанные рекомендации не отменяются и применяются в части, не противоречащей Приказу ФСТЭК №17. Этот документ представляет большой интерес, так как подробнейшим образом определяет порядок защиты информационных систем органов государственной власти. Положительным моментом является то, что указанные стандарты обязательны для соблюдения не только органами г.в. и м.с.у., но могут также, по решению обладателя информации (заказчика) или

¹ Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21.

² Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации. // URL: [<https://fstec.ru/component/attachments/download/296>].

³ Информационное сообщение ФСТЭК России от 15.07.2013 N 240/22/2637 По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Сайт компании «Консультант Плюс». – (<http://www.consultant.ru/law/hotdocs/26995.html/>). – Дата обращения: 17.12.2017.

оператора информационной системы, применяться и для защиты информации, содержащейся в негосударственных информационных системах. Такое условие очень важно, особенно в случае исполнения условий госзаказа организациями, либо передаче информации подведомственным организациям органов г.в. и м.с.у..

В свою очередь разработка и производство средств защиты конфиденциальной информации и деятельность по технической защите конфиденциальной информации является лицензируемой деятельностью. Вне зависимости от того, кто является «потребителем» услуг по защите информации – коммерческая организация либо государственные органы – лицензирование происходит по правилам, установленным постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»¹ и постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

В то же время стоит отметить, что в названном приказе ФСТЭК подробно описаны и процедуры, которые должны быть соблюдены при создании системы обеспечения ее целостности и безопасности. Кроме того, как следует из Приказа, такие требования могут быть также применены и для защиты системы, содержащей общедоступную информацию. Цели защиты значительно шире утечки информации. Целью защиты информации также является недопущение удаления, изменения информации. Для нас этот приказ важен тем, что он свидетельствует о необходимости точной систематизации информации, точной классификации и определения конкретных сведений, оборот которых должен быть защищен. При такой регламентации защиты информации тезис о том, что невозможно установить конкретный перечень

¹ О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации: постановление Правительства Российской Федерации от 3.03.2012 № 171.

информации и четко определить пределы служебной необходимости, является несостоятельным, поскольку при отсутствии четкого определения круга информации и степени ее важности, представляется трудным в технологическом плане обеспечить безопасность данных.

Об этом также свидетельствует и требование, установленное п.14.4 названного приказа ФСТЭК, в соответствии с которым при принятии решения о необходимости защиты информации необходимо определение информации, подлежащей обработке в информационной системе, поскольку для разработки и функционирования системы безопасности является необходимым установление перечня объектов защиты информационной системы.

Также в документе определяются уровни значимости охраняемой информации, и, как следствие, от уровня значимости зависит режим защиты информации, который необходимо применить. При этом уровень значимости, как правило, определяется руководителем подразделения. Вместе с тем, стоит отметить, что критерии для разграничения таких сведений являются крайне условными. Так, к примеру, устанавливается высокий уровень значимости, «если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны *существенные негативные последствия* в социальной, политической, международной, экономической, финансовой *или иных областях деятельности*¹. Как видим, для обладателя информации устанавливается максимальная степень свободы и возможность усмотрения при определении степени значимости информации.

С точки зрения технических регламентов, такое установление правил определения степени важности представляется вполне оправданным, когда единственной целью классификации информации является лишь определение степеней аппаратной защиты. Однако если же рассматривать такую

¹ Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17. – Приложение №1.

классификацию в контексте общего массива нормативных актов, регламентирующих право на доступ к информации, а также порядок ограничения и основания доступа к ней, то подобная классификация не соответствует нормам законодательства. Нормативные акты все же требуют определенности при ограничении доступа к сведениям, доступ к которым не может быть ограничен.

В то же время, следует отметить, что система защиты информации в режиме служебной тайны является достаточно условной во многих органах г.в. и м.с.у.. Это связано порой как с архаичностью заведенного порядка документооборота (только бумажная форма), несогласованностью мер по защите информации, так и с низкой степенью ответственности государственных и муниципальных служащих, которая часто ограничивается исключительно дисциплинарными мерами ответственности. При этом немаловажным считаем и тот факт, что система охраны сведений не всегда учитывает реальную картину информационных угроз для сохранения сведений. Так, к примеру, из бесед с некоторыми государственными служащими удалось выяснить, что зачастую информация копируется, передается не через информационно-телекоммуникационные сети, в том числе сеть Интернет, а путем снятия фотографии с экрана компьютера, на котором и отображается защищаемая информация. Соответственно, в таких государственных органах нет ограничения на пользование мобильными устройствами, а также на выход в Интернет с персональных мобильных устройств. При этом стоит отметить, что в нормативных актах сложно найти запрет на такого рода доступ к информации, поскольку там речь идет о проставлении отметок и копировании именно с бумажных носителей на бумажные, также о передаче электронного документа по каналам электронной связи. В редких нормативных актах можно встретить ограничение на осуществление выписок из актов/копирования материалов иным образом.

Подводя итог изложенному, необходимо отметить отсутствие четко выстроенной системы защиты информации в каждом государственном органе,

выстроенной и интегрированной единой системы бумажного и электронного документооборота, что значительно снижает уровень защищенности информации. Кроме того, отмечено, что, при ограничении доступа к информации в электронной системе документооборота, необходимо установление точного перечня защищаемых сведений, что свидетельствует о недопустимости либо крайней неэффективности защиты информации, определяемой в официальных перечнях как «иная информация», что позволяет относить туда фактически любую информацию, ограничение доступа к которой диктуется «служебной необходимостью», по факту же, усмотрением уполномоченного лица.

Стоит отметить, что установление конкретного перечня защищаемых сведений, соблюдение принципов достаточности и разумности диктуется не только необходимостью обеспечения права граждан на информацию, но и экономическими соображениями. Как следует из анализа нормативных актов, вопросы эффективной технологической защиты доступа к информации требуют значительных финансовых вложений.

На основании вышеизложенного, полагаем, что необходимо установить единые стандарты защиты информации, охраняемой в режиме служебной тайны, в которые будут входить:

1. Организационные требования общего характера, под которыми понимается перечень мер, направленных на защиту информации, интегрированные правила бумажного и электронного документооборота. Организационные требования должны содержать такие разделы как:

а. порядок ограничения доступа к информации, правила ограничения доступа к информации;

б. порядок и основания допуска государственных и муниципальных служащих (иных лиц, если речь идет о подведомственных или сторонних организациях);

с. порядок работы с электронными и бумажными документами, электронными носителями. Этот раздел должен подробно описывать

ограничения. При этом правила должны учитывать современные технологические и аппаратные возможности электронных устройств, исключая возможность несанкционированного доступа, копирования и передачи информации;

d. порядок передачи информации, порядок учета переданной информации, ответственных лиц.

2. Организационные меры защиты информации индивидуального характера – отражение в трудовых договорах или контрактах обязательств по неразглашению информации, определенной как служебная тайна. Ранее мы уже указывали на законодательные недостатки, когда требование к государственному служащему предъявляется требование о неразглашении информации, ставшей ему известной в ходе исполнения должностных обязанностей.

3. Технологические требования, которые в части классификации уровня значимости защищаемой информации должны соответствовать законодательству о доступе к информации и законодательству, устанавливающему правила ограничения доступа к информации.

Также немаловажным моментом является установление определенных требований к защите информации, охраняемой в режиме служебной тайны, для организаций, которым была передана такая информация. Унификация мер безопасности поможет осуществлять более эффективную государственную информацию во всех сферах.

2.5. Ответственность за нарушение требований режима служебной тайны

Одной из составляющих механизма защиты информации является ответственность за нарушение в сфере производства и оборота информации, охраняемой в режиме служебной тайны.

Как правило, в литературе рассматривается ответственность именно за разглашение служебной тайны и отмечается ее плохая юридическая проработанность¹.

Однако круг вопросов и область ответственности в сфере служебной тайны гораздо шире проблемы разглашения. Ответственность должна быть предусмотрена за нарушения на любом из этапов оборота информации, охраняемой в режиме служебной тайны, не только для субъектов, осуществляющих работу со сведениями, охраняемыми в режиме служебной тайны, но и для субъектов, которые осуществляют отнесение информации к сведениям, охраняемым в режиме служебной тайны, субъектов, которые обеспечивают функционирование систем защиты информации, охраняемой в режиме служебной тайны, организацию работы и учет информации.

Рассмотрим основные виды ответственности, предусмотренные законодательством Российской Федерации и целесообразность их применения относительно нарушения режима служебной тайны.

Дисциплинарная ответственность. Как отмечают исследователи, в настоящее время вопрос ответственности за разглашение информации в основном ограничивается лишь дисциплинарной ответственностью². Возможность применения такого вида ответственности предусмотрена как Трудовым кодексом Российской Федерации (пп. в) п.6 ст. 81 ТК РФ), так и Законом о государственной гражданской службе (пп. в) п. 3 ст. 37 ФЗ № 79). За разглашение тайны в таком случае предусмотрена возможность применения такого вида дисциплинарного взыскания, как увольнение в соответствии с Трудовым кодексом и расторжение контракта в соответствии с ФЗ «О государственной гражданской службе». При этом стоит отметить, что в сфере государственной гражданской службы предусмотрена ответственность не только за разглашение охраняемой законом тайны, но также и за

¹ Занина, Т. М. Кораблев, П. Н. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России. – 2008. – №1 – С. 34.

² Там же.

разглашение служебной информации. Как было указано в четвертом параграфе первой главы, такое регулирование и ответственность за разглашение служебной информации в целом не представляется целесообразным и обоснованным, поскольку вся служебная информация сама по себе не является информацией ограниченного доступа только в силу служебного характера.

Исследователи отмечают сложность в сфере определения понятия «разглашение охраняемой законом тайны»¹. По мнению А. В. Стремоухова, определение разглашения должно отвечать требованиям нормативности, точности и определенности. Так, в частности, отмечается, что во многих законодательных определениях отсутствует субъект разглашения – а именно лицо, обязанное хранить охраняемую законом тайну.

Также важно разграничивать понятие «разглашение» информации и нарушение правил работы с информацией, охраняемой в режиме служебной тайны, поскольку далеко не всегда такое нарушение обязательно ведет к разглашению такой информации. Вопрос разграничения таких категорий давно обсуждается применительно к институту «коммерческой тайны»². В данном случае к работникам может быть применена дисциплинарная ответственность, не предусматривающая возможность увольнения в соответствии с ТК РФ. Однако считаем, что возможна ситуация, при которой с государственным служащим может быть расторгнут контракт по такому основанию как «утрата доверия» (пп. 1.1, п. 1 ст. 37 Закона о государственной гражданской службе).

¹ Стремоухов, А. В., Топоркова, С. А. Разглашение охраняемой законом тайны как основание увольнения работника / А. В. Стремоухов, С. А. Топоркова // Ленинградский юридический журнал. – 2012. – №2. – С.9-19.

Топоркова, С. А. Разглашение охраняемой законом тайны как трудовое правонарушение / С. А. Топоркова // Трудовое право в России и за рубежом. – 2012. – №3. – С.26-30.

² См. Разглашение коммерческой тайны: чем рискуют сотрудники. – (<http://www.glavbukh.ru/art/21636-razglashenie-kommercheskoy-tayny-chem-riskuyut-sotrudniki>). – Дата обращения: 17.12.2017.

Норма о прекращении трудового договора/расторжении служебного контракта в ТК РФ и в Законе О государственной гражданской службе является диспозитивной. Работодатель в данном случае сам вправе решать, к какой мере дисциплинарного воздействия должен быть привлечен работник/государственный служащий. По мнению Н. Ю. Агафоновой такой диспозитивный подход в части наложения дисциплинарного взыскания прямо нарушает принцип неотвратимости наказания и приводит к неэффективности регулирования поведения государственных гражданских служащих¹. Кроме того, в литературе высказывается позиция, в соответствии с которой законодательно необоснованно пытаться применить частно-правовые приемы диспозитивного регулирования трудовых отношений к сфере государственной гражданской службы, которая сама по себе обеспечивает функционирование государственно-властного аппарата и всей системы управления. В данном случае представитель нанимателя действует в государственных интересах, а не в частных. В связи с этим, по мнению И. В. Алениной, необходимо в некоторых аспектах снизить степень диспозитивности при принятии решения о привлечении государственного гражданского служащего к ответственности². С одной стороны, такое мнение весьма обоснованно, с другой же стороны, для установления императивного требования о наложении дисциплинарного взыскания (в том числе и такой меры как расторжение служебного контракта), необходимо четкое нормативное регулирование самого института служебной тайны, которое бы позволяло минимизировать субъективизм при отнесении информации к сведениям, охраняемым в режиме служебной тайны, а также позволило бы выработать конкретные требования для соблюдения требования конфиденциальности таких сведений. Также полагаем, что просто наличие формального состава дисциплинарного

¹ Агафонова, Н. Ю. Дисциплинарные взыскания в контексте ответственности государственных гражданских служащих / Н. Ю. Агафонова // Вестник ПАГС. – 2011. – №1. – С. 89-93.

² Аленина, И. В. Направления совершенствования системы оснований прекращения трудовых отношений с государственными гражданскими служащими / И. В. Аленина // Вестник Омского университета. Серия «Право». – 2015. – № 2 (43). – С. 198–209.

проступка как соответствующий ответственный субъект и факт известности информации третьим лицам недостаточен для наложения такого дисциплинарного взыскания как расторжение служебного контракта, так как при решении вопроса должны учитываться и обоснованность отнесения информации к сведениям, охраняемым в режиме служебной тайны, и обеспечение мер для защиты информации, охраняемой в режиме служебной тайны, и четкость организации системы работы с информацией ограниченного доступа.

Стоит отметить, что дисциплинарная ответственность, как правило, налагается именно за разглашение охраняемой законом тайны. В то же время, как было сказано раньше, случаи нарушения требований режима служебной тайны гораздо шире разглашения такой информации. Так, к примеру, указанные нарушения могут относиться к необоснованному отнесению информации к сведениям, охраняемым в режиме служебной тайны, а также к нарушению правил учета такой информации, работы с ней¹. В данном случае ответственность, безусловно, должна быть применима не только к лицам, непосредственно работающим с информацией, охраняемой в режиме служебной тайны, но также и к лицам, которые применяют решение об отнесении той или иной информации к сведениям, охраняемым в режиме служебной тайны, а также оформляют допуск и ведут учет работы с информацией этой категории.

Помимо всего прочего, важным вопросом является вопрос последствий расторжения контракта с государственным служащим при разглашении служебной тайны и разграничение случаев применения дисциплинарной ответственности от случаев применения административной ответственности.

Административная ответственность. В юридической литературе отмечается, что при установлении административной ответственности за

¹ Подробнее см. Станскова, У. М. Трудовые средства обеспечения конфиденциальности информации ограниченного доступа: автореф. дис. ... канд. юрид. наук: 12.00.05 / У. М. Станскова. – Екатеринбург, 2014. – 22 с.

нарушения в сфере служебной тайны, необходимо учитывать следующие направления правового регулирования:

1) обеспечение доступа граждан и (или) организаций к достоверной информации, необходимой для реализации их прав, свобод и обеспечения законных интересов;

2) организацию (и обеспечение) предупреждающего оповещения граждан и (или) организаций о фактах и событиях, создающих угрозу безопасности;

3) защиту информации ограниченного доступа;

4) предупреждение правонарушений в данной сфере¹.

В настоящий момент в КоАП существуют общие нормы, относящиеся к нарушениям в сфере обращения с информацией ограниченного доступа. Так, основной нормой, устанавливающей ответственность в сфере нарушения конфиденциальности информации, является ст. 13.14. «Разглашение информации с ограниченным доступом», санкцией в которой является штраф для должностных лиц и граждан.

Важным аспектом правового регулирования является также наличие ответственности за использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации, а также за нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации. Однако и в данном случае максимальный размер ответственности для должностного лица составляет пять тысяч рублей (ст. 13.14 КоАП РФ). Анализ такой нормы в сочетании с анализом норм о дисциплинарной ответственности очень важен, так как в данном случае становится очевидно несоответствие мер взыскания, поскольку

¹ Занина, Т. М., Караваев, А. А. Административная ответственность за правонарушения в сфере охраны конфиденциальной информации / Т. М. Занина, А. А. Караваев // Вестник ВИ МВД России. – 2013. – №3 – С.123-130.

В данном случае дисциплинарное взыскание в виде увольнения представляется более серьезным, нежели ответственность за несоблюдение мер защиты с учетом возможных последствий указанных правонарушений: так, при нарушении/игнорировании правил защиты и работы с информацией ограниченного доступа возможны большие объемы разглашенных сведений, чем в случае единичного акта разглашения информации государственным гражданским служащим.

В проекте нового КоАП¹ статья об ответственности за разглашение конфиденциальной информации, а также за нарушение требований защиты информации ограниченного доступа не претерпели существенных изменений, штраф увеличен до 7 000 рублей.

Следует отметить, что судебная практика по данной категории споров в абсолютном большинстве касается именно частных интересов (защита коммерческой, врачебной, иной профессиональной тайны). В отношении разглашения служебной тайны судебная практика практически отсутствует.

В литературе высказывается точка зрения, в соответствии с которой административная ответственность за нарушение в сфере работы со служебной тайной недостаточно проработана, поскольку такие нарушения значительно шире, чем разглашение информации. Так, к примеру, Швецов полагает, что необходимо установить административную ответственность за перенос сведений, охраняемых в режиме служебной тайны на неучтенные носители². На наш взгляд, такой подход излишне казуистичен, поскольку в данном случае принимается лишь один из аспектов нарушения правил работы со сведениями, охраняемыми в режиме служебной тайны.

В КоАП отсутствует какая-либо ответственность за необоснованное ограничение доступа к информации либо не отнесение информации к

¹ Проект № 957581-6 «Кодекса Российской Федерации об административных правонарушениях» // Сайт компании «Гарант». – (<http://www.garant.ru/hotlaw/federal/678561/>). – Дата обращения: 17.12.2017.

² Швецов, А. В. Защита информации в сфере служебной тайны в деятельности ОВД: Правовой аспект: дисс... канд. юрид. наук. 05.13.19 / А. В. Швецов. – Воронеж, 2005. – 189с.

категории ограниченного доступа, что в значительной мере способно снизить уровень открытости органов государственной власти. Единственный вид ответственности, встречающийся в этой сфере – ответственность за отказ в предоставлении информации.

Проводя анализ дисциплинарной и административной ответственности, нельзя не задаться вопросом о разграничении оснований для применения мер дисциплинарной и административной ответственности. Особенно этот вопрос актуален в области гражданской государственной службы, когда привлечение служащих возможно как в рамках административной, так и в рамках дисциплинарной ответственности.

Отмечается, что в литературе нет однозначной позиции относительно принадлежности института ответственности государственных служащих к отрасли трудового либо административного права¹.

В то же время «в странах континентальной правовой семьи (например,

¹ Носова, Ю. Б. Дисциплинарная ответственность в системе правового регулирования: соотношение административно-правового и трудового правового аспектов / Ю. Б. Носова // Вестник ВГУ. Серия: Лингвистика и межкультурная коммуникация. – 2007. – №2-2. – С.179-187.

Пашерстник, А. Е. К вопросу о советской государственной службе // А. Е. Пашерстник // Вопросы советского административного права: Сборник. – М., Л.: Изд-во АН СССР, 1949. – С. 123.

Иванов, А. С., Иванкина, Т. В., Куренной, А. М., Маврин, С. П., Хохлов, Е. Б. Правовое регулирование отношений в сфере госслужбы / А. С. Иванов, Т. В. Иванкина, А. М. Куренной, С. П. Маврин, Е. Б. Хохлов // ЭЖ Юрист. – 2004. – № 6. – С. 10.
Чиканова, Л. А. Правовое регулирование служебных отношений на государственной гражданской службе: вопросы теории и практики / Л. А. Чиканова // Журнал российского права. – 2005. – № 4. – С. 67;

Манохин, В. М., Адушкин, Ю. С. Российское административное право: учебник / В. М. Манохин, Ю. С. Адушкин. – Саратов: Изд-во Саратов. гос. акад. Права, 2000. – 416 с.
Старилов, Ю. Н. Административное право: в 2 ч.: ч. 2 Кн. 1: Субъекты. Органы управления. Государственная служба // Ю. Н. Старилов. – Воронеж: Изд-во ВГУ, 2001. – С. 352-384.
Ноздрачев, А. Ф. От концепции реформирования государственной службы к новым идеям правового регулирования государственно-служебных отношений в Российской Федерации / А. Ф. Ноздрачев // Модернизация экономики России: итоги и перспективы. – М., 2003. – С. 184-186.

Атаманчук, Г. В. Сущность государственной службы: история, теория, закон, практика: Монография / Г. В. Атаманчук. – М.: Изд-во РАГС, 2003. – С. 162-164.
Гришковец, А. А. Правовое регулирование государственной гражданской службы в Российской Федерации: учеб. курс / А. А. Гришковец. – М.: Дело и Сервис, 2003. – С. 32-62.

Франции и Германии) правовой статус карьерного чиновника, в том числе и его дисциплинарная ответственность, регулируется нормами не трудового, а исключительно административного права. В Великобритании и США правовой статус гражданских служащих также определяется системой специальных правовых норм. Для стран социалистической системы права, напротив, характерно отнесение дисциплинарной ответственности к трудовому праву с принципиальным отождествлением рабочих и служащих согласно доктрине, в соответствии с которой каждый человек участвует в жизни общества вне зависимости от сферы применения его труда»¹.

Вместе с тем, даже если исходить из позиции отношения института гражданской службы исключительно к административному регулированию, не снимается вопрос о применимых мерах ответственности, поскольку дисциплинарная ответственность предусмотрена ФЗ «О государственной гражданской службе», а также предусмотрена административная ответственность КоАП.

Как отмечается в литературе², КоАП не дает однозначного ответа на этот вопрос. И существуют различные точки зрения относительно возможности применения мер административной и дисциплинарной ответственности к государственным и муниципальным служащим. Так, к примеру, В. И. Манохин считал допустимым применение одновременно административной и дисциплинарной ответственности³. Другие авторы высказывают позицию, в соответствии с которой в каждом случае вопрос должен разрешаться в зависимости от того, какая ответственность будет в

¹ Носова, Ю. Б. Дисциплинарная ответственность в системе правового регулирования: соотношение административно-правового и трудового правового аспектов / Ю. Б. Носова // Вестник ВГУ. Серия: Лингвистика и межкультурная коммуникация. – 2007. – №2-2. – С.179-187.

² Сандальникова, Е. В. Юридическая ответственность государственных гражданских служащих в Российской Федерации: теоретико-правовое исследование: дис. ... канд. юрид. наук: 12.00.01 / Е. В. Сандальникова. – Ульяновск, 2007. – 180 с.

³ Манохин, В. М. Советская государственная служба / В. М. Манохин. – М.: Юрид. лит., 1966. – 195 с.

конкретном случае наиболее эффективна¹.

На первый взгляд, разрешение такого вопроса можно было бы найти в подходе, в соответствии с которым должностные лица, наделенные государственно-властными полномочиями, должны были бы нести ответственность в рамках административного права, а иные государственные служащие и граждане несли бы дисциплинарную ответственность. В то же время, на наш взгляд, такой подход был бы несправедлив. Как отмечалось ранее, меры дисциплинарной и административной ответственности в настоящее время не сопоставимы ни по последствиям правонарушений, ни по применимым мерам. Именно поэтому необходимо упорядочить меры ответственности за правонарушения в сфере государственной гражданской службы, определив сферу, случаи и субъекты ответственности более детально.

Все же стоит отметить, что анализ норм кодекса об административных правонарушениях показал, что ни за одно нарушение правового режима информации для должностных лиц и граждан не устанавливается такая ответственность как дисквалификация. Вместе с тем, полагаем, что вопрос введения такого вида ответственности как дисквалификация является достаточно перспективным для разработки, поскольку сама дисквалификация позволит исключить доступ нарушителя к объекту посягательств (информации) и позволит предупредить дальнейшие правонарушения.

На наш взгляд, было бы целесообразно ввести административную ответственность в виде дисквалификации на определенный срок. При таком виде ответственности лицо лишается доступа к объекту незаконных посягательств.

Кроме того, важно предусмотреть административную ответственность не только за разглашение информации, охраняемой в режиме служебной тайны, но также и за неправомерное либо необоснованное ограничение

¹ Бачило, И. Л., Калла, Х. Я., Катрич, С. В., Ларьков, А. Н. Ответственность в управлении / Бачило И. Л., Калла Х. Я., Катрич С. В., Ларьков А. Н., и др. – М.: Наука, 1985. – 303 с.

доступа к информации, содержащейся в органах государственной власти.

Также представляет интерес такой вопрос как ответственность за разглашение информации, охраняемой в режиме служебной тайны, которая передана либо образована в организациях в рамках выполнения обязательств по договору с органами государственной власти или местного самоуправления. В данном случае полагаем, что на первое место будет выходить договорная материальная ответственность и вопрос будет решаться исходя из положений договора и норм гражданского кодекса о материальной ответственности.

Материальная ответственность. Одним из камней преткновения в теории правового регулирования ответственности за нарушения в сфере оборота служебной тайны является вопрос о материальной ответственности государственных гражданских служащих. Природа такой ответственности неоднозначна: одни исследователи причисляют ее к мере дисциплинарной ответственности¹, другие считают ее гражданско-правовой ответственностью², существует также позиция, в соответствии с которой материальная ответственность выделяется как самостоятельный вид ответственности³. По мнению Е. Г. Бабелюк, нецелесообразно отождествлять материальную ответственность с гражданско-правовой, поскольку она только наступает при наличии виновных действий государственного служащего и носит преимущественно штрафной характер⁴.

ФЗ «О государственной гражданской службе» не предусматривает материальную ответственность гражданских служащих. Вместе с тем, при установлении ответственности за нарушение положений Федерального

¹ Самощенко, И. С. Понятие правонарушения по советскому законодательству / И. С. Самощенко. – М.: Юрид. лит., 1963. - 285 с.

² Смирнов, В. Т. О соотношении материальной ответственности рабочих и служащих по советскому трудовому праву / В. Т. Смирнов // Вестник ЛГУ. – 1963. – № 17. – С. 29 – 31.

³ Сыроватская, Л. А. Материальная ответственность рабочих и служащих по советскому трудовому праву: автореф. дис. ... канд. юрид. наук / Сыроватская Л. А. – М., 1966. – 16 с.

⁴ Бабелюк, Е. Г. Ответственность государственных служащих Российской Федерации: Административно-правовой аспект: дисс. ... канд. юрид. наук. 12.00.14 / Е. Г. Бабелюк. – Спб, 2005. – 203с.

закона, статья 68 Федерального закона дает отсылку к иным нормативным правовым актам. Логично предположить, что в субсидиарном порядке можно применить для таких отношений положения Трудового кодекса, который устанавливает случаи, размеры и порядок привлечения работника к ограниченной и полной материальной ответственности. В общем порядке работники (статус которых также распространяется на госслужащих в данной ситуации) несут ограниченную материальную ответственность, которая определяется размером прямого действительного ущерба и не может превышать размера одного среднего месячного заработка.

В то же время, специфика информационных отношений (к коим относятся и отношения в сфере оборота служебной тайны) такова, что размер реального действительного ущерба практически неизмерим, поскольку информация несет в себе потенциальную ценность, несопоставимую с ее материальным/электронным выражением. В связи с этим У. М. Станкова предлагает расширить категорию материальной ответственности за разглашение охраняемой законом тайны и включать в нее убытки, состоящие из реального ущерба и упущенной выгоды¹. Вместе с тем, следует отметить, что далеко не всегда даже возможно определить размер упущенной выгоды, особенно когда речь идет о разглашении служебной тайны, в том числе конфиденциальной информации о третьих лицах, поскольку такая информация не является оборотоспособной и может затрагивать права и свободы других лиц. Материальное выражение таких прав и свобод можно рассматривать только с точки зрения возмещения морального вреда.

Вопрос привлечения к такому виду ответственности представляется нам достаточно сложным в силу проблематичности материальной оценки ущерба/убытков, которые могут возникнуть в результате разглашения информации, охраняемой в режиме служебной тайны. В случае разглашения

¹ Станкова, У. М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореф. дис. ... канд. юрид. наук: 12.00.05 / У. М. Станкова. – Екатеринбург, 2014. – С.8.

внутренней информации, охраняемой в режиме служебной тайны, оценка ущерба представляется затруднительной. В связи с чем полагаем, что материальная ответственность государственных служащих в сфере оборота сведений, составляющих охраняемую законом тайну, носит компенсационный, а не штрафной характер, и применима далеко не всегда.

Уголовной ответственности за разглашение служебной тайны как таковой не предусмотрено. В то же время, предусмотрена уголовная ответственность за разглашение отдельных видов тайн, образующихся в государственных органах: Ст. 137 УК РФ «Нарушение тайны личной жизни»; ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»; ст. 285 «Злоупотребление должностными полномочиями»; ст. 293 «Халатность»; Статья 310. «Разглашение данных предварительного расследования», Статья 311. «Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса», Статья 320. «Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа», Статья 275. «Государственная измена», Статья 276. «Шпионаж», Статья 283. «Разглашение государственной тайны».

Предусмотренная ответственность направлена на защиту наиболее значимых общественных интересов.

Между тем, разглашение иной информации ограниченного доступа, находящейся в органах государственной власти, достигло глобальных масштабов. Как отметил Генеральный прокурор Российской Федерации Ю. В. Чайка, «Государственные служащие торгуют вверенной им информацией, оказывают подконтрольным структурам содействие в получении незаконных льгот и привилегий»¹.

¹ Дворников, А. А. Уголовно-правовая охрана государственной и служебной тайны в органах внутренних дел: автореф. дис.... к. ю. н. / А. А. Дворников. – Тюмень, 2007. – 22с.

В ряде исследований были сделаны предложения о введении уголовной ответственности за разглашение служебной тайны. Так А. А. Дворников предлагал ввести в Уголовный кодекс Российской Федерации статью 293.1 «Разглашение либо блокирование служебной тайны»¹.

Также в литературе предлагалось ввести статью «Нарушение установленного законом порядка получения, сбора, хранения, обработки, распространения и предоставления информации ограниченного доступа, не являющейся государственной тайной»².

На наш взгляд, введение уголовной ответственности необходимо для пропорциональности и уравнивания системы мер ответственности за нарушение правовых режимов информации ограниченного доступа. Вместе с тем, останется вопрос реализации таких мер ответственности, а также того, насколько это будет отвечать целям правового режима. В данном случае необходимо будет также решить вопрос гармонизации уголовного законодательства в части соотнесения различных видов составов преступлений, в которых объектом является информация, доступ к которой ограничен, а объективной стороной состава преступления выступает ее разглашение. В то же время, ужесточение административной ответственности путем введения дисквалификации как меры ответственности за разглашение служебной тайны, упорядочение соотношения норм административной и дисциплинарной ответственности, на наш взгляд, является необходимым.

Одним из важных вопросов, который необходимо решить при установлении ответственности за правонарушение в сфере охраны служебной тайны, является вопрос контроля и надзора за установлением режима «служебной тайны» и порядка его соблюдения. На данный же момент ситуация такова, что доступ к документам с грифом «ДСП», находящимся в

¹ Щадрин, С. Ф. Уголовно-правовая охрана служебной тайны: Автореф. дисс.... канд. юрид.наук. / С. Ф. Щадрин. – Ростов-на-Дону, 2002. – С. 5.

² Занина, Т. М., Караваев, А. А. Административная ответственность за правонарушения в сфере охраны конфиденциальной информации / Т. М. Занина, А. А. Караваев // Вестник ВИ МВД России. – 2013. – №3 – С.123-130.

распоряжении государственных органов, крайне затруднен как для других государственных органов, так и для прокуратуры (п. 2.1. ст. 4 ФЗ «О прокуратуре» предусматривает, что органы прокуратуры в связи с осуществлением ими в соответствии с настоящим Федеральным законом прокурорского надзора вправе получать в установленных законодательством Российской Федерации случаях доступ к необходимой им для осуществления прокурорского надзора информации, доступ к которой ограничен в соответствии с федеральными законами; вместе с тем, для служебной тайны такие случаи не установлены). Так в Проекте Закона о служебной тайне был предусмотрен ведомственный контроль и надзор, осуществляемый генеральным прокурором и подчиненными ему прокурорами. В законопроекте, разработанном Минэкономразвития, предполагалось создание информационной комиссии, которая будет разрешать вопросы правомерности и обоснованности отнесения той или иной информации к сведениям, охраняемым в режиме служебной тайны, а также был предусмотрен ведомственный контроль. На наш взгляд, формирование комиссии было бы слишком затратно, а эффективность ее функционирования вызывает большие сомнения, поскольку в настоящее время даже судебных споров относительно обжалования актов с грифом «ДСП» крайне мало. Во многом это связано с информационной закрытостью органов государственной власти и непроработанным порядком обжалования таких актов.

Как отмечалось ранее в исследовании, механизм обжалования ограничения доступа к информации к сведениям, охраняемым в режиме служебной тайны, также является затруднительным и малоэффективным в силу отсутствия прямого законодательного регулирования института и нередко отсутствия в свободном доступе документов, устанавливающих перечень информации, отнесенной к сведениям, охраняемым в режиме служебной тайны.

В результате проведенного исследования считаем, что необходимо решение следующих вопросов:

1. Необходимо решить вопрос о качественной проработке и применении мер ответственности не только за разглашение информации, но также и за неправомерное отнесение информации к сведениям, охраняемым в режиме служебной тайны, за нарушения режима работы с информацией, необеспечение мер защиты информации. На наш взгляд, необходимо введение дисквалификации как меры ответственности за разглашение служебной тайны, а также упорядочение соотношения норм административной и дисциплинарной ответственности.

2. Необходимо установление Порядка осуществления контроля и надзора за отнесением информации к сведениям, охраняемым в режиме служебной тайны, а также необходимы эффективные механизмы оспаривания ограничения доступа к информации, включающие в себя судебный и внесудебный порядок.

3. Необходимо внедрение механизма административного и судебного порядка обжалования процедуры отнесения информации к сведениям, охраняемым в режиме служебной тайны, который должен позволить эффективно разрешать вопросы обоснованности и законности ограничения доступа к данным сведениям.

ЗАКЛЮЧЕНИЕ

Проведенный анализ правового регулирования информации ограниченного доступа в целом и служебной тайны в частности показал серьезные недостатки правового регулирования. Прежде всего, необходимо говорить об отсутствии целостной системы регулирования информации ограниченного доступа, зачастую несогласованности правовых режимов, а также отсутствии как такового федерального закона, который бы регулировал отнесение информации к сведениям, охраняемым в режиме служебной тайны, а также их всемерную защиту.

В 2011 году, при рассмотрении Проекта закона о служебной тайне от Министерства экономического развития, была высказана точка зрения о том, что если в течение 2011 года возникнут спорные ситуации, связанные с непредставлением гражданам информации о деятельности государственного органа по причине конфиденциальности этой информации, тогда нужен закон «О служебной тайне», в противном случае разработка закона нецелесообразна¹. В связи с неосновательным ограничением доступа к информации, считаем такую позицию недопустимой и противоречащей требованиям Конституции и Федеральных Законов. Решение вопросов о защите конституционных прав граждан не должно ставиться в зависимость от возникновения спорных ситуаций. Регулирование в сфере обеспечения прав и свобод граждан должно быть упреждающим.

Отсутствие правового регулирования режима служебной тайны порождает несколько существенных проблем:

- отсутствие юридического основания для ограничения доступа к информации в режиме служебной тайны;

¹ Волчинская, Е. К., Гришанков, М. Некоторые проблемы формирования института служебной тайны в Российской Федерации / Е. К. Волчинская, М. Гришанков // Государственная служба. – 2011. – № 2. – С. 39-44.

- нарушение принципа свободы информации и права на доступ к информации;

- малоэффективность механизма защиты служебной тайны ввиду отсутствия четких унифицированных правил и, как следствие, угроза информационной безопасности как отдельных государственных органов, так и государства в целом.

В результате проведенного исследования приходим к следующим выводам:

1. С целью упорядочения научно-теоретических представлений о правовой природе информации, охраняемой в режиме служебной тайны, в зависимости от единства и дифференциации используемых правовых режимов информации, в которых охраняются сведения, существующие в органах власти, выделены следующие модели правового регулирования: 1. модель, в основу которой положена категория «государственные секреты» (в нее, в том числе, входит такая категория, как «служебная тайна»); модель, которая характеризуется использованием единственной категории – информации ограниченного доступа в сфере управления (государственная либо служебная тайна – наименование единого института зависит от особенностей перевода); модель, которая характеризуется разграничением правового режима государственная и служебная тайн.

2. С целью развития и унификации понятийно-категориального аппарата понятие «служебная информация» рассматривается как родовое для всей информации, используемой в органах государственной власти и органах местного самоуправления, а также подведомственных им организациях и государственных корпорациях. Понятие «служебная тайна» при этом должно обозначать правовой режим соответствующей информации ограниченного доступа. В отношении информации, охраняемой в режиме служебной тайны, автором предлагается использовать такое понятие как «сведения, охраняемые в режиме служебной тайны». При этом понятия «сведения» и «информация» синонимичны по своему значению, а понятие «служебная тайна»

тождественно понятию «правовой режим служебной тайны». В целях развития доктрины информационного права разработано авторское определение понятия «правовой режим служебной тайны», который представляет собой совокупность правовых, организационных и технических методов и средств, обеспечивающих защиту сведений, формирующихся в результате деятельности органов государственной власти и органов местного самоуправления, а также подведомственных им организаций, а также информации ограниченного доступа о физических и юридических лицах, ставшая известной указанным субъектам в результате осуществления возложенных на них полномочий и обязанностей.

3. Обосновано, что в целях правовой идентификации сведений, охраняемых в режиме служебной тайны, данные сведения должны обладать следующими признаками:

– формируются в результате осуществления государственной (муниципальной) управленческой и (или) связанной с ней хозяйственной деятельности либо является информацией ограниченного доступа о физических или юридических лицах, ставшей известной органам власти и подведомственным им организациям в результате осуществления возложенных на них полномочий и обязанностей;

– характеризуются закрытым перечнем субъектов, которые могут ими обладать: органы государственной власти, органы местного самоуправления, подведомственные им организации и государственные корпорации. В некоторых случаях сведения могут передаваться в ходе исполнения договоров гражданско-правового характера;

– доступ к данным сведениям ограничен требованиями федерального закона.

4. Разработан элементный состав правового режима служебной тайны, включающий в себя следующие элементы:

- принципы ограничения доступа к сведениям в режиме служебной тайны;

- объект режима – сведения, охраняемые в режиме служебной тайны;
- субъекты правоотношений в сфере оборота сведений, охраняемых в режиме служебной тайны, на которые возложены обязанности защиты сведений, охраняемых в режиме служебной тайны;
- содержание правоотношений в сфере оборота сведений, охраняемых в режиме служебной тайны;
- совокупность организационных и технических требований обеспечения конфиденциальности сведений, охраняемых в режиме служебной тайны;
- ответственность за нарушения требований режима служебной тайны.

5. С целью формирования единого теоретического подхода к правовому регулированию института служебной тайны, автором предложена и обоснована концепция правового регулирования служебной тайны, в соответствии с которой механизмы ограничения доступа к информации должны формироваться в соответствии с правовыми принципами законности, обоснованности, срочности характера ограничения, соблюдения прав и свобод человека и гражданина, интересов общественности, контроля за ограничением доступа к сведениям, охраняемым в режиме служебной тайны. Автором обоснована необходимость учета международных принципов национальной безопасности («Тсваньские принципы»)¹ при теоретическом осмыслении и формировании пути развития законодательства в сфере служебной тайны.

6. В работе доказывается, что при формировании классификации сведений, охраняемых в режиме служебной тайны, должно учитываться существующее нормативное регулирование, а также уже существующие перечни сведений, охраняемых в настоящее время под грифом «Для служебного пользования». В состав основных разделов данной классификации необходимо включать сведения об информационной и

¹ Global principles on national security and the right to information (“THE TSHWANE PRINCIPLES”) // Приняты в Тсване, Южная Африка, 12.06.2013. – URL: [https://fas.org/sgp/library/tshwane.pdf]

физической безопасности, информацию о непосредственной деятельности, связанной с реализацией властных полномочий, сведения в области геодезии, картографии и проектировании, информацию о научно-технических разработках, сведения об административно-хозяйственной деятельности, а также информацию, составляющую тайну третьих лиц.

7. В целях систематизации прав и обязанностей субъектов правоотношений в сфере служебной тайны разработана их классификация по различным основаниям. В зависимости от объема возложенных полномочий субъектов предложено подразделять на: субъектов, уполномоченных устанавливать правила оборота и основания отнесения информации к сведениям, охраняемым в режиме служебной тайны; субъектов, уполномоченных устанавливать конкретный перечень категорий сведений, доступ к которым может быть ограничен; субъектов, которые уполномочены относить ту или иную информацию к сведениям, охраняемым в режиме служебной тайны; субъектов, обеспечивающие соблюдение режима охраны сведений, охраняемых в режиме служебной тайны; субъектов, осуществляющих работу с документами, в которых содержатся сведения, охраняемые в режиме служебной тайны. В зависимости от основания получения доступа к сведениям, охраняемым в режиме служебной тайны предложено подразделять субъектов на: субъектов, получающих доступ к сведениям в силу закона; и субъектов, получающих доступ к сведениям в силу договора.

8. В целях формирования и развития комплексного правового регулирования служебной тайны как правового института, отвечающего требованиям современного информационного законодательства, разработаны и обоснованы следующие правовые средства:

– нормативная унификация порядка работы со сведениями, охраняемыми в режиме служебной тайны;

– определение и законодательная фиксация порядка осуществления государственного надзора за процедурой отнесения информации к сведениям, охраняемым в режиме служебной тайны;

– внедрение механизма административного и судебного порядка обжалования процедуры отнесения информации к сведениям, охраняемым в режиме служебной тайны, который должен позволить эффективно разрешать вопросы обоснованности и законности ограничения доступа к данным сведениям;

– введение системы мер юридической ответственности за нарушение требований режима служебной тайны.

В приложении к работе приведена концепция федерального закона о служебной тайне, в которой отражена авторская позиция в отношении принципов, в соответствии с которым должно происходить ограничение доступа к сведениям в режиме служебной тайны; концепция порядка установления перечня сведений, в частности, предложено деление категорий сведений на те сведения, доступ к которым должен быть ограничен в безусловном порядке, и те сведения, ограничение доступа к которым происходит по решению соответствующего органа. Также в концепции предусмотрена необходимость интеграции нормативного регулирования информационных систем, используемых в органах государственной власти, местного самоуправления и подведомственных организациях, и опубликования перечней сведений на сайтах органах г.в. и м.с.у.. Концепция также устанавливает необходимость существования административного и судебного порядка обжалования решения ограничения доступа к той или иной информации. Также концепцию отличает то, что в отношениях, основанных на договорных связях с организациями и гражданами, предусмотрен не односторонний механизм предоставления информации, а возможность возникновения и защиты информации, охрана которой должна быть в режиме служебной тайны. Также в концепции предусмотрена необходимость осуществления прокурорского надзора за соблюдением законодательства.

В современной России остро назрела необходимость правового регулирования института служебной тайны. За годы функционирования органов государственной власти в реалиях новой правовой системы накопился значительный опыт регулирования информации ограниченного доступа. Соответственно, есть возможность обобщения опыта и унификации правового регулирования. Кроме того, уже наметились тенденции к наведению порядка в сфере информации ограниченного доступа в органах государственной власти. Так многие положения о работе с информацией ограниченного доступа публикуются официально (другой вопрос заключается в том, что указанные положения во многом носят лишь рамочный и типовой характер), а в 2015 году было внесено существенное изменение в Концепцию развития уголовно-исполнительной системы Российской Федерации, которое предусматривает «пересмотр ведомственных нормативных правовых актов с грифом ограничения доступа к документу в целях исключения указанного грифа из актов, затрагивающих права и обязанности осужденных и лиц, содержащихся под стражей, либо исключения этих положений из указанных актов»¹. Также назрела острая необходимость в защите интересов национальной безопасности, а достижение такой цели невозможно себе представить без создания четкой системы информационной безопасности, одной из составляющих которой является защита информации, представляющей служебную тайну.

¹ О внесении изменений в Концепцию развития уголовно-исполнительной системы Российской Федерации до 2020 года: распоряжение Правительства РФ от 23.09.2015 г. № 1877-р.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативные правовые акты и другие официальные документы

1. Всеобщая декларация прав человека. Принята и провозглашена Генеральной Ассамблеей ООН 10 декабря 1948 г. // Российская газета. – 1998. – 10 дек.

2. Конвенция о защите прав человека и основных свобод от 04.11.1950 // СЗ РФ. – 1998. – №20. – Ст. 2143.

3. Международный пакт о гражданских и политических правах от 16.12.1966 // Ведомости ВС СССР. – 1976. – № 17. – Ст. 291.

4. Положение о межгосударственном обмене отправлениями специальной связи. Утверждено Соглашением Совета глав правительств Содружества Независимых Государств о межгосударственном обмене отправлениями специальной связи от 23 декабря 1993 года. (ред. от 15.03.2001) // СЗ РФ. – 2001. – № 13. – ст. 1274.

5. Решение Совета Евразийской экономической комиссии от 18.09.2014 № 71 «О Порядке работы с документами ограниченного распространения (конфиденциальными и для служебного пользования) в Евразийской экономической комиссии» // Официальный сайт Евразийской экономической комиссии. – (<http://www.eurasiancommission.org/>). – Дата обращения: 17.12.2017.

6. Модельный информационный кодекс для государств-участников СНГ. Принят в г. Санкт-Петербурге 23.11.2012 постановлением 38-6 на 38-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2013. – № 57 (часть 1). – С. 44-73.

7. Global Principles on national security and the right to information («the tshwane principles»). finalized in Tshwane, South Africa issued on 12 June 2013. – (<http://fas.org/sgp/library/tshwane.pdf>). – Дата обращения: 17.12.2017.

8. Модельный закон об информации, информатизации и обеспечении информационной безопасности. Принят в г. Санкт-Петербурге 28.11.2014 постановлением 41-15 на 41-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Сайт компании «Консультант Плюс». – (<http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=41358#0>). – Дата обращения: 17.12.2017.

9. Модельный информационный кодекс для государств-участников СНГ. Принят в г. Санкт-Петербурге 23.11.2012 постановлением 38-6 на 38-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2013. – №57 (часть 1). – С. 44-73.

10. CPNI information exchange membership guidelines. – (<http://webarchive.nationalarchives.gov.uk/20100815133302/http://www.cpni.gov.uk/Docs/ie-membership-guidelines.pdf>). – Дата обращения: 17.12.2017.

1.1. Нормативные правовые акты Российской Федерации

11. Конституция Российской Федерации от 12.12.1993 // СЗ РФ. – 2014. – № 31. – ст. 4398.

12. О Правительстве Российской Федерации: федер. констит. закон от 17.12.1997 №2-ФКЗ // СЗ РФ. – 1997. – № 51. – ст. 5712.

13. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской

Федерации: федер. закон от 30.11.2011 № 342-ФЗ // СЗ РФ. – 2011. – № 49 (ч. 1). – ст. 7020.

14. О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 27.07.2010 № 224-ФЗ // СЗ РФ. – 2010. – № 31. – ст. 4193

15. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 09.02.2009 № 8-ФЗ // СЗ РФ. – 2009. – № 7. – ст. 776.

16. О противодействии коррупции: федер. закон от 25.12.2008 № 273-ФЗ // СЗ РФ. – 2008. – № 52 (ч. 1). – ст. 6228.

17. О Государственной корпорации по атомной энергии «Росатом»: федер. закон от 01.12.2007 № 317-ФЗ // СЗ РФ. – 2007. – №49. – ст. 6078.

18. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // Российская газета. – 2006. – № 165.

19. О Персональных данных: федер. закон от 27.07.2006 № 152-ФЗ // СЗ РФ. – 2006. – № 31 (1 ч.). – ст. 3451.

20. О рекламе: федер. закон от 13.03.2006 № 38-ФЗ // СЗ РФ. – 2006. – №12. – ст. 1232.

21. О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ // СЗ РФ. – 2004. – № 32. – ст. 3283.

22. О государственной гражданской службе: федер. закон от 27.07.2004 № 79-ФЗ // СЗ РФ. – 2004. – № 31. – ст. 3215.

23. О страховании вкладов физических лиц в банках Российской Федерации: федер. закон от 23.12.2003 № 177-ФЗ // СЗ РФ. – 2003. – № 52 (часть I). – ст. 5029.

24. О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров: федер. закон от 08.12.2003 № 165-ФЗ // СЗ РФ. – 2003. – № 50. – ст. 4851.

25. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – ст. 3.
26. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – ст. 1.
27. Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ // СЗ РФ. – 2000. – № 32. – ст. 3340.
28. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // СЗ РФ. – 1998. – № 31. – ст. 3824.
29. О государственной тайне: закон РФ от 21.07.1993 № 5485-1 // СЗ РФ. – 1997. – № 41. – стр. 8220-8235.
30. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. – 1996. – № 25. – ст. 2954.
31. О рынке ценных бумаг: федер. закон от 22.04.1996 № 39-ФЗ // СЗ РФ. – 1996. – № 17. – ст. 1918.
32. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: федер. закон от 21.12.1994 № 68-ФЗ // СЗ РФ. – 1994. – № 35. – ст. 3648.
33. О прокуратуре: федер. закон от 17.01.1992 № 2202-1 // СЗ РФ. – 1995. – № 47. – ст. 4472.
34. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СЗ РФ. – 1994. – № 32. – ст. 3301.
35. О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 // Российская газета. – 1992. – № 32.
36. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 № 683 // СЗ РФ. – 2016. – № 1 (часть II). – ст. 212.
37. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 // СЗ РФ. – 1997. – № 10. – ст. 1127.

38. Об утверждении Перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 30.11.1995 № 1203 // СЗ РФ. – 1995. – № 49. – ст. 4775.

39. Об информации о деятельности Совета Федерации Федерального Собрания Российской Федерации, размещаемой в сети Интернет: постановление СФ ФС РФ от 25 декабря 2009г. № 556-СФ // СЗ РФ. – 2010. – №1. – ст. 65.

40. Об обеспечении доступа к информации о деятельности государственной Думы Федерального Собрания Российской Федерации: постановление ГД ФС РФ от 23 декабря 2009г. № 3018-5 ГД // СЗ РФ. – 2009. – №52 (ч. I). – ст. 6487.

41. О внесении изменений в Концепцию развития уголовно-исполнительной системы Российской Федерации до 2020 года: распоряжение Правительства РФ от 23.09.2015 г. № 1877-р // СЗ РФ. – 2015. – № 40. – ст. 5581.

42. Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных: постановление Правительства РФ от 10 июля 2013 № 583. // СЗ РФ. – 2013. – 30 (часть II). – ст. 4107.

43. О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных: распоряжение Правительства Российской Федерации от 10 июля 2013 г. № 1187-р // СЗ РФ. – 2013. – № 30 (часть II). – ст. 4128.

44. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии: постановление Правительства РФ от 3.11.1994 г. № 1233 // СЗ РФ. – 2005. – № 30 (ч. II). – ст. 3165

45. Об утверждении типового Кодекса профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с формированием и инвестированием средств пенсионных накоплений, и Правил согласования Кодексов профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с формированием и инвестированием средств пенсионных накоплений, с Федеральной службой по финансовым рынкам: постановление Правительства РФ от 12.12.2004 № 770 // СЗ РФ. – 2004. – № 51. – ст. 5185.

1.2. Нормативные правовые акты федеральных органов исполнительной власти

47. Об официальном сайте Федеральной службы государственной регистрации, кадастра и картографии» (вместе с «Положением об официальном сайте Федеральной службы государственной регистрации, кадастра и картографии в информационно-телекоммуникационной сети «Интернет», содержащем блоки региональной информации территориальных органов Росреестра», «Регламентом взаимодействия структурных подразделений центрального аппарата и территориальных органов Росреестра по информационному наполнению официального сайта Федеральной службы государственной регистрации, кадастра и картографии, содержащего блоки региональной информации территориальных органов Росреестра»): приказ Росреестра от 26.07.2016 № П/0359 // Документ опубликован не был.

48. Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральной службе по регулированию алкогольного рынка (вместе с «Порядком передачи служебной информации ограниченного распространения другим государственным органам власти и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения»): Приказ

Росалкогольрегулирования от 29.01.2015 № 20 // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2015. – № 30.

49. Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве регионального развития Российской Федерации и его территориальных органах (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения», «Порядком организации защиты служебной информации ограниченного распространения»): приказ Минрегиона России от 20.05.2014 № 148 // Российская газета. – 2014. – № 211.

50. Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации и организаций, находящихся в его ведении: Приказ Минфина России от 17.06.2014 № 162 // документ опубликован не был.

51. Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральном агентстве по рыболовству и его территориальных органах (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения»): Приказ Росрыболовства от 11.12.2014 № 986.

52. Об утверждении Инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации: приказ Министерства образования и науки Российской Федерации от 30 декабря 2010 г. № 2233 // Вестник образования. – 2011. – №3.

53. Об утверждении Инструкции о порядке ведения официального сайта Следственного комитета Российской Федерации в сети Интернет: приказ Следственного комитета РФ от 30 сентября 2011г. № 141.

54. О предоставлении доступа пользователей к информационному фонду и сервисам центрального узла информационно-коммуникационной системы Росатома: приказ Росатома от 17.12.2007 № 651 // Документ опубликован не был

55. Об организации доступа пользователей к информационному фонду и сервисам центрального узла информационно-коммуникационной системы Росатома» (вместе с «Порядком подключения пользователей к системе электронного документооборота Росатома», «Инструкцией по обеспечению информационной безопасности при организации доступа пользователей к информационным ресурсам и сервисам центрального узла информационно-коммуникационной системы Росатома»): приказ Росатома от 22.10.2007 № 544 // Документ опубликован не был.

56. Об обеспечении доступа к информации о деятельности Министерства финансов Российской Федерации» (вместе с «Порядком обеспечения доступа граждан и организаций к информации о деятельности Министерства финансов Российской Федерации», «Порядком предоставления средствам массовой информации сведений о деятельности Министерства финансов Российской Федерации», «Порядком формирования информации о мероприятиях, проводимых с участием руководства Министерства финансов Российской Федерации»). Приказ Минфина РФ от 07.11.2005г. № 133н.

57. О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом и от проведения операции с денежными средствами или иным имуществом: указание Банка России от 26.11.2004 № 1519-У // Вестник Банка России. – 2004. – № 73.

58. О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом и от проведения операции с денежными средствами или иным имуществом: указание Банка России от 26.11.2004 № 1519-У» // Вестник Банка России. – 2004. – № 73.

59. Об утверждении Порядка доступа к конфиденциальной информации налоговых органов: приказ МНС РФ от 03.03.2003 № БГ-3-28/96) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2003. – № 23.

60. Об утверждении инструкции по делопроизводству в вооруженных силах российской федерации: приказ Министра обороны РФ от 23.05.1999 №170. // документ опубликован не был.

1.3. Нормативные акты субъектов и муниципальных образований Российской Федерации

61. Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в государственном комитете Кабардино-Балкарской республики по транспорту и связи: приказ государственного комитета Кабардино-Балкарской республики по транспорту и связи от 16 января 2015 года № 4-П.

62. Об утверждении Положения о порядке работы со служебной информацией ограниченного распространения в администрации Волжского муниципального района: распоряжение администрации Волжского муниципального района от 18.04.2012 №71. – (http://www.rvolzsk.ru/municipalnaja-sluzhba/pravovue_aktu). – Дата обращения 17.06.2017.

63. Об организации работы со служебной информацией ограниченного доступа в исполнительных органах государственной власти

Архангельской области: указ Губернатора Архангельской области от 25.08.2011 № 125-у.

64. Инструкция о порядке обращения со служебной информацией ограниченного распространения в исполнительных органах государственной власти Ямало-Ненецкого автономного округа: постановление администрации Ямало-Ненецкого автономного округа от 28.01.2010 № 49-А.

65. Об утверждении временного перечня сведений, составляющих служебную информацию ограниченного распространения: постановление Администрации Кировской области от 18.06.1997 № 183 (ред. от 08.10.1997).

66. Постановление администрации Кировской области от 18.06.1997 № 183 «Об утверждении временного перечня сведений, составляющих служебную информацию ограниченного распространения» (ред. От 08.10.1997). – (<http://docs.cntd.ru/document/973010567>). – Дата обращения: 17.06.2017.

67. О работе со служебной информацией в Совете депутатов муниципального образования «Пироговское»: решение Совета депутатов муниципального образования «Пироговское» 28.08.2014 № 89.

68. Перечень сведений, составляющих служебную информацию в Нижнегорском районном совете и его исполнительном аппарате: распоряжение председателя Нижнегорского районного совета от 20.06.2011 №12.

2. Исторические нормативные акты

69. Полное собрание законов Российской Империи. Собрание Первое. 1649-1825 гг. / под ред. М.М. Сперанского. – Спб: Тип. II Отделения Собственной Его Императорского Величества Канцелярии. – 1830.

70. Инструкция начальникам контрразведывательных отделений от 8 июня 1911 г. – (http://www.e-reading.by/chapter.php/1004112/36/Linder_Iosif_-_Specsluzhby_Rossii_za_1000_let.html). – Дата обращения: 17.06.2017.

71. Россия. Законы и постановления. Временное положение о военной цензуре от 20.07.1914. – [Пг., 1914]. – 15, [2] с.

72. О шпионаже, а равно о собирании и передаче экономических сведений, не подлежащих оглашению: постановление СНК СССР от 14 августа 1925 года.

73. Об утверждении перечня сведений, являющихся по своему содержанию специально охраняемой государственной тайной: Постановление СНК СССР от 27.04.1926 // СЗ СССР. – 1926. – № 32. – ст. 213

74. О введении в действие уголовного кодекса Р.С.Ф.С.Р.: постановление ВЦИК от 22 ноября 1926 года // СУ РСФСР. – 1926. – № 80. – ст. 600.

75. Положение о преступлениях государственных (контрреволюционных и особо для Союза ССР опасных преступлениях против порядка управления): постановление ЦИК СССР от 25.02.1927 // СЗ СССР. – 1927. – № 12. – ст. 123.

76. Об изменении Уголовного Кодекса Р.С.Ф.С.Р.: Постановление ВЦИК, СНК РСФСР от 06.06.1927 // СУ РСФСР. – 1927. – № 58. – ст. 404.

77. Об утверждении Положения о Главном управлении по делам литературы и издательств и его местных органах: постановление СНК РСФСР от 06.06.1931 // СУ РСФСР. – 1931. – № 31. – ст. 273.

78. Об ответственности за разглашение государственной тайны и за утрату документов, содержащих государственную тайну: указ Президиума ВС СССР от 09.06.1947 // Ведомости ВС СССР. – 1947. – № 20.

79. Об установлении перечня сведений, составляющих государственную тайну, разглашение которых карается по закону: постановление Совмина СССР от 08.06.1947 № 2009. // Известия. – 1947. – С. 1.

80. О Перечне сведений органов прокуратуры, не подлежащих опубликованию в открытой печати, передачах по радио и телевидению: Приказ Генпрокуратуры СССР от 22.11.1971 № 45.

3. **Нормативные акты иностранных государств**

81. Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» // URL: [<http://www.kgb.by/ru/zakon170-3/>]

82. Закон Республики Казахстан от 15 марта 1999 года № 349-І «О государственных секретах» // «Казахстанская правда» от 19 марта 1999 года №53 (22770).

83. Закон Республики Армения от 30 декабря 1996 года №ЗР-94 «О государственной и служебной тайне» // Официальные ведомости Республика Армения, декабрь 1996 года, №23-24 (1123-1124), Ст.298.

84. Постановление совета министров Республики Беларусь от 12 августа 2014 года №783 О служебной информации ограниченного распространения (ред. от 20.10.2015) // Национальный правовой Интернет-портал Республики Беларусь от 16 августа 2014 года, 5/39265.

4. **Специальная научная литература**

85. Абрамова, А. А. Дисциплина труда в СССР. Правовые вопросы. / А. А. Абрамова. – М.: Юрид. лит., 1969. – 176 с.

86. Алексеев, С. С. Общие дозволения и общие запреты в советском праве / С. С. Алексеев. – М.: Юрид. Лит., 1989. – 288 с.

87. Алексеев, С. С. Собрание сочинений. В 11 томах. / С. С. Алексеев. – М.: Статут, 2010. – 3 т.

88. Атаманчук, Г. В. Сущность государственной службы: история, теория, закон, практика: Монография / Г. В. Атаманчук. — М.: Изд-во РАГС, 2003. – 272 с.

89. Бачило, И. Л. О методологии выявления и классификации понятийного аппарата в информационном праве // Понятийный аппарат информационного права / отв. Ред. И. Л. Бачило, Э. В. Талапина. Сб. науч.

Работ. – М.: ИГП РАН – Издательство «Канон+» РООИ «Реабилитация», 2015. – С.8-18.

90. Бачило, И. Л., Лопатин, В. Н., Федотов, М. А. Информационное право: учебник / под ред. Б. Н. Топорнина. – СПб.: Юридический центр Пресс, 2001. – 789 с.

91. Бачило, И. Л., Калла Х. Я., Катрич С. В., Ларьков А. Н. Ответственность в управлении / Бачило И. Л., Калла Х. Я., Катрич С. В., Ларьков А. Н., и др.; Отв. ред.: Лазарев Б. М., Лунев А. Е. – М.: Наука, 1985. – 303 с.

92. Бачило, И. Л. О векторах эволюции государственных и правовых институтов в условиях глобальной информатизации // Эволюция государственных и правовых институтов в условиях развития информационного общества / Сборник научных работ. – М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», – 2012 г.

93. Бахрах, Д. Н. Административное право России. Учебник для Вузов. / Д. Н. Бахрах. – М.: Издательство «Норма», 2000. – 640 с.

94. Вавулин, Д. А. Комментарий к Федеральному закону «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» / Д. А. Вавулин. – М.: Деловой двор, 2015.

95. Гришковец, А. А. Правовое регулирование государственной гражданской службы в Российской Федерации: учеб. курс / А. А. Гришковец. – М.: Дело и Сервис, 2003. – 464 с.

96. Дурманов, Н. Д. Понятие преступления / Н. Д. Дурманов; Отв. ред.: Шаргородский М.Д. – М., Л.: Изд-во АН СССР, 1948. – 315 с.

97. Жилинский, С. Э. Предпринимательское право (правовая основа предпринимательской деятельности) / С. Э. Жилинский, – М.: Издательство НОРМА, 2001. – 944 с.

98. Зенин, И. А. Гражданское и торговое право капиталистических государств: Учеб. Пособие / И. А. Зенин. – М.: МГУ, 1992. – 192 с.
99. Камалова, Г. Г. О субъектах правоотношений в области защиты служебной тайны / Г. Г. Камалова // колл. монография / под общ. ред. И. Л. Бачило. – М.: Издательство Юрайт, 2009. – 530 с.
100. Каплин, С. Ю. Государственная корпорация как субъект права: монография / Каплин С. Ю.; Науч. ред Павлушина А. А. – Самара: Инсома-пресс, 2011. – 98 с.
101. Ковалева, Н. Н. Информационное право России / Н.Н. Ковалева. - Учебное пособие, — М.: Дашков и Ко, 2007. – 360 с.
102. Коваленко, Ю. И. Организационно-правовое обеспечение информационной безопасности: Учебно-методическое пособие / Ю. И. Коваленко. – М.: МИНИТ ФСБ России, 2003. – 148 с.
103. Колпакиди, А. А., Север, А. Спецслужбы Российской Империи. Уникальная энциклопедия / А. А. Колпакиди, А. Север, – М.: Эксмо, 2010.
104. Копылов, В. А. Информационное право / В. А. Копылов. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – 512 с.
105. Кучеров, И. И., Торшин А. В. Налоговая тайна: правовой режим защиты информации / И. И. Кучеров, А. В. Торшин. – М.: АО «Центр ЮрИнфоР», 2003. — 328 с.
106. Лебедев, В. И. Реформы Петра I: сборник документов / В. И. Лебедев. – М., 1937. – 379 с.
107. Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство: Монография / В. Н. Лопатин. – Спб.: Фонд «Университет», 2000. – 426 с.
108. Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин. /Санкт-Петербургский университет МВД России. – СПб.: Фонд «Университет», 2000. – С. 175-176.
109. Мазуров, В. А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: Учебное пособие / В.

А. Мазуров. – М.: Издательско-торговая корпорация «Дашков и К0», 2003. – 156 с.

110. Малько, А. В. Стимулы и ограничения в праве / А. В. Малько. – М., 2003. – 250 с.

111. Манохин, В. М. Советская государственная служба. / В. М. Манохин – М.: Юрид. лит., 1966. – 195 с.

112. Манохин, В. М., Адушкин, Ю. С. Российское административное право: учебник / В. М. Манохин, Ю. С. Адушкин. – Саратов: Изд-во Сарат. гос. акад. Права, 2000. – 416 с.

113. Морозов, А. В., Полякова, Т. А. Организационно-правовое обеспечение информационной безопасности: монография / А. В. Морозов, Т. А. Полякова; РПА Минюста России. – М.: РПА Минюста России, 2013. – 276с.

114. Никонов, Д. А., Стремоухов, А. В. Трудовое право: курс лекций. / Д. А. Никонов, А. В. Стремоухов. – М.: Норма, 2007. – 431 с.

115. Полякова, Т. А. Информационная безопасность в условиях построения информационного общества в России. Монография / Т. А. Полякова; ГОУ ВПО РПА Минюста России. – М.: ГОУ ВПО РПА Минюста России, 2007. – 170 с.

116. Прокопенко, А. А., Дрога, А. А. Правовое регулирование оборота информации, относящейся к служебной и профессиональной тайне в органах внутренних дел: монография / А. А. Прокопенко, А. А. Дрога. – Белгород: БелЮИ МВД России, 2011. – 97 с.

117. Римаренко, Ю. І. Приватне життя і поліція. Концептуальні підходи. Теорія та практика / Ю. І. Римаренко – К.: КНТ, 2006. – 740 с.

118. Самощенко, И. С. Понятие правонарушения по советскому законодательству. / И. С. Самощенко. – М.: Юрид. лит., 1963. – 263 с.

119. Старилов, Ю. Н. Административное право: в 2 ч.: ч. 2 Кн. 1: Субъекты. Органы управления. Государственная служба // Ю. Н. Старилов. – Воронеж: Изд-во ВГУ, 2001. – С. 352-384.

120. Суханов, Е. А. Гражданское право: В 4 т. Учебник. / Е. А. Суханов. – 2008, – 2т. – 463 с.

121. Терещенко, Л. К. Модернизация информационных отношений и информационного законодательства: Монография / Терещенко Л. К. – М.: ИНФРА-М, 2013. – 227 с.

122. Фатьянов, А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве): Моногр. / А. А. Фатьянов. – М.: Изд-во МИФИ, 1998. – 288 с.

123. Яковец, Е. Н., Смирнова, И. Н. Нормативное регулирование оборота сведений, составляющих служебную тайну / Е. Н. Яковец, И. Н. Смирнова. // Электронный ресурс. – 2009.

124. Якуба, О. М. Административная ответственность / О. М. Якуба. – М., 1972. – 152 с.

125. Ястребов, О. А. Публичные субъекты административного права. Учебное пособие. / О. А. Ястребов. – М., 2008. – 188 с.

2.1. Статьи, периодические издания

124. Агафонова, Н. Ю. Дисциплинарные взыскания в контексте ответственности государственных гражданских служащих / Н. Ю. Агафонова // Вестник ПАГС. – 2011. – №1 – С.89-93.

125. Аленина, И. В. Направления совершенствования системы оснований прекращения трудовых отношений с государственными гражданскими служащими / И. В. Аленина // Вестник Омского университета. Серия «Право». – 2015. – № 2 (43). – С. 198–209.

126. Алексеенцев, А. И. «О составе защищаемой информации / А. И. Алексеенцев // Безопасность информационных технологий. – 1999. – № 2. – С. 5-7.

127. Антопольский, А. А. Региональное законодательство о конфиденциальной служебной информации / А. А. Антопольский // Информационные ресурсы России. – 2005. – № 3. – С. 28-31.
128. Афанасьева, О. Право граждан на информацию и его гарантии / О. Афанасьева // Отечественные записки. – 2004. – № 3 (18)
129. Балашкина, И. В. Модернизация законодательства о личной и семейной тайне: проблемы и перспективы / И. В. Балашкина // Модернизация правовой системы России: сборник научных статей. – М.: Изд-во РАГС, 2011. – С. 156-168.
130. Батулин, П. В. Перечни военной цензуры 1912-1923 гг. // Ленинградский юридический журнал. – 2012. – № 4. – С.152-165.
131. Бачило, И. Л. Правовые проблемы развития информационного общества // Информационное право: актуальные проблемы теории и практики: сб. докладов науч.- практ. Конференции, Москва, 3 апреля 2015/ ред.совет: Ю. Л. Васильченко, И. М. Рассолов, С. Г. Чубукова. – М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2015. – С. 6-14.
132. Волчинская, Е. К. К юбилею Закона Российской Федерации «О государственной тайне» // Информационное право. – 2013. – № 2.
133. Волчинская, Е. К. О проблемах формирования правовой системы ограничения доступа к информации / Е. К. Волчинская // Информационное право. – 2013. – № 4.
134. Волчинская, Е. К. Некоторые приоритеты национальной безопасности в информационной сфере и проблемы их законодательного обеспечения / Е. К. Волчинская // Информационное право. – 2009. – № 4. – С. 4.
135. Волчинская, Е. К. Роль государства в обеспечении информационной безопасности / Е. К. Волчинская // Информационное право. – 2008. – № 4.

136. Волчинская, Е., Гришанков, М. Некоторые проблемы формирования института служебной тайны в Российской Федерации / Е. Волчинская, М. Гришанков // Государственная служба, - 2011. № 2.- С. 39-44.
137. Гаврилов, Э. К. вопросу об охране коммерческой, служебной и личной тайны. Гражданско-правовые аспекты // Хозяйство и право. – 2003. – №5 – С. 27.
138. Дементьев, А. Н. Принципы местного самоуправления / А. Н. Дементьев // Право и образование. – 2006. – №5. – С. 131-135.
139. Епифанова, Е. В. «Общественная опасность» как признак преступления в доктринах российского уголовного права в XVIII-XIX в.в. / Е. В. Епифанова // Юридическая наука. – 2011. – № 3. – С. 12-15.
140. Занина, Т. М., Караваев, А. А. Административная ответственность за правонарушения в сфере охраны конфиденциальной информации / Т.М. Занина, А. А. Караваев // Вестник ВИ МВД России. – 2013. – № 3 – С.123-130.
141. Занина, Т. М. Кораблев, П. Н. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России, 2008. – № 1 – С. 31-34.
142. Зданович, А. А. Забытое дело подполковника Грима / А. А. Зданович // Независимое военное обозрение. – 1998. – № 6.
143. Иванов, А. С., Иванкина, Т. В., Куренной, А. М., Маврин, С. П., Хохлов, Е. Б. Правовое регулирование отношений в сфере госслужбы / А.С. Иванов, Т. В. Иванкина, А. М. Куренной, С. П. Маврин, Е. Б. Хохлов // ЭЖ Юрист. – 2004. – № 6. – С. 10-15.
144. Камалова, Г. Г. О правовом режиме служебной тайны / Г. Г. Камалова // Вестник УдмГУ. – 2014. – №2-4. – С.145-152.
145. Кузнецов, П. У., Андреев, П. Г. Структура и содержание модели закона об информационной безопасности / П. У. Кузнецов, П. Г. Андреев // Вестник УрФО. Безопасность в информационной сфере. – № 1(3) – 2012 г. – С. 4-10.

146. Ковалева, Е. В. Международно-правовое регулирование права доступа к информации/ Е. В. Ковалева // Власть. – 2010. – №7 – С. 106-109.
147. Кузнецов, П. У. К вопросу об информационной свободе как правовой категории гражданского общества / П. У. Кузнецов // Информационное право и становление основ гражданского общества в России. Материалы теоретического семинара по информационному праву 2007г. – М: ИГП РАН, 2008. – С.31-36.
148. Кузнецов, П. У. Правовой режим как категория и метод информационного права / П. У. Кузнецов // Правовые понятия и категории в контексте информационного права. Материалы теоретического семинара по информационному праву. – М. 2006 – С. 12-32.
149. Михеев, Д. С. Закрепление принципа гласности в Европейской Хартии местного самоуправления / Д. С. Михеев // Ученые записки Казанского Университета. – Т.155. – кн.4. – 2013. – С. 62-68.
150. Минбалеев, А. В. Принципы информационного права / А. В. Минбалеев // Вестник ЮУрГУ. Серия: Право. – 2015. №1 – С.79-84.
151. Минбалеев, А. В. Характеристика метода правового регулирования (на примере метода информационного права) / А. В. Минбалеев // Вестник ЮУрГУ. Серия: Право. – 2013. №2 – С.91-94.
152. Минбалеев, А. В. Кванина, В. В. Правовая сущность информации, являющейся общественным достоянием, и информации, являющейся национальным достоянием / А. В. Минбалеев, В. В. Кванина // Вестник Южно-Уральского государственного университета. Серия «Социально-гуманитарные науки». – 2005. – Вып. 4. – № 7 (47).
153. Николаев, А. М. Общественная опасность деяний как отличительный признак их преступности / А. М. Николаев // Пробелы в российском законодательстве. – 2011. – №5. – С.160-162.
154. Носова, Ю. Б. Дисциплинарная ответственность в системе правового регулирования: соотношение административно-правового и

трудового правового аспектов / Ю. Б. Носова // Вестник ВГУ. Серия: Лингвистика и межкультурная коммуникация. – 2007. – №2-2. – С.179-187.

155. Ноздрачев, А. Ф. От концепции реформирования государственной службы к новым идеям правового регулирования государственно-служебных отношений в Российской Федерации / А. Ф. Ноздрачев // Модернизация экономики России: итоги и перспективы. – М., 2003. – С. 184-186.

156. Отнюкова, Г. Д. Коммерческая тайна / Г. Д. Отнюкова // Закон. – 1998. – № 2. – С. 55-59.

157. Павлов, И. Ю. Современные проблемы правового регулирования государственной и служебной тайны в России // Ленинградский юридический журнал. – 2013. – №1 (31). – С. 29-37.

158. Пашерстник, А. Е. К вопросу о советской государственной службе // А. Е. Пашерстник // Вопросы советского административного права: Сборник. – М. – Л., 1949. – С. 123-137.

159. Полякова, Т. А. Доктрина информационной безопасности России: правовые вопросы модернизации / Т. А. Полякова // Информационное право: актуальные проблемы теории и практики: сб. докладов науч.-практ. Конференции, Москва, 3 апреля 2015 г. / ред. Совет: Ю. Л. Васильченко, И. М. Рассолов, С. Г. Чубукова. – М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), – 2015. – С. 18-34.

160. Полякова, Т. А. Семизорова, Е. В., Александрова, О. А. Обеспечение информационной открытости при противодействии коррупции в Российской Федерации: проблемы правового регулирования / Т. А. Полякова, Е. В. Семизорова, О. А. Александрова // Эволюция государственных и правовых институтов в условиях развития информационного общества/ Сборник научных работ. – М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», – 2012. – 340с.

161. Полякова, Т. А., Акулова, Е. В. Правовое обеспечение информационной безопасности: проблемы понятийного аппарата. / Т. А. Полякова, Е. В. Акулова // Понятийный аппарат информационного права. Сб.

Науч. Работ. – М. ИГП РАН – Издательство «Канон +» РООИ «Реабилитация», 2015. – 280 с.

162. Смирнов, В. Т. О соотношении материальной ответственности рабочих и служащих по советскому трудовому праву / В. Т. Смирнов // Вестник ЛГУ. – 1963. – № 17. – С. 29-31.

163. Соболева В. Служебная тайна и коммерческая тайна: о чем должен молчать профессионал / В. Соболева // Секретарское дело. – 2009. – №3.

164. Стефанович, П. С. Понятие верности в отношениях князя и дружины на Руси в XII–XIII в. // Древняя Русь. Вопросы медиевистики. – 2008. – № 1 (32). – С. 72-82.

165. Стефанович, П. С. Дружинный строй в древней Руси и у древних германцев: существовала ли клятва верности вождю (правителю)? // Древняя Русь. Вопросы медиевистики. – 2008. – № 2 (32). – С. 33-40.

166. Стремоухов, А. В., Топоркова, С. А. Разглашение охраняемой законом тайны как основание увольнения работника / А. В. Стремоухов, С. А. Топоркова // Ленинградский юридический журнал. – 2012. – №2. – С.9-19.

167. Тедеев, А. А. Понятие, виды и система источников информационного права в современных условиях / А. А. Тедеев // Вопросы правоведения. – № 3–4/2009 – С.37-35.

168. Тедеев, А. А. Формирование доктринального понимания сущности источников информационного права / А. А. Тедеев // Вопросы правоведения. – 2010. – №1. – С. 101-113.

169. Тедеев, А. А. Предмет информационного права в условиях Интернета / Тедеев А. А. // Информационное право. – 2006. – №3. – С. 3-5.

170. Тедеев, А. А. Понятие, виды и система источников информационного права в современных условиях /А. А. Тедеев. // Вопросы правоведения. – 2009. – № 3-4. – С. 37-75.

171. Терещенко, Л. К. Правовые основы специальных режимов информации / Л. К. Терещенко // Юридический консультант. – 2007. – № 9.

172. Терещенко Л. К. Доступ к информации: правовые гарантии / Л. К. Терещенко // Журнал российского права. – 2010. – №10 (166). – С. 46-53.

173. Топоркова, С. А. Разглашение охраняемой законом тайны как трудовое правонарушение / С. А. Топоркова // Трудовое право в России и за рубежом. – 2012. – №3.

174. Храпцовская, Н. Документы «Для служебного пользования» в электронном документообороте государственных органов // Делопроизводство и документооборот на предприятии. - 2011. – № 3. – С.45-53.

175. Чиканова, Л. А. Правовое регулирование служебных отношений на государственной гражданской службе: вопросы теории и практики / Л. А. Чиканова // Журнал российского права. – 2005. – № 4. – С. 67.

176. Шабанов, Д. С. Личная и семейная тайны в законодательстве Российской Федерации / Д. С. Шабанов // Право и государство. – 2010. – № 6. – С. 39-42.

177. Шавырина, А. С. Вопросы соотношения преступлений и смежных административных правонарушений / А. С. Шавырина // Пробелы в российском законодательстве. – 2010. – №1. – С. 256-260.

2.3. Литература на иностранных языках

178. Shils, E. The Torment of Secrecy: The Background & Consequences Of American Security Policies / E. Shills – Chicago: Dee. – 1956.

179. Security policy framework, April 2014. – (<https://www.gov.uk/government/publications/security-policy-framework>). – Дата обращения: 17.06.2017.

180. Executive Order 13526 of December 29, 2009 Classified National Security Information. – (<http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf>). – Дата обращения: 17.06.2017.

2.2. Диссертации, авторефераты

181. Антопольский, А. А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. ... канд. юрид. наук: 12.00.14 / А. А. Антопольский. Ин-т государства и права РАН. – М., 2004. – 29 с.

182. Бабелюк, Е. Г. Ответственность государственных служащих Российской Федерации: Административно-правовой аспект: дисс. ... канд.юрид.наук. 12.00.14 / Е. Г. Бабелюк. – СПб., 2005. – 203 с.

183. Бондарь, И. В. Тайна по российскому законодательству: Проблемы теории и практики: автореф. дис. ... канд. юрид. наук: 12.00.01 / Нижегород. акад. МВД России. – Нижний Новгород, 2004. – 27 с.

184. Волчинская, Е. К. Ограничение доступа к служебной информации: административно-правовые аспекты // магистерская диссертация. – Челябинск, 2014. – 180 с.

185. Горяева, Т. М. История советской политической цензуры, 1917-1991 гг.. автореф. дис. ... докт. ист. н. Спец. 07.00.02 / Горяева Т. М. – М., 2000. – 40 с.

186. Дворников, А. А. Уголовно-правовая охрана государственной и служебной тайны в органах внутренних дел: автореф. дисс.... канд. юрид. наук. / А. А. Дворников. – Тюмень, 2007. – 22 с.

187. Исмагилов, Р. Ф. Экономическая безопасность России: Теоретико-правовой анализ: дисс докт. юрид. Наук 12.00.01 / Р. Ф. Исмагилов. – Спб, 2000. – 424 с.

188. Клепиков, Н. Н. Политическая цензура на Европейском Севере РСФСР/СССР в 1920-1930-е гг.. автореф. дис. ... ист.н. 07.00.02 / Н. Н. Клепиков. – Архангельск. – 2005. – 28 с.

189. Левин, А. А. Приоритетные направления деятельности государства по обеспечению информационной безопасности

Российской Федерации: Политологический анализ: дисс. ... канд. полит. наук: 20.01.02. / А. А. Левин, – Москва, – 2004 – 150 с.

190. Минбалеев, А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества. дисс. ... докт. юрид. Наук. / Алексей Владимирович Минбалеев. – Челябинск, 2012. – 374 с.

191. Мирских, И. Ю. Коммерческая тайна как вид конфиденциальной информации: Трудоправовой и цивилистический аспекты: дис. ... канд. юрид. наук. / И. Ю. Мирских. – Пермь, 2005. – 207с.

192. Ожегов, С. И., Шведова, Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова. – 4-е изд., дополненное. – М.: Азбуковник, 1999. – 944 с.

193. Павленко, С. З. Безопасность Российского государства как политическая проблема: дисс. ... док. полит. Наук. / С. З. Павленко. – М., 1998. – 156 с.

194. Пермяков, М. В. Категория «тайна» в системе правового регулирования: Дис. ... канд. юрид. Наук: 12.00.01 / М. В. Пермяков. – Екатеринбург, 2006. – 234 с.

195. Полякова, Т. А. Информационная безопасность при построении информационного общества: Дисс. д.ю.н. / Т. А. Полякова.– М., 2008. – 438 с.

196. Радиков, И. В. Военная безопасность общества и государства: Политологический анализ: дисс. ... докт. полит. наук / И. В. Радиков. – Спб, 2000.

197. Салихов, И. И. Информация с ограниченным доступом как объект гражданских правоотношений: автореф. дис. ... канд. юрид. наук. / И. И. Салихов. – Казань, 2004. – С. 12-13.

198. Сандальникова, Е. В. Юридическая ответственность государственных гражданских служащих в Российской Федерации:

теоретико-правовое исследование: дисс. ... канд. юрид. наук: 12.00.01 / Е. В. Сандальникова. – Ульяновск, 2007. – 180 с.

199. Соколова, О. С. Административно-правовые режимы конфиденциальной информации: дисс. ... канд. юрид. Наук. 12.00.14 / Соколова О. С. – СПб., 2005. – 211 с.

200. Станскова, У. М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореферат дис. ... канд. юрид. наук: / У. М. Станскова. – Екатеринбург, 2014. – 24 с.

201. Сыроватская, Л. А. Материальная ответственность рабочих и служащих по советскому трудовому праву. автореф. дис. ... канд. юрид. наук / Сыроватская Л. А. – М., 1966. – 16 с.

202. Талапина, Э. В. Модернизация государственного управления в информационном обществе: информационно-правовое исследование. автореф. дисс. докт. юрид. наук. / Э. В. Талапина. – М., 2015. – 46 с.

203. Талапина, Э. В. Модернизация государственного управления в информационном обществе: информационно-правовое исследование: Дисс. докт. юрид. Наук. / Э. В. Талапина. – М., 2015. – 469 с.

204. Тедеев, А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей: автореф. ... дисс. докт. юрид. наук. / А. А. Тедеев. – М. 2007 – 58 с.

205. Терещенко, Л. К. Правовой режим информации. Автореф. ... дисс. докт. юрид. наук. / Л. К. Терещенко. – М. 2011. – 54 с.

206. Фролова, Н. А. Правовая политика Российской Федерации в сфере социальной безопасности: на опыте борьбы с наркотиками: автореф. дис. ... докт. юрид. наук: 12.00.01 / Н. А. Фролова. – М., 2009. – 48 с.

207. Чебышев-Дмитриев, А. О преступном действии по русскому допетровскому праву. / А. О. Чебышев-Дмитриев. – Казань: Тип. Имп. ун-та, 1862. – 246 с.

208. Чижик, П. И. Духовная безопасность российского общества как фактор военной безопасности государства: диссертация ... докт. фил. наук / П. И. Чижик. – М., 2000. – 408 с.

209. Швецов, А. В. Защита информации в сфере служебной тайны в деятельности ОВД: Правовой аспект.: дисс... канд.юрид. наук. 05.13.19 / А. В. Швецов. – Воронеж, 2005. – 189 с.

210. Щадрин, С. Ф. Уголовно-правовая охрана служебной тайны: автореф. дисс.... канд. юрид.наук. / С. Ф. Щадрин. – Ростов-на-Дону, 2002. – 28 с.

2.3. Судебная практика

211. Постановление Европейского Суда по правам человека от 10 декабря 2007 г. Дело «Штоль против Швейцарии» [Stoll v. Switzerland] (жалоба № 69698/01) (Большая Палата) // Бюллетень Европейского Суда по правам человека. Российское издание. № 6/2008

212. Постановление Европейского Суда по правам человека от 12 февраля 2008 г. Дело «Гуджа против Молдавии» [Guja v. Moldova] (жалоба № 14277/04) (Большая Палата) // Бюллетень Европейского Суда по правам человека. Российское издание. № 8/2008

213. Решение Верховного Суда РФ от 19.09.2011 № ГКПИ11-856 «Об оставлении без удовлетворения заявления о признании недействующим Приказа МВД РФ от 06.06.2000 № 605 ДСП «О мерах по совершенствованию деятельности органов внутренних дел по исполнению административного законодательства» // СПС «Консультант Плюс»

214. Определение ВАС РФ от 23.08.2012 № ВАС-10500/12 по делу № А27-12862/2011 //СПС «Консультант Плюс»

215. Определение Верховного Суда РФ от 10.11.1997 № 10-Г97-4 // СПС «Конкультант Плюс»

2.4. Интернет-ресурсы

216. Куренков, Г.А. Секретное делопроизводство ЦК (до Великой Отечественной войны). – <http://www.opentextnn.ru/history/deloproizvodstvo/?id=4897>). – Дата обращения 17.06.2017.

217. Кузнецов, П.У. Методологические проблемы информационного права: [выступление на] V Международной научно-практической конференции «Право и информация: вопросы теории и практики», 17 апреля 2015 г., Санкт-Петербург / Президентская библиотека, [Научный отдел]. – Санкт-Петербург: Президентская библиотека, 2015. – <http://www.prilib.ru/Lib/pages/item.aspx?itemid=133065>). – Дата обращения: 17.06.2017.

218. Погосова (Фролова), А.С. Инсайдерская и служебная информация: соотношение понятий. – http://www.juristlib.ru/book_9079.html). – Дата обращения: 17.06.2017.

219. Чертопруд, С. Организация защиты государственных секретов в МИДе Российской империи в период с 1903 по 1917 год. – <http://www.agentura.ru/press/cenzura/secret-russia/>). – Дата обращения: 17.06.2017.

220. Чертопруд, С. Зарождение и становление системы защиты государственной тайны в Советском Союзе с 1918 по 1930 год. – <http://www.agentura.ru/press/cenzura/secret-ussr/>). – Дата обращения: 17.06.2017.

221. Текст доклада депутата Христоса Пургуридиса, представленного в Парламентской Ассамблее Совета Европы 19 апреля 2007 г. Депутаты ПАСЕ. – <http://www.agentura.ru/dossier/russia/process/pace/>). – Дата обращения: 17.06.2017.

222. TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance – Version 1.0. – (<https://www.us-cert.gov/sites/default/files/tlp/tlp-v1.pdf>). – Дата обращения: 17.06.2017.

КОНЦЕПЦИЯ ФЕДЕРАЛЬНОГО ЗАКОНА О СЛУЖЕБНОЙ ТАЙНЕ

Статья 1. Сфера действия федерального закона

Федеральный закон регулирует отношения, возникающие в связи с отнесением информации к сведениям, охраняемым в режиме служебной тайны, установлением и снятием ограничений на доступ к указанным сведениям, охраной сведений в режиме служебной тайны, обеспечением доступа к указанным сведениям в целях обеспечения прав, свобод и законных интересов человека и гражданина, осуществления полномочий органов государственной власти и местного самоуправления в Российской Федерации.

Статья 2. Принципы правового регулирования

Ограничение доступа к информации должно основываться на следующих принципах:

- ограничение доступа к информации только на основании и в соответствии с федеральным законом;
- обоснованность ограничения доступа к информации;
- соблюдение прав и свобод человека и гражданина;
- надзор за ограничением доступа к информации;
- временный характер ограничения.

Статья 3. Используемые понятия

- Сведения, охраняемые в режиме служебной тайны.
- Служебная тайна.
- Система защиты служебной тайны.
- Отнесение сведений к служебной тайне.

– Нарушение требований режима служебной тайны.

Статья 4. Законодательство о служебной тайне

1. Регулирование отношений, связанных с служебной тайной осуществляется:

- 1) Конституцией Российской Федерации;
- 2) Федеральными законами, регулирующими отношения в сфере государственной и муниципальной службы;
- 3) настоящим Федеральным законом;
- 4) другими федеральными законами;
- 5) указами Президента Российской Федерации;
- 6) постановлениями Правительства Российской Федерации;
- 7) нормативными правовыми актами федеральных органов исполнительной власти;
- 8) Конституциями (уставами), законами и иными нормативными правовыми актами субъектов Российской Федерации;
- 10) нормативными правовыми актами органов местного самоуправления.

2. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, то применяются правила международного договора.

Статья 5. Сведения, охраняемые в режиме служебной тайны

Определить категории сведений, которые государственные органы и органы местного самоуправления вправе относить к сведениям, охраняемым в режиме служебной тайны. В перечень могут войти многие виды информации, ограничение доступа к которым установлено в настоящий момент федеральными законами. При интеграции указанных сведений в правовое регулирование режима служебной тайны, будут образованы две группы сведений: сведения, доступ к которым должен быть ограничен в обязательном

порядке (информация, полученная от граждан и организаций, составляющая тайну) и сведения, касающиеся деятельности органов государственной власти и местного самоуправления, доступ к которым ограничивается на основании решения руководителя государственного органа, органа местного самоуправления либо соответствующей организации.

Статья 6. Порядок отнесения сведений к служебной тайне

Отнесение информации к сведениям, охраняемым в режиме служебной тайны, осуществляется на основании перечней сведений, разрабатываемых государственными органами и иными организациями, которым предоставлено право отнесения сведений к режиму служебной тайны в соответствии с федеральным законом. Эти перечни должны размещаться на официальных сайтах соответствующих органов государственной власти, местного самоуправления, сайтах иных организаций, которым федеральным законом предоставлено право ограничение доступа к информации в режиме служебной тайны в сети Интернет. Указанные перечни подлежат пересмотру не реже, чем один раз в пять лет. Должностные лица, принявшие решение об отнесении сведений к служебной тайне, должны нести персональную ответственность за обоснованность решения отнесения или не отнесения информации к сведениям, охраняемым в режиме служебной тайны.

Статья 7. Меры защиты служебной тайны

Меры защиты служебной тайны включают в себя правовые, организационные, технические и иные меры. Меры защиты служебной тайны должны быть направлены на охрану сведений от неправомерного доступа, изменения, уничтожения, блокирования, копирования, распространения и иных неправомерных действий. В государственных органах, органах местного самоуправления и иных подведомственных организациях должны быть приняты нормативные акты, устанавливающие порядок работы с информацией, охраняемой в режиме служебной тайны, на федеральном

уровне должны быть установлены единые требования к информационным системам, используемым в органах государственной власти, местного самоуправления и иных подведомственных организациях. Ответственность за организационное и технологическое обеспечение режима служебной тайны несет руководитель соответствующего органа государственной власти, местного самоуправления или соответствующей организации.

Статья 8. Реквизиты сведений, охраняемых в режиме служебной тайны

Вне зависимости от вида носителя, содержащего сведения, охраняемые в режиме служебной тайны, он должен содержать указание «для служебного пользования», а также указание правообладателя (госорган/организацию, в которой было введено ограничение доступа к указанным сведениям).

Статья 9. Срок охраны сведений в режиме служебной тайны

Установить срок охраны сведений. При этом следует учитывать, что сведения, составляющие тайну третьих лиц, охраняются в течение срока, предусмотренного законодательством для соответствующего вида тайн.

Статья 10. Прекращение режима служебной тайны

Установить порядок снятия ограничения доступа к информации в режиме служебной тайны. Установить основания для досрочного пересмотра перечней информации ограниченного доступа. Определить порядок обжалования решения об ограничении доступа к той или иной информации в режиме служебной тайны по заявлению любого лица, в том числе лица, непосредственно осуществляющего работу со сведениями, охраняемыми в режиме служебной тайны, а также порядок рассмотрения указанного заявления как в административном, так и в судебном порядке.

Статья 11. Защита сведений при прохождении службы, в гражданских и трудовых отношениях

Необходимо закрепить в служебном контракте или трудовом договоре обязательства государственных и муниципальных служащих, иных работников государственного органа или органа местного самоуправления по сохранению конфиденциальности сведений, охраняемых в режиме служебной тайны. Установить сроки соблюдения этих обязательств, в том числе сроки после расторжения служебного контракта или трудового договора, в течение которых не допускается разглашение сведений, составляющих служебную тайну.

Статья 12. Доступ к сведениям, составляющим служебную тайну

Доступ предоставляется физическим лицам в целях обеспечения их прав, свобод и законных интересов. Ознакомление физических лиц с конкретными сведениями, составляющими служебную тайну, подлежит учету. Необходимо установить порядок учета этих фактов для органов исполнительной власти, для органов законодательной власти и для органов судебной системы.

Статья 13. Особенности доступа к сведениям, составляющим служебную тайну, в рамках гражданско-правовых отношений

В случае, когда исполнение договора на выполнение работ или оказание услуг предполагает доступ к сведениям, составляющим служебную тайну, договор должен включать положения, регламентирующие порядок обращения со сведениями, минимальные технические требования к безопасности системы защиты информации, гражданско-правовую ответственность за разглашение указанных сведений.

В случае, когда в ходе исполнения договора будут образовываться сведения, которые должны составлять служебную тайну, в договоре

необходимо предусмотреть перечень таких сведений, порядок проставления ограничительных надписей и их охраны.

Определить порядок передачи сведений и возможность приостановить выполнение договора заказчиком при нарушении исполнителем взятых на себя обязательств по охране служебной тайны.

Статья 14. Прокурорский надзор

Предусмотреть надзор за соблюдением законодательства в сфере служебной тайны, а также право доступа органов прокуратуры к любым сведениям, составляющим служебную тайну, на основании мотивированного запроса.

Статья 15. Ответственность за несоблюдение положений федерального закона

Несоблюдение положений федерального закона влечет наступление уголовной, административной, дисциплинарной и гражданско-правовой ответственности в соответствии с законодательством Российской Федерации.

Статья 16. Переходные положения

Установить сроки, в течение которых федеральные органы государственной власти должны утвердить Перечни сведений, составляющих служебную тайну, и решить вопрос об отнесении к служебной тайне сведений, содержащихся в документах, имеющих пометку «Для служебного пользования», нанесенную до вступления в силу федерального закона, а также привести в соответствие информационные системы, используемые в органах государственной власти. Установить срок, в течение которого государственные библиотеки совместно с федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации обязаны принять решение об отмене режима ограничения доступа к документам, имеющим пометку «Для служебного

пользования». Установить источники финансирования мероприятий по обеспечению информационной безопасности.

Статья 17. Вступление в силу федерального закона.

Не менее чем через один год со дня его официального опубликования.

	Налоговая тайна	Отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд	Сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния	Сведения, содержащиеся в личном деле и документах учета сотрудника органов внутренних дел, в реестре сотрудников органов внутренних дел, а также сведения о гражданах, поступающих на службу в органы внутренних дел	Сведения о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей
Основание ограничения доступа к информации	Ст.102 НК РФ; Закон РФ от 21.03.1991 N 943-1 "О налоговых органах Российской Федерации"	Статьи 51, 60, 66, 68 Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"	Ст. 12 ФЗ "Об актах гражданского состояния"	Статьи 39 и 40 Федерального закона от 30.11.2011 N 342-ФЗ "О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации"	Статья 23 Федерального закона от 03.07.2016 N 226-ФЗ "О войсках национальной гвардии Российской Федерации"
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	Налоговые органы, органы внутренних дел, следственные органы, органы государственного внебюджетного фонда и таможенные органы	Оператор электронной площадки	Работники органов записи актов гражданского состояния	Кадровые подразделения главных управлений, департаментов, управлений МВД России, Национального центрального бюро Интерпола МВД России, территориальных органов МВД России, образовательных, научных, медико-санитарных и санаторно-курортных организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел	Не определены конкретно
Правовое регулирование мер защиты информации и используемые информационные системы	Приказ Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@ "Об утверждении Концепции информационной безопасности Федеральной налоговой службы"	Используются 5 аккредитованных электронных торговых площадок, требования к которым указаны в Приказе Минэкономразвития России от 23.07.2015 N 495 "Об утверждении Порядка проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, Требованиям к операторам электронных площадок, к электронным площадкам, в том числе технологическим, программным, лингвистическим, правовым и организационным средствам, необходимым для проведения торгов в электронной форме по продаже	Информационные системы ЗАГС (требования к системам установлены ст. 14 Закона об информации, Постановлением Правительства РФ от 06.07.2015 N 676	Приказ МВД России от 28.04.2014 N 381 "О некоторых вопросах централизованного учета персональных данных сотрудников органов внутренних дел Российской Федерации, граждан Российской Федерации, поступающих на службу в органы внутренних дел Российской Федерации" (вместе с "Положением о централизованном учете персональных данных сотрудника органов внутренних дел Российской Федерации и ведении его личного дела", "Положением о централизованном учете персональных данных гражданина Российской Федерации, поступающего на службу в органы внутренних дел Российской Федерации")	Предусмотрена возможность создания информационных систем (пп.25 п. 9 ч. 2 Указ Президента РФ от 30.09.2016 N 510 "О Федеральной службе войск национальной гвардии Российской Федерации")
Ответственность за нарушение требований правового режима	Общие меры ответственности.	7.31.1 КоАП	Общие меры ответственности.	Общие меры ответственности	Общие меры ответственности.

	Сведения, содержащиеся в личном деле и документах учета сотрудника федеральной противопожарной службы	Сведения о несовершеннолетних, ставшие известными органам и учреждениям системы профилактики безнадзорности и правонарушений несовершеннолетних	Сведения о доходах, об имуществе и обязательствах имущественного характера, представляемые государственными и муниципальными служащими, а также иными лицами, указанными в части 1 статьи 8 Федерального закона от 25.12.2008 N 273-ФЗ
Основание ограничения доступа к информации	Статья 39 Федерального закона от 23.05.2016 N 141-ФЗ "О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации"	Статья 9 Федерального закона от 24.06.1999 N 120-ФЗ "Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних	Статья 8 Федерального закона от 25.12.2008 N 273-ФЗ "О противодействии коррупции"; Статья 20 Федерального закона от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации"; Статья 15 Федерального закона от 02.03.2007 N 25-ФЗ "О муниципальной службе в Российской Федерации";
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	Директор Департамента кадровой политики МЧС России, начальника Управления специальной пожарной охраны МЧС России, руководителей территориальных органов МЧС России и организаций МЧС России, являющихся самостоятельными юридическими лицами, - операторов.	Органы и учреждения системы профилактики безнадзорности и правонарушений несовершеннолетних; орган прокуратуры; комиссия по делам несовершеннолетних и защите их прав; органы опеки и попечительства; орган управления социальной защитой населения; орган внутренних дел; уголовно-исполнительные инспекции; орган управления здравоохранением; орган, осуществляющий управление в сфере образования; орган по делам молодежи	Органы государственной власти, местного самоуправления, публичные акционерные общества, корпорации, иные организации, создаваемые Российской Федерацией на основании федерального закона, организации, создаваемые для выполнения задач, поставленных перед федеральными государственными органами.
Правовое регулирование мер защиты информации и используемые информационные системы	На уровне проекта Приказа МЧС России "О некоторых вопросах централизованного учета персональных данных сотрудников федеральной противопожарной службы Государственной противопожарной службы, граждан Российской Федерации, поступающих на службу в федеральную противопожарную службу Государственной противопожарной службы"	Используемые информационные системы зависят от субъекта отношений, единые требования к безопасности конкретно указанной категории информации в свободном доступе отсутствуют	Используемые информационные системы зависят от конкретного субъекта, осуществляющего работу с указанной информацией, единые требования в свободном доступе отсутствуют
Ответственность за нарушение требований правового режима	Общие меры ответственности	Общие меры ответственности.	Общие меры ответственности.

	Сведения о расходах по приобретению земельного участка, другого объекта недвижимости, транспортного средства, ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций) и об источниках получения средств, за счет которых совершена сделка, представляемые лицами, замещающими (занимающими) одну из должностей, указанных в пункте 1 части 1 статьи 2 Федерального закона от 03.12.2012 N 230-ФЗ	Факт передачи в федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма информации,	Тайна усыновления	Информация, полученная в ходе проведения проверок российских участников внешнеэкономической деятельности
Основание ограничения доступа к информации	Статья 8 Федерального закона от 03.12.2012 N 230-ФЗ "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам"	Статья 7.1-1 Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"	Ст. 139 Семейного кодекса РФ	П. 8 ст. 17 ФЗ "Об экспортном контроле"
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	Федеральный государственный орган (подразделение федерального государственного органа), определяемый (определяемое) Президентом Российской Федерации; Подразделение кадровой службы федерального государственного органа по профилактике коррупционных и иных правонарушений (должностное лицо кадровой службы федерального государственного органа, ответственное за работу по профилактике коррупционных и иных правонарушений); Государственный орган субъекта Российской Федерации (подразделение государственного органа либо должностное лицо указанного органа, ответственное за работу по профилактике коррупционных и иных правонарушений), определяемый (определяемые) законами и иными нормативными правовыми актами субъекта Российской Федерации; Подразделение Банка России (уполномоченное должностное лицо Банка России), определяемое Банком России; Подразделения по профилактике коррупционных и иных правонарушений (должностные лица, ответственные за работу по профилактике коррупционных и иных правонарушений) государственной корпорации, Пенсионного фонда Российской Федерации, Фонда социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, иной организации, созданной Российской Федерацией на основании федеральных законов.	Организатор торговли, клиринговая организация и центральный контрагент	Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении	Должностные лица федеральных органов исполнительной власти, осуществляющих полномочия в области экспортного контроля
Правовое регулирование мер защиты информации и используемые информационные системы	Используемые информационные системы зависят от конкретного субъекта, осуществляющего работу с указанной информацией, единые требования в свободном доступе отсутствуют	Информация отсутствует. Порядок защиты конфиденциальности определяет непосредственно организатор торговли	Информационные системы ЗАГС (требования к системам установлены ст. 14 Закона об информации, Постановлением Правительства РФ от 06.07.2015 N 676	Используемые информационные системы не установлены, единые требования в свободном доступе отсутствуют
Ответственность за нарушение требований правового режима	Общие меры ответственности.	ст. 15.27 КоАП, ст. 174 УК РФ, 205.1 УК РФ	Ст. 155 УК РФ - Разглашение тайны усыновления.	Общие меры ответственности.

	Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, сведения, содержащиеся в планах обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств, информационные ресурсы единой государственной информационной системы обеспечения транспортной безопасности	Сведения, составляющие дактилоскопическую информацию	Сведения о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, поступающие в финансовые органы от органов Федерального казначейства	Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц в системе обязательного пенсионного страхования	Информация о получателе социальных услуг
Основание ограничения доступа к информации	Статьи 5, 9, 11 Федерального закона от 09.02.2007 N 16-ФЗ "О транспортной безопасности"	Статья 12 Федерального закона от 25.07.1998 N 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации"	Статья 241 Бюджетного кодекса РФ	Статья 6 Федерального закона от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования"	Статья 6 Федерального закона от 28.12.2013 N 442-ФЗ "Об основах социального обслуживания граждан в Российской Федерации"
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	Субъекты транспортной инфраструктуры, специализированные организации в области обеспечения транспортной безопасности, компетентные органы в области обеспечения транспортной безопасности	Государственные органы исполнительной власти, указанные в ст. 11, 14 ФЗ "О государственной дактилоскопической регистрации в РФ"	Финансовые органы, получающие от органов Федерального казначейства сведения о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках	Руководители, а также должностные лица органов Пенсионного фонда Российской Федерации, участвующие в соответствии с настоящим Федеральным законом в сборе, хранении, передаче и использовании сведений, содержащихся в индивидуальных лицевых счетах застрахованных лиц	Лица, которым эта информация стала известна в связи с исполнением профессиональных, служебных и (или) иных обязанностей.
Правовое регулирование мер защиты информации и используемые информационные системы	ст. 11 ФЗ "О транспортной безопасности", ст. 14 Закона об информации. - единая государственная информационная система.	Приказ МВД РФ N 688, МЧС РФ N 472, Министра обороны РФ N 1214, Минфина РФ N 110н, Минюста РФ N 235, Минтранса РФ N 205, СВР РФ N 36, ФТС РФ N 1785, ФСБ РФ N 456, ФСО РФ N 468, ФСКН РФ N 402, ФМС РФ N 299 от 27.09.2010 "Об утверждении Положения о порядке формирования и ведения информационного массива, создаваемого в процессе проведения государственной дактилоскопической регистрации"	Используется ГИС ГМП. Приказ Казначейства России от 30.11.2012 N 19н "Об утверждении Порядка ведения Государственной информационной системы о государственных и муниципальных платежах" не предусматривает отдельную регламентацию мер информационной безопасности и соблюдения конфиденциальности некоторых данных.	Используется АИС ПФР	Приказ Минтруда России от 25.07.2014 N 485н "Об утверждении рекомендаций по формированию и ведению регистра получателей социальных услуг"+ Закон "О персональных данных"
Ответственность за нарушение требований правового режима	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.

	Сведения, содержащиеся в Федеральной государственной информационной системе учета результатов проведения специальной оценки условий труда	Сведения, ставшие известными судебным приставам в связи с исполнением должностных обязанностей	Информация, представляемая заинтересованным лицом в орган, проводящий расследования в целях принятия решения о целесообразности введения, применения, пересмотра или отмены специальной защитной меры, антидемпинговой меры или компенсационной меры	Информация о членах политической партии, представляемая для сведения в уполномоченные органы	Сведения о населении, содержащиеся в переписных листах
Основание ограничения доступа к информации	Статья 18 Федерального закона от 28.12.2013 N 426-ФЗ "О специальной оценке условий труда"	Статья 4 Федерального закона от 21.07.1997 N 118-ФЗ "О судебных приставах"	Статья 32 Федерального закона от 08.12.2003 N 165-ФЗ "О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров"	Статья 19 Федерального закона от 11.07.2001 N 95-ФЗ "О политических партиях"	Статья 8 Федерального закона от 25.01.2002 N 8-ФЗ "О Всероссийской переписи населения"
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере труда, подведомственная ему федеральная служба и координируемые им государственные внебюджетные фонды, а также федеральный орган исполнительной власти, осуществляющий функции по организации и осуществлению федерального государственного санитарно-эпидемиологического надзора, органы исполнительной власти субъектов Российской Федерации в области охраны труда и страховщиками	Судебные приставы	Орган, проводящий расследование	Уполномоченные органы (Минюст, избирательные комиссии)	Лица, которые имеют доступ к сведениям о населении, содержащимся в переписных листах,
Правовое регулирование мер защиты информации и используемые информационные системы	Приказ Минтруда России от 03.11.2015 N 843н "Об утверждении Порядка формирования, хранения и использования сведений, содержащихся в Федеральной государственной информационной системе учета результатов проведения специальной оценки условий труда"	Используется АИС ФССП	Используемые информационные системы не установлены, единые требования в свободном доступе отсутствуют	Используемые информационные системы не установлены, единые требования в свободном доступе отсутствуют	Требования к защите конфиденциальности предусмотрены в ст. 8 Федерального закона от 25.01.2002 №8-ФЗ "О Всероссийской переписи населения"
Ответственность за нарушение требований правового режима	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.

	Сведения, содержащиеся в переписных листах об объектах сельскохозяйственной переписи	Первичные статистические данные, содержащиеся в формах федерального статистического наблюдения	Сведения, содержащиеся в заявках на участие в конкурсе на право заключить контракт на проведение лотерей	Сведения, ставшие известными уполномоченному по правам человека в процессе рассмотрения жалобы о частной жизни лица, подавшего жалобу, и других лиц без их письменного согласия	Данные предварительного расследования
Основание ограничения доступа к информации	Статья 12 Федерального закона от 21.07.2005 N 108-ФЗ О Всероссийской сельскохозяйственной переписи"	Статья 9 Федерального закона от 29.11.2007 N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в Российской Федерации"	Статья 24.10 Федеральный закон от 11.11.2003 N 138-ФЗ "О лотереях	Статья 16.1 Федерального закона от 06.10.1999 N 184-ФЗ "Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации"	Ст. 161 УПК РФ
Субъекты, на которые возложена обязанность по обеспечению конфиденциальности информации	Должностные лица государственных органов, органов местного самоуправления, организаций, а также иные лица, которые в силу своего служебного положения или рода осуществляемой деятельности имели доступ к содержащимся в переписных листах сведениям об объектах сельскохозяйственной переписи	федеральные органы государственной власти, иные федеральные государственные органы, Центральный банк Российской Федерации (Банк России), осуществляющие формирование официальной статистической информации в установленной сфере деятельности в соответствии с законодательством Российской Федерации	Участники размещения заказа, подавшие заявки на участие в конкурсе, организатор лотереи, Лица, осуществляющие хранение конвертов с заявками на участие в конкурсе и заявок на участие в конкурсе, поданных в форме электронных документов,	Уполномоченные по правам человека	Органы, ведущие предварительное расследование, а также участники уголовного судопроизводства
Правовое регулирование мер защиты информации и используемые информационные системы	Требования к защите конфиденциальности предусмотрены в ст. 12 Федерального закона от 21.07.2005 N 108-ФЗ О Всероссийской сельскохозяйственной переписи"	Центральная база статистических данных (ЦБСД) Банк готовых документов (БГД)	Используемые информационные системы прямо не установлены. Только требования к конфиденциальности	Прямо не установлены. Только требования к конфиденциальности	Используется АИС ОПС. В законодательстве требование конфиденциальности
Ответственность за нарушение требований правового режима	Общие меры ответственности.	Общие меры ответственности.	Общие меры ответственности.+ СТ. 7.31.1 КоАП РФ	. Общие меры ответственности.	Общие нормы об ответственности+ ст. 310 УК РФ.