

Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

На правах рукописи

Силкин Владислав Валерьевич

**ПРАВОВОЙ СТАТУС ГОСУДАРСТВЕННЫХ ОРГАНОВ
ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ
(СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ)**

5.1.2 – Публично-правовые (государственно-правовые) науки

Диссертация на соискание учёной степени

кандидата юридических наук

Научный руководитель:

Богдановская Ирина Юрьевна,
доктор юридических наук, профессор

Москва - 2023

ОГЛАВЛЕНИЕ

<u>ВВЕДЕНИЕ.....</u>	<u>3</u>
<u>ГЛАВА 1. СИСТЕМА ОРГАНОВ ПУБЛИЧНОЙ ВЛАСТИ, РЕГУЛИРУЮЩИХ ИНФОРМАЦИОННУЮ СФЕРУ</u>	<u>16</u>
1.1. МЕСТО ГЛАВЫ ГОСУДАРСТВА И ПРАВИТЕЛЬСТВА В РЕГУЛИРОВАНИИ ИНФОРМАЦИОННОЙ СФЕРЫ.....	20
1.1.1. РОЛЬ АППАРАТОВ ГЛАВЫ ГОСУДАРСТВА И ПРАВИТЕЛЬСТВА В РЕГУЛИРОВАНИИ ИНФОРМАЦИОННОЙ СФЕРЫ.....	27
1.2. МИНИСТЕРСТВА И ИНЫЕ ВЕДОМСТВА	45
1.3. ОРГАНЫ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ СУБЪЕКТОВ ФЕДЕРАТИВНЫХ ГОСУДАРСТВ В ИНФОРМАЦИОННОЙ СФЕРЕ	58
<u>ГЛАВА 2. ПОЛНОМОЧИЯ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ</u>	<u>68</u>
2.1. НОРМОТВОРЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ.....	69
2.2. ОКАЗАНИЕ ГОСУДАРСТВЕННЫХ УСЛУГ	93
2.3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ	108
2.4. ПРИМЕНЕНИЕ МЕР АДМИНИСТРАТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ.....	116
<u>ГЛАВА 3. ПРАВОВЫЕ МОДЕЛИ РЕГУЛИРОВАНИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА.....</u>	<u>130</u>
3.1. ЗАКОНОДАТЕЛЬСТВО ОБ ЭЛЕКТРОННОМ ПРАВИТЕЛЬСТВЕ.....	130
3.2. ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО В ЭПОХУ ЦИФРОВЫХ ПЛАТФОРМ	139
3.3. ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ОБМЕНА ДАННЫМИ	152
3.4. ГОСУДАРСТВЕННАЯ ЭЛЕКТРОННАЯ ИДЕНТИФИКАЦИЯ.....	161
<u>ЗАКЛЮЧЕНИЕ</u>	<u>174</u>
<u>СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ</u>	<u>180</u>
<u>ПРИЛОЖЕНИЕ. ПРЕДЛАГАЕМЫЕ ИЗМЕНЕНИЯ В ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 09.02.2009 № 8-ФЗ «ОБ ОБЕСПЕЧЕНИИ ДОСТУПА К ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ»</u>	<u>219</u>

ВВЕДЕНИЕ

Актуальность темы исследования.

В постиндустриальную эпоху информационные технологии становятся неотъемлемой частью общественных отношений. Появляются различные способы автоматизированной обработки информации, что способствует развитию оборота данных.

Научно-технологический прогресс влияет на деятельность органов исполнительной власти в Российской Федерации, приводит к переходу органов исполнительной власти на электронный документооборот и реестровую модель оказания государственных услуг.

Усиливается роль цифровых платформ в общественных отношениях. Органы исполнительной власти создают цифровые платформы, обеспечивающие эффективное оказание государственных услуг в электронной форме и электронных государственных услуг. Переход к платформенному подходу позволяет государству выступать гарантом надежности при реализации иных правовых отношений в электронной форме.

Хотя совершенствуется взаимодействие невластных субъектов информационных отношений с государственными органами, органы исполнительной власти получают возможность сбора большего количества информации, необходимой для прогнозирования и планирования. Внедрение новых технологий для сбора и анализа информации требует дополнительного правового регулирования, по-новому ставит вопрос о развитии правового института открытости информации о деятельности органов исполнительной власти.

Другим направлением развития регулирования деятельности органов исполнительной власти в России является информационная безопасность. В отличие от узкого понятия кибербезопасности, более распространенного в зарубежной литературе, информационная безопасность включает в себя не только

вопросы предотвращения кибератак, но также регулирование негативного информационного воздействия на общество и личность в целом. Данный вопрос актуален как для России, так и для зарубежных стран.

Для реагирования на происходящие изменения расширяется компетенция органов исполнительной власти. Российский подход основан на укрупнении полномочий органов, регулирующих информационную сферу, и усилении централизации. В зарубежных странах система органов исполнительной власти в информационной сфере может развиваться в других направлениях.

Сходства и различия в развитии правового статуса государственных органов исполнительной власти в информационной сфере в России и зарубежных странах позволяют, во-первых, определить особенности российского подхода, во-вторых, учесть зарубежный опыт при формировании национального правового регулирования.

Степень научной разработанности темы и теоретическая основа исследования.

Теоретической основой диссертационного исследования являются работы ученых юристов в России и за рубежом по вопросам правового регулирования деятельности органов исполнительной власти.

Работы Б.М. Лазарева, М.И. Пискотина, Б.П. Курашвили, В.Г. Вишнякова, И.Л. Бачило, Ю.М. Козлова, Г.В. Атаманчука послужили основой для исследования вопросов государственного управления.

Значимую роль в теоретическом осмыслении особенностей правового регулирования деятельности органов исполнительной власти сыграли работы российских и советских авторов. Отдельные вопросы административного принуждения были рассмотрены в работах М.И. Еропкина, Ю.С. Рябова, А.Е. Лунева, Г.И. Петрова, Д.Н. Бахраха. Теория органов управления развивалась в исследованиях В.М. Манохина, Ц.А. Ямпольской, Ю.А. Тихомирова, И.Л. Бачило. Стоит также выделить сравнительные исследования в сфере деятельности публичной администрации М.А. Штатиной. Анализ компетенции агентств США проведен в работах Р. Пирса младшего, П. Веркюля (Verkuil), А. Вермюля

(Vermeule), Е. Каган, К.Р. Санстейна, Д. Валдо. При анализе французского права теоретической базой послужили работы Ж. Риверо, Ж. Валин, а в части вопросов правового статуса независимых административных ведомств - Ж. Шевалье, Ж.Л. Отан (Autin).

Фундаментальные вопросы правового регулирования информационной безопасности подробно изложены в работах Т.А. Поляковой, В.Н. Лопатина. Отдельным аспектам информационной безопасности посвящены работы А.В. Туликова, М.С. Журавлева. Информационно-правовые аспекты обеспечения государственного суверенитета в сети Интернет подробно проанализированы А.А. Ефремовым.

Отдельные вопросы правового регулирования деятельности органов исполнительной власти в информационной сфере рассмотрены в работах российских исследователей. Э.В. Талапиной¹ исследованы основные направления модернизации государственного управления. Административно-правовые аспекты регулирования информационных технологий в деятельности органов исполнительной власти проанализированы Н.Н. Ковалевой².

Положения об электронном государстве и публичных услугах раскрываются в работах И.Л. Бачило, И.Ю. Богдановской, Н.Н. Ковалевой, Н.А. Данилова, Е.Г. Иншаковой. Сравнительный юридический анализ права на доступ к информации государственных органов представлен А.С. Агеевым³.

В работе Л.К. Терещенко изложены фундаментальные теоретические основания правового режима информации⁴, которые определяют терминологический аппарат исследования отдельных элементов правового статуса государственных органов исполнительной власти.

¹ Талапина Э.В. Модернизация государственного управления в информационном обществе: автореф. дис. ... д.ю.н. Москва, 2015.

² Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении: автореф. дис. ... д.ю.н. Саратов, 2014.

³ Агеев А.С. Право на доступ к информации, находящейся в распоряжении государственных органов (особенности конституционно-правового регулирования в России и в Германии): автореф. дис. ... к.ю.н. Москва, 2016.

⁴ Терещенко Л.К. Правовой режим информации: дис. ... д.ю.н. Москва, 2011.

Отдельные разновидности правовых режимов информации также получили рассмотрение в работах российских исследователей. Исследованию теоретических основ соотношения транспарентности и режима тайны, смешанных режимов информации, посвящена работа Д.И. Гунина⁵. Общие теоретические положения о категории тайны получили свое рассмотрение у М.В. Пермякова⁶. Обоснование понятия тайны и выделение отдельных режимов тайн были проведены И.В. Бондарем⁷. Правовому режиму информации ограниченного доступа, обоснованию понятия информационного объекта посвящена работа А.А. Антопольского⁸. Отдельные разновидности тайн также рассматривались в российской юридической науке⁹.

В контексте рассмотрения проблем формирования государственных систем электронной идентификации, использования электронной подписи необходимо отметить работы зарубежного исследователя С. Мэйсона¹⁰, российских авторов - А.И. Савельева, В.Б. Наумова.

При проведении сравнительного исследования используется теория правовых семей, развитая в работе Р. Давида.

Методология исследования.

Общенаучные методы использованы для обобщения материала и анализа. Системный метод позволил обобщить результаты исследования, проанализировать взаимосвязи исследуемых правовых институтов. Дедуктивный метод позволил на основе общих положений выделить конкретные случаи их применения. Индуктивный метод позволил соотнести конкретные правовые

⁵ Гунин Д.И. Транспарентность и тайна информации: теоретико-правовой аспект: автореф. дис. ... к.ю.н. Екатеринбург, 2008.

⁶ Пермяков М.В. Категория «тайна» в системе правового регулирования: дис. ... к.ю.н. Екатеринбург, 2006.

⁷ Бондарь И.В. Тайна по российскому законодательству (Проблемы теории и практики): дис. ... к.ю.н. Н. Новгород, 2004.

⁸ Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: дис. ... к.ю.н. Москва, 2004.

⁹ См. напр.: Потапов Н.А. Правовое регулирование коммерческой тайны в Российской Федерации: автореф. дис. ... к.ю.н. Москва, 2010; Жирнова Н.А. Банковская и налоговая тайны как объекты финансово-правового регулирования: автореф. дис. ... к.ю.н. Саратов, 2013.

¹⁰ Mason S. Electronic Signatures in Practice // J. High Tech L. 2006. Issue 148. P. 149–164.

явления с теоретическими положениями о регулировании деятельности органов исполнительной власти в информационной сфере.

Среди юридических методов необходимо отметить формально-юридический метод, используемый для анализа норм позитивного права.

В ходе исследования используется метод сравнительного правоведения. Для сравнения были выбраны страны со сложившейся правовой традицией из различных правовых семей. В качестве представителя правовой семьи общего права исследуются США, для которых характерны активное развитие вопросов электронного правительства и поиск новых моделей государственного управления. В рамках континентально-правовой семьи в работе анализируется право Франции как страны с развитой системой административного права. Сопоставление развития схожих правовых институтов в России, Франции и США направлено на поиск общих направлений развития регулирования информационной сферы органами исполнительной власти. Предложенные в результате сравнения изменения в российское законодательство учитывают особенности национальной правовой системы, основаны на выявленных общих тенденциях и не исходят из преимущества какой-либо одной правовой системы над другой. В исследовании также учитывается опыт и других зарубежных стран, представляющий интерес в рамках сравнительного анализа отдельных вопросов.

Выбранная методология сравнительного исследования позволяет охарактеризовать сходства и различия в подходах к правовому регулированию информационной сферы, проанализировать развивающиеся российские правовые институты в сравнении с зарубежным опытом. Результатом проводимого сравнительного исследования является новое знание об объектах сравнения (правовых институтах), которое выражается в предложении изменений в национальное законодательство либо в обособлении объектов сравнения по определенному признаку (выделении моделей).

Используемая при сравнении терминология подобрана исходя из сопоставимости инородных терминов и понятий зарубежных стран с российскими. Устоявшиеся общеупотребимые термины российской правовой науки

используются для описания сравниваемого объекта без анализа либо дополнения указанных понятий.

В российской юридической науке получил развитие системно-функциональный метод анализа органов исполнительной власти¹¹. Значение указанного метода для правовых исследований состоит в определении компетенций и особенностей организации системы органов исполнительной власти.

В ходе исследования был использован также исторический метод для более углубленного рассмотрения особенностей развития анализируемых органов исполнительной власти и правовых институтов в исследуемых странах.

Эмпирическую базу исследования составляют действующие и утратившие силу законы и подзаконные акты, правовые акты органов исполнительной власти рассматриваемых стран, судебная практика, проекты нормативно-правовых актов.

Научная новизна работы состоит в комплексном сравнительном исследовании ключевых особенностей развития системы и компетенции российских и зарубежных органов исполнительной власти в информационной сфере, в результате которого:

- выявлены и проанализированы тенденции к централизации и децентрализации в системе органов исполнительной власти, регулирующих информационную сферу;
- разработана классификация видов координации в регулировании информационной сферы;
- определена правовая природа мер административного принуждения в информационной сфере;
- выявлены правовые особенности внедрения платформенного подхода в государственное управление.

¹¹ Атаманчук Г.В. Теория государственного управления: учебник. М., Омега-Л, 2010. С. 154–165; Бахрах Д.Н., Россинский Б.В., Стариков Ю. Н. Административное право: Учебник для вузов. 2-е изд., изм. и доп. М.: Норма, 2005. С. 38–43; Сорокин Д.С. Реформирование системы и структуры федеральных органов исполнительной власти Российской Федерации: автореферат дис. ... к.ю.н. Москва, 2004.

Объект исследования: деятельность органов исполнительной власти, направленная на регулирование информационной сферы или определяемая ее развитием.

Предмет исследования: законы и подзаконные акты, регулирующие деятельность государственных органов исполнительной власти в информационной сфере, судебная и административная практика, научные, аналитические и статистические материалы о деятельности органов исполнительной власти.

Цель исследования: углубить теоретические положения об отдельных элементах правового статуса органов исполнительной власти в информационной сфере с учетом зарубежного опыта и на основе проведенного исследования разработать научно обоснованные предложения по совершенствованию российского правового регулирования.

Задачи исследования:

проанализировать особенности организации системы органов исполнительной власти в информационной сфере и их место в системе органов публичной власти в России и за рубежом;

исследовать изменение отдельных полномочий органов исполнительной власти в информационной сфере в России и за рубежом;

проанализировать подходы к формированию законодательства в сфере электронного правительства в различных странах;

выявить основные подходы к регулированию электронного обмена данными органами исполнительной власти и формирования системы государственной электронной идентификации;

исследовать правовые проблемы использования органами исполнительной власти государственных и частных цифровых платформ.

Основные научные положения, выносимые на защиту:

1. Выявлено, что развитие регулирования информационной сферы сопровождается усилением централизации системы органов исполнительной власти в указанной сфере. Централизация осуществляется путем: расширения аппарата правительства и главы государства (в зависимости от формы правления)

для координации развития электронного правительства (Россия, Франция, США, Сингапур); учреждения профильных министерств, участвующих в регулировании информационной сферы (Россия, Индия, Сингапур, Китай); централизованного развития электронного правительства на местном и региональном уровне (Россия, Франция).

2. Обосновано, что действующий правовой режим открытости информации о деятельности органов исполнительной власти не позволяет обеспечить информированность граждан о целях и результатах использования новых технологий в государственном управлении. В связи с чем сделан вывод, что использование органами исполнительной власти технологий искусственного интеллекта в пределах их компетенции должно быть ограничено публично объявленными целями с обязательным опубликованием отчета о результатах использования ими цифровых технологий, достижении поставленных целей и выявленных недостатков их использования.

3. Проведенное сравнение регулирования полномочий органов исполнительной власти в сфере информационной безопасности показывает, что эффективной формой согласования интересов и обмена информацией являются совещательные органы, объединяющие должностных лиц органов исполнительной власти, ответственных за информационную безопасность. Совещательные органы могут содействовать формированию стандартов в сфере информационной безопасности с учетом опыта различных органов исполнительной власти.

4. На основе анализа развития мер административного принуждения в информационной сфере в России и Франции сделан вывод о целесообразности выделения мер административного информационного воздействия в качестве отдельного вида мер административного принуждения, поскольку: 1) регулирование применения указанных мер целесообразно осуществлять обособленно в рамках информационного законодательства в силу схожести их процедур; 2) отмечена тенденция к увеличению видов таких мер, что требует их единой законодательной классификации.

Выявлены общие для России и Франции меры административного информационного воздействия: 1) ограничение доступа к информационному ресурсу; 2) запрет на поисковую выдачу; 3) информирование пользователей операторами поисковых систем о нарушении законодательства на информационном ресурсе.

5. Выявлено, что в зависимости от сложившейся правовой традиции, определяющей целесообразность обособления электронного правительства в качестве отдельного правового института, в ряде стран приняты законы, регулирующие электронное правительство (США, Италия, Германия, Австрия). В других странах законодательство, регулирующее деятельность органов исполнительной власти, лишь дополняется отдельными нормами об электронном правительстве (Россия, Франция, Швеция), что способствует более комплексному развитию сложившихся правовых институтов в информационной сфере.

6. Выявлено, что развитие сетевых связей в государственном управлении путем использования частных и государственных цифровых платформ органами исполнительной власти осуществляется на основе сочетания частного и публичного правовых методов регулирования деятельности органов исполнительной власти. Предложено предоставить Правительству Российской Федерации полномочия по определению условий использования органами исполнительной власти учетных записей частных цифровых платформ, что позволит быстрее адаптировать регулирование с учетом нового функционала частных цифровых платформ.

7. Проведенное сравнение позволяет заключить, что организация электронного обмена данными органов исполнительной власти (Россия, Франция, США) может осуществляться путем заключения органами исполнительной власти соглашений об информационном взаимодействии либо в рамках предоставления информации о деятельности органов исполнительной власти.

Соглашения об информационном взаимодействии могут заключаться как для исполнения обязанности органа исполнительной власти по подключению к единой информационной инфраструктуре (Россия), так и по усмотрению органа

исполнительной власти для электронного обмена данными в пределах его полномочий (Франция, США, Россия).

Предложено закрепить в российском законодательстве полномочия органов исполнительной власти по предоставлению данных заинтересованному лицу за плату при необходимости проведения дополнительной аналитической работы, а также предоставить органу исполнительной власти возможность ограничить использование полученной информации заинтересованным лицом на основании отдельного соглашения. Предложенные изменения изложены в приложении.

8. Определено право на цифровую идентичность как право лица в случаях, предусмотренных в законодательстве, требовать от органа исполнительной власти – оператора информационной системы – обеспечения возможности для использования уникальных идентификационных данных такого лица для целей его идентификации или аутентификации в государственных и негосударственных информационных системах.

Теоретическая значимость исследования состоит в выделении нескольких уровней координации для анализа разграничения полномочий между различными органами исполнительной власти; формировании теоретических основ и введении понятия мер административного информационного воздействия в качестве отдельной разновидности мер административного принуждения; выявлении тенденций развития системы органов исполнительной власти в информационной сфере в России и за рубежом. Результаты работы могут быть использованы при проведении других исследований в сфере публичного права.

Практическая значимость исследования обусловлена разработкой правовых подходов и предложений, призванных решить сложившиеся проблемы правового регулирования и правоприменения, осуществляемыми органами исполнительной власти в информационной сфере. Результаты исследований также могут быть использованы в учебных курсах образовательных программ бакалавриата и магистратуры.

Достоверность и апробация результатов исследования

Отдельные результаты и аспекты исследования отражены в пяти публикациях из перечня ВАК, из которых три опубликованы в изданиях, рекомендованных НИУ ВШЭ (список D):

- Силкин В.В., Данилов Н.А. Правовое регулирование доступа к информации пользователя сети Интернет после его смерти: сравнительно-правовое исследование // Журнал зарубежного законодательства и сравнительного правоведения. 2021. Т. 17. № 1. С. 86–101;

- Силкин В.В. Исключения из принципа открытости информации о деятельности государственных органов // Вестник Воронежского государственного университета. Серия: Право. 2021. № 2 (45). С. 164–171;

- Силкин В.В. Транспарентность исполнительной власти в цифровую эпоху // Российский юридический журнал. 2021. № 4 (139). С. 20–31.

Иные публикации в изданиях перечня ВАК:

- Силкин В.В. Права собственника при использовании изображения его имущества: французский опыт // Журнал Суда по интеллектуальным правам. 2020. № 2 (28). С. 53–56;

- Силкин В.В. Пределы отказа в предоставлении доступа к информации о деятельности государственных и муниципальных органов // Правовая политика и правовая жизнь. 2021. № 3 (84). С. 275–281.

Отдельные особенности электронной идентификации, осуществляемой в публично-правовой сфере, были также рассмотрены в публикациях, не входящих в перечень ВАК и списки изданий НИУ ВШЭ:

- Силкин В.В. Электронная идентификация юридических лиц и органов публичной власти // Право в цифровую эпоху. Материалы секции молодых исследователей V Международной научно-практической конференции. М.: 2016. С. 121–126;

- Силкин В.В. Электронная идентичность в информационном праве: сравнительно-правовой аспект // Право. Гражданин. Общество. Экономика: сборник статей аспирантов, магистров и студентов. Выпуск 10. М.: Проспект, 2017. С. 352–358.

Отдельные результаты исследования были также представлены на конференциях, круглых столах и летних школах:

- Совместный круглый стол НОЦ «Право и СМИ» Юридического факультета Московского государственного университета им. М.В. Ломоносова, посвященный вопросам защиты цифровой репутации. 2023 год. Доклад: «Административный порядок защиты цифровой репутации»;

- Международная конференция студентов, аспирантов и молодых учёных «Ломоносов-2022». Доклад: «Практика органа по защите персональных данных (в России, Франции и США)»;

- XXVIII Международная конференция студентов, аспирантов и молодых учёных «Ломоносов» (Москва). 2021. Доклад: «Транспарентность использования органами исполнительной власти систем автоматизированной обработки данных».

- VIII International summer school on cyber law. 2019. Доклад на англ. яз.: «Public Sector Information: Openness and its Limitations».

Результаты исследования также использовались соискателем в рамках работы стажером-исследователем в различных подразделениях факультета права НИУ ВШЭ:

- Участие в написании научно-исследовательской работы «Исследование зарубежного опыта правового регулирования управления данными, формирование предложений по совершенствованию правового регулирования управления данными для Российской Федерации» в рамках реализации мероприятий по созданию национальной системы управления данными в рамках федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации»;

- Участие в написании разделов об идентификации и безопасности в сфере телемедицины в рамках проекта «Комплексное правовое регулирование перспективных направлений цифровой экономики»¹².

¹² URL: <https://www.hse.ru/org/projects/408455784> (дата обращения: 12.06.2023).

Результаты проведенного исследования были использованы соискателем и в образовательном процессе в ходе ведения предметов «Цифровое право», «Право и информационная безопасность» в Лицее НИУ ВШЭ, «Правовая грамотность», «Управление интеллектуальной собственностью» (на английском) - для студентов НИУ ВШЭ.

ГЛАВА 1. СИСТЕМА ОРГАНОВ ПУБЛИЧНОЙ ВЛАСТИ, РЕГУЛИРУЮЩИХ ИНФОРМАЦИОННУЮ СФЕРУ

В литературе сложились разные подходы к пониманию правового статуса как в общетеоретическом смысле¹³, так и в отдельных отраслевых науках. В юридических исследованиях правового статуса государственных органов зачастую анализируется система органов и компетенция¹⁴. В отдельных исследованиях вместо полномочий рассматриваются формы и методы деятельности соответствующих органов¹⁵ либо функции органов исполнительной власти¹⁶.

Наиболее близким и наиболее полным отраслевым термином для описания правового статуса органа исполнительной власти целесообразно считать его административно-правовой статус. По справедливому замечанию В.М. Манохина правовой статус субъекта административных отношений образуют его полномочия¹⁷. Ю.Н. Старилов определяет правовой статус как совокупность прав, свобод, гарантий, обязанностей, правоограничений и объема ответственности¹⁸. Более широкий подход предлагает Н.Ф. Попова, выделяя в составе правового статуса органа исполнительной власти три группы элементов: компетенцию; место органа в системе органов государственной власти; особенности формирования

¹³ Редких С.В. Понятие правового статуса: формально-правовой контекст. Пробелы в российском законодательстве // Юридический журнал. 2009. № 3. С. 42–44.

¹⁴ Напр.: Пилия Д.Э. Правовой статус органов исполнительной власти Республики Абхазия: дис. ... к.ю.н. Москва, 2010; Бочарников Ю.Ф. Конституционно-правовой статус органов административной юстиции Италии: дис. ... к.ю.н. Москва, 2007; Злобин А.В. Общая характеристика органов государства с особым правовым статусом // Вестник Саратовской государственной военной юридической академии. 2014. № 6. С. 66–71.

¹⁵ Ганя Д.В. Административно-правовой статус органов государственного управления Республики Молдова: дис. ... к.ю.н. Москва, 1999.

¹⁶ Аялутдинов Ф.М. Конституционно-правовой статус органов исполнительной власти в Российской Федерации: дис. ... к.ю.н. Москва, 2001.

¹⁷ Манохин В.М. Административное право России: учебник. Саратов: Ай Пи Эр Медиа, 2011. С. 33.

¹⁸ Бахрах Д. Н., Российский Б. В., Старилов Ю. Н. Административное право: Учебник для вузов. 2-е изд., изм. и доп. М.: Норма, 2005. С. 121.

структуры и штата органа исполнительной власти, процедур и методов его деятельности¹⁹.

Не только изменения в компетенции и системе органов исполнительной власти определяют их правовой статус в информационной сфере. По справедливому замечанию Ю.А. Тихомирова «информация – живая ткань управления»²⁰. Информационная сфера является как отдельным объектом государственного управления, так и непосредственно условием реализации органами исполнительной власти возложенных на них полномочий. В связи с чем изменения, происходящие в информационной сфере, влияют на правовой статус органов исполнительной власти, определяя особенности их деятельности.

Для сравнительного исследования целесообразно выделить такие элементы правового статуса органов исполнительной власти в информационной сфере, в отношении которых может быть проведено сопоставление с зарубежным опытом. Кроме того, некоторые элементы правового статуса органов исполнительной власти не обладают отдельной спецификой в информационной сфере²¹. Поэтому в рамках проводимого исследования целесообразно выделить те элементы правового статуса органов исполнительной власти, которые относятся к информационной сфере.

Правовое определение информационной сферы в российском праве дано в действующей Доктрине информационной безопасности, утвержденной Указом Президента Российской Федерации от 05.12.2016 г. № 646²². Предложенное определение информационной сферы охватывает технологии передачи

¹⁹ Попова Н. Ф. Правовое обеспечение государственного и муниципального управления: учебник и практикум для вузов / под общей редакцией Г. Ф. Ручкиной. Москва: Издательство Юрайт, 2023. С. 85.

²⁰ Тихомиров Ю.А. Научная организация управления. М.: Сов. Россия, 1973. С. 71.

²¹ Например, вопрос ответственности органов исполнительной власти за действия в информационной сфере должен рассматриваться в более широком контексте, безотносительно отдельной сферы государственного регулирования. Частично указанный вопрос рассмотрен во втором параграфе последней главы в контексте имущественной ответственности публично-правовых образований.

²² Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: <http://kremlin.ru/acts/bank/41460/page/1> (дата обращения: 05.03.2023).

информации, информационные ресурсы, субъектов информационных отношений и правовые механизмы регулирования информационных отношений. Такое определение отражает субъективный подход к понятию информационной сферы, характеризующий ее в качестве деятельности людей по обработке доступной для их восприятия информации.

В правовой литературе информационная сфера определяется также как доступное для познания объективно выраженное состояние информации²³, что характеризует информационную сферу именно с точки зрения теории информации и опосредует объективный подход. Информационная сфера в рамках объективного подхода определяется в качестве обособленной и независимой от деятельности людей совокупности информации.

Оба подхода представляются верными. С одной стороны, информационная сфера характеризует все источники выражения информации в целом. С другой стороны, к информационной сфере относится и деятельность людей, включая использование информационных технологий, по обработке и управлению информацией.

Регулирование информационной сферы затрагивает всю систему публичной власти в государстве в целом. С принятием поправок к Конституции Российской Федерации в 2020 году термин публичной власти получил новое рассмотрение в правовой литературе. Публичная власть характеризует деятельность органов различных ветвей власти, а также иных государственных органов, не входящих ни в одну из ветвей власти²⁴. Деятельность же, непосредственно связанную с осуществлением государственного управления в узком смысле, осуществляют органы исполнительной власти²⁵.

²³ Информационное право: учебник / Бачило И.Л. 4-е изд., перераб. и доп. М.: Юрайт, 2016. С. 131.

²⁴ Публичная власть: система, компетенции: монография / под общ. ред. М.Н. Кобзарь-Фроловой; отв. ред. И.В. Глазунова. Воронеж: Издательско-полиграфический центр «Научная книга», 2021. С. 35.

²⁵ В литературе встречается и более широкий термин публичной администрации как «организации и деятельности органов и учреждений, подчиненных политической власти, обеспечивающих исполнение закона, действующих в публичных интересах и наделенных прерогативами публичной власти». Публичная администрация является одним из коллективных

Конституционный подход к пониманию системы публичной власти свидетельствует об усилении централизации в системе государственного управления, возрастании потребности в координации деятельности органов на различных уровнях публичной власти. Однако он не исключает необходимости распределения компетенций между различными органами публичной власти, позволяющего учесть как общегосударственные интересы, так и потребности местного населения в информационной сфере²⁶.

Организация системы органов исполнительной власти для регулирования информационной сферы характеризуется распределением компетенций на различных уровнях как по вертикали, так и по горизонтали. Усиление внимания государства к регулированию информационной сферы приводит к укреплению роли центральных органов исполнительной власти в организации управления информационной сферой на нижестоящих уровнях и усилению централизации в системе органов публичной власти в информационной сфере в целом.

В юридической науке общепризнан факт необходимости выделения управленческих функций для распределения компетенции отдельных органов исполнительной власти²⁷. По мере развития государства перед ним ставятся новые задачи, возникают новые функции, которые приводят к увеличению объема компетенции государственных органов²⁸ либо к учреждению новых органов.

субъектов осуществления публичной власти в государстве, осуществляющим непосредственное управленческое воздействие на информационную сферу. Однако ключевую роль в деятельности публичной администрации играют органы исполнительной власти. Козырин А.Н., Глушко Е.К., Штатина М.А. Публичная администрация и административные реформы в зарубежных странах: учеб. пособие. Гос. ун-т - Высш. шк. экономики. М.: ТЕИС, 2006. С. 9.

²⁶ В.Е. Чиркин справедливо отмечал, что публичная власть реализуется путем сочетания союза и состязательности в территориальном коллективе. См.: Чиркин В.Е. Публичная власть. М.: Юристъ, 2005. С. 33.

²⁷ См. Ямпольская Ц.А. Органы советского государственного управления в современный период / Отв. ред.: Коток В.Ф. М.: Изд-во АН СССР, 1954. С. 11; Лазарев Б.М. Компетенция органов управления. М.: Юрид. лит., 1972. С. 29; Тихомиров Ю.А. Теория компетенции. М.: Юстицинформ, 2001. С. 43.

²⁸ Тихомиров Ю.А. Указ. соч. С. 39.

Указанный подход был использован в том числе при реформировании системы исполнительных органов Российской Федерации в начале 2000-х²⁹ и сохраняет свою актуальность в свете обсуждения новых реформ системы исполнительной власти³⁰.

Однако предлагаемые классификации управленческих функций различаются. Некоторые исследователи выделяют ряд управленческих функций по способам осуществления государственного управления (Б.М. Лазарев³¹, Ю.Н. Старилов³², И.Л. Бачило³³). Другие исследователи предлагали разные основания классификации управленческих функций (Г.В. Атаманчук³⁴, Б.П. Курашвили³⁵, М.И. Пискотин³⁶).

Для сравнительного анализа более подходит классификация управленческих функций по способам управления.

1.1. Место главы государства и правительства в регулировании информационной сферы

Значимую роль в государственном управлении информационной сферой играют глава государства и правительство. Они выполняют функции прогнозирования, планирования и координации политики государства в информационной сфере. Роль главы государства и его взаимоотношения с исполнительной властью определяются формой правления.

²⁹ Напр.: Сорокин Д.С. Реформирование системы и структуры федеральных органов исполнительной власти Российской Федерации: автореферат дис. ... к.ю.н. Москва, 2004.

³⁰См.: Калинин А. О реформировании системы и структуры органов исполнительной власти в РФ // Общество и экономика. 2019. № 5. С. 78-86; Зверев М.А. Тенденции развития административной реформы на примере реформирования системы федеральных органов исполнительной власти // Бизнес, менеджмент и право. 2020. № 3 (47). С. 57-63.

³¹ Лазарев Б.М. Компетенция органов управления. М.: Юрид. лит., 1972. С. 32 – 38.

³² Бахрах Д.Н., Российский Б. В., Старилов Ю.Н. Административное право: Учебник для вузов. 2-е изд., изм. и доп. М.: Норма, 2005. С. 39–40.

³³ См.: Бачило И.Л. Функции органов управления. М., 1976.

³⁴ Атаманчук Г.В. Теория государственного управления: учебник. М.: Омега-Л, 2010. С. 158–161.

³⁵ Курашвили Б.П. Очерк теории государственного управления / отв. ред.: Пискотин М.И. М.: Наука, 1987. С. 174–189.

³⁶ Государственное управление в СССР в условиях научно-технической революции / Отв. ред. М. И. Пискотин. М.: Наука, 1978. С. 34–39.

В рамках регулирования информационной сферы сравнительное исследование не показывает возникновения каких-либо новых полномочий глав государства и правительства. Сложившиеся в соответствующей стране полномочия лишь конкретизируются в рамках соответствующего направления информационной сферы.

В Российской Федерации Президент не входит в систему исполнительной власти и координирует взаимодействие всех государственных органов власти различного уровня³⁷. Глава государства определяет политику развития государства в различных направлениях, включая сферу научно-технологического развития, а также информационную сферу. Такие полномочия предоставлены ему частью 3 статьи 80 Конституции Российской Федерации³⁸. К примеру, глава государства в своих обращениях часто отмечает необходимость развития цифровых платформ и новых технологий в государственном управлении³⁹. Определение политики осуществляется главой государства в тесном взаимодействии с различными государственными органами с учетом взаимодействия различных политических сил в государстве и общественной реакции на обозначенные главой государства направления его политики⁴⁰.

Президент определяет структуру органов исполнительной власти по предложению Председателя Правительства Российской Федерации⁴¹. Органы исполнительной власти могут учреждаться в ведении Правительства Российской Федерации или в ведении главы государства. Распределение подведомственности

³⁷ Бондарец Е.Б. Конституционно-правовой статус главы государства в системе власти современной России: автореф. дис. ... к.ю.н. Москва, 2014. 27 с.

³⁸ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: <http://publication.pravo.gov.ru/Document/View/0001202007040001> (дата обращения: 05.03.2023).

³⁹ Тасс. Путин считает, что нужно вывести на качественно новый уровень эффективность управления. 16.03.2023. URL: <https://tass.ru/ekonomika/17284875> (дата обращения - 12.05.2023); РБК. Путин призвал сделать Россию одним из мировых центров «больших данных». 01.03.2018. URL: <https://www.rbc.ru/rbcfreeneews/5a97d1bd9a79476b19eab85c> (дата обращения - 12.05.2023)

⁴⁰ Бархатова Е.Ю. Комментарий к Конституции Российской Федерации: новая редакция (постатейный). 3-е изд., перераб. и доп. М.: Проспект, 2020.

⁴¹ Указ Президента РФ от 21.01.2020 № 21 «О структуре федеральных органов исполнительной власти» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 346.

происходит на основании части 2 статьи 12 Федерального конституционного закона от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации»⁴². В частности, к ведению главы государства отнесены органы исполнительной власти в сфере обороны и безопасности, внутренних и иностранных дел, юстиции. Деятельность указанных органов определяет и регулирование информационной сферы в части обеспечения информационной безопасности и государственного суверенитета в сети Интернет.

Президент определяет направления регулирования сферы информационной безопасности личности, общества и государства⁴³. Для целей определения политики в сфере информационной безопасности в Российской Федерации главой государства утверждены Доктрина информационной безопасности Российской Федерации⁴⁴, определившая основные цели и задачи развития системы информационной безопасности в России⁴⁵, Стратегия национальной безопасности⁴⁶, а также дополнительные акты, конкретизирующие отдельные направления развития системы информационной безопасности⁴⁷.

Во Франции как смешанной республике, в отличие от Российской Федерации, руководство исполнительной властью осуществляется совместно Премьер-министром и Президентом. Их взаимодействие осуществляется в Совете

⁴² Федеральный конституционный закон от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» // Собрание законодательства РФ, 09.11.2020, № 45, ст. 7061.

⁴³ Колосова Н.М., Колосов К.М. Президент Российской Федерации как гарант информационной безопасности личности // Журнал российского права. 2020. № 4. С. 17–27.

⁴⁴ Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: <http://kremlin.ru/acts/bank/41460/page/1> (дата обращения: 05.03.2023).

⁴⁵ Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. № 8 (224). С. 100–109; Гриценко В.В. Доктрина информационной безопасности Российской Федерации: сущность, современное значение и организационно-правовые основы // Вестник ВГУ. Серия: Право. 2017. №1 (28). С. 78–88.

⁴⁶ Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 05.03.2023).

⁴⁷ Указ Президента Российской Федерации от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». URL: <http://www.kremlin.ru/acts/news/69810> (дата обращения: 05.03.2023).

министров, где председательствует глава государства. На заседаниях Совета министров рассматриваются и акты главы государства – его декреты и ордонансы.

В сфере информационной безопасности глава государства, как и в России, председательствует на советах и комитетах по национальной безопасности (статья 15 Конституции Франции). Во Франции стратегия национальной безопасности определялась главой государства в «белых книгах»⁴⁸, а позже в обзорах⁴⁹. Вопросы кибербезопасности рассматриваются главой государства в совокупности всей системы направлений развития национальной безопасности в целом.

В США как президентской республике глава государства осуществляет руководство исполнительной властью. Содействие в реализации его политики главе государства оказывает аппарат Президента⁵⁰. Глава государства как определяет политику развития отдельных направлений в информационной сфере в целом, так и дает более конкретные поручения федеральным агентствам в части информатизации и информационной безопасности. В частности, Президентом США за период 2020–2022 годов приняты исполнительные указы и меморандумы как в целом в сфере организации системы национальной информационной безопасности⁵¹, так и по отдельным направлениям: в сфере обеспечения

⁴⁸ Livre blanc sur la défense et la sécurité nationale. Le 13 juillet 2012. URL: <http://www.livreblancdefenseetsecurite.gouv.fr/index.html> (дата обращения: 05.03.2023).

⁴⁹ Revue nationale stratégique 2022, présentée le mercredi 9 novembre par le Président de la République. URL: http://www.sgdsn.gouv.fr/communiqués_presse/revue-nationale-strategique-2022/ (дата обращения: 05.03.2023).

⁵⁰ Чепус А. В. Организация работы Правительства в России и США // Право и современные государства. 2012. № 3. С. 30-38.

⁵¹ Memorandum on Renewing the National Security Council System. February 4, 2021. URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system/> (дата обращения: 05.03.2023); Executive Order on Improving the Nation's Cybersecurity. May 12, 2021. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> (дата обращения: 05.03.2023); Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. January 19, 2022. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/> (дата обращения: 05.03.2023).

безопасности данных американских граждан⁵², а также в сфере обеспечения национальной безопасности при использовании цифровых активов⁵³.

В 2023 году Президентом США была утверждена Национальная стратегия кибербезопасности⁵⁴ — результат усиления политики в указанной сфере. Среди стратегических направлений выделяются как изменения в регулировании деятельности агентств по обеспечению информационной безопасности, так и необходимость уменьшения рисков кибербезопасности в частном секторе. Политика кибербезопасности определяется и политическим курсом соответствующего Президента США. В частности, политика Б. Обамы предполагала меньшую роль органов безопасности в обеспечении кибербезопасности США, отдавая предпочтение демократическим ценностям. В период Д. Трампа политика изменилась, а роль органов безопасности стала возрастать⁵⁵. Намечившийся курс на усиление регулирования вопросов кибербезопасности продолжил развитие и в период Дж. Байдена.

Однако есть и различия между политикой Дж. Байдена и Д. Трампа в информационной сфере. В частности, изначально в 2019 году определенная Д. Трампом политика развития искусственного интеллекта была сосредоточена на достижении эффективности внедрения технологий⁵⁶, в то время как с приходом к

⁵² Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries. June 9, 2021. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/> (дата обращения: 05.03.2023).

⁵³ Executive Order on Ensuring Responsible Development of Digital Assets. March 9, 2022. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (дата обращения: 05.03.2023).

⁵⁴ National Cybersecurity Strategy. March 2023. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> (дата обращения: 05.03.2023).

⁵⁵ Lonergan E.D., Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation // Journal of Cybersecurity. Volume 9. Issue 1. 2023. URL: <https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988> (дата обращения: 05.05.2023).

⁵⁶ Executive Order 13859 of February 11, 2019. Maintaining American Leadership in Artificial Intelligence. URL: <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence> (дата обращения: 05.03.2023); Executive Order 13960 of December 3, 2020. Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. URL: <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government> (дата обращения: 05.03.2023).

власти Дж. Байдена акцент сменился в сторону необходимости уважения прав человека в рамках развития искусственного интеллекта⁵⁷.

Следует отметить, что в парламентских республиках (Индия, Сингапур) глава государства не играет значимой роли в определении политики в информационной сфере и координации развития информационных технологий в деятельности органов исполнительной власти. В Сингапуре реализация электронного правительства осуществляется премьер-министром как главой исполнительной власти⁵⁸.

В смешанных республиках (Франция, Россия) правительство участвует в регулировании информационной сферы совместно с главой государства.

Правительство Российской Федерации обеспечивает реализацию государственной политики в информационной сфере, определенной главой государства, осуществляет руководство подведомственными ему органами исполнительной власти и координацию органов исполнительной власти в ведении главы государства. В свою очередь Правительство утверждает программные документы по отдельным направлениям информационной сферы: например, в части мер, направленных на обеспечение технологического суверенитета⁵⁹, обеспечения информационной безопасности детей⁶⁰.

⁵⁷ Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public. October 04, 2022. URL: <https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/> (дата обращения: 05.03.2023).

⁵⁸ Пехтерева Е.А. Электронное правительство Сингапура // Экономические и социальные проблемы России. 2015. № 2. С. 107–125.

⁵⁹ Постановление Правительства Российской Федерации от 15.04.2023 № 603 «Об утверждении приоритетных направлений проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации и Положения об условиях отнесения проектов к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации, о представлении сведений о проектах технологического суверенитета и проектах структурной адаптации экономики Российской Федерации и ведении реестра указанных проектов, а также о требованиях к организациям, уполномоченным представлять заключения о соответствии проектов требованиям к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации». URL: <http://static.government.ru/media/files/8JsiO5kSItJA1g5IHhGd5qiQVACelECn.pdf> (дата обращения: 05.05.2023).

⁶⁰ Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28.04.2023 № 1105-р). URL:

Правительство готовит законопроекты для регулирования информационной сферы. В Плане законопроектной деятельности Правительства на 2023 год цифровизация выделена в отдельное направление, для которого предусмотрена подготовка трех законопроектов профильными министерствами в информационной сфере⁶¹.

Правительство также самостоятельно принимает соответствующее подзаконное регулирование в разных направлениях информационной сферы. Оно определяет порядок строительства и эксплуатации линий связи⁶², порядок подготовки и использования единой сети электросвязи⁶³, правила присоединения к сетям электросвязи⁶⁴, утверждает порядок регулирования и правила оказания услуг связи. Указанная сфера требует постоянного обсуждения в условиях меняющихся отношений. В связи с этим на обсуждения была вынесена Стратегия связи, направленная на обеспечение технологического суверенитета страны в условиях санкций⁶⁵.

Во Франции полномочия Премьер-министра шире, чем в России, однако для обеих стран свойственно перераспределение полномочий между правительством и президентом. Национальная политика определяется и реализуется Правительством

<http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf> (дата обращения: 05.05.2023).

⁶¹ План законопроектной деятельности Правительства Российской Федерации на 2023 год (утв. Распоряжением Правительства Российской Федерации от 23.12.2022 № 4112-р). URL: <http://static.government.ru/media/files/ON30zFKdZXJwOeXlaJRB62ID4uu8trDE.pdf> (дата обращения: 05.03.2023).

⁶² Статья 9 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» // Российская газета, № 135, 10.07.2003.

⁶³ Постановление Правительства РФ от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» // Собрание законодательства РФ, 17.06.2019, № 24, ст. 3099.

⁶⁴ Постановление Правительства РФ от 21.01.2022 № 29 «Об утверждении Правил присоединения сетей электросвязи и их взаимодействия и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации» // Собрание законодательства РФ, 31.01.2022, № 5, ст. 763.

⁶⁵ Дмитрий Чернышенко: Разработка стратегии отрасли связи на базе современных и надёжных решений позволит России обеспечить свой технологический суверенитет. URL: <http://government.ru/news/48031/> (дата обращения: 16.05.2023). Дата опубликования: 18.03.2023.

Франции (статья 20 Конституции Франции⁶⁶). Премьер-министр отвечает за национальную безопасность (статья 21 Конституции Франции), реализуя намеченные главой государства направления политики. Премьер-министр определяет требования к безопасности информационных систем операторов жизненной важности⁶⁷, определяет порядок одобрения продуктов в сфере безопасности и надежных поставщиков услуг в сфере безопасности⁶⁸.

Сравнительный анализ показывает развитие регулирования в пределах сложившихся полномочий отдельных аспектов информационной сферы главой государства и правительством, которые представляют отдельный интерес для государственной политики в целом: информационная безопасность, электронное правительство, внедрение систем искусственного интеллекта в деятельность органов исполнительной власти. В смешанных республиках (Россия, Франция) регулирование информационной сферы осуществляется в совместном взаимодействии главы государства и правительства. Если президент определяет направления развития государственной политики в информационной сфере, правительство обеспечивает их реализацию по отдельным направлениям регулирования информационной сферы.

1.1.1. Роль аппаратов главы государства и правительства в регулировании информационной сферы

Необходимость решения новых управленческих задач в условиях развития информационной сферы ведет к расширению аппаратов глав государств и правительств.

⁶⁶ Constitution du 4 octobre 1958. URL: <https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095822> (дата обращения: 05.03.2023).

⁶⁷ Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405967> (дата обращения: 05.03.2023).

⁶⁸ Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405903> (дата обращения: 05.03.2023).

В Российской Федерации глава государства самостоятельно определяет структуру своего аппарата. В его аппарате действуют как подразделения, осуществляющие информационное сопровождение деятельности главы государства в целом, так и иные подразделения, содействующие главе государства уже в определении и реализации государственной политики в информационной сфере.

В целом в Администрации Президента России действует несколько управлений, обеспечивающих его технологическое и информационное сопровождение.

Например, в Управлении делами Президента в качестве структурного подразделения учреждено Управление информационных и коммуникационных технологий, отвечающее за технологическое сопровождение главы государства и его аппарата, осуществляющее в этой связи контроль над деятельностью Федерального государственного унитарного предприятия «Главный научно-исследовательский вычислительный центр» Управления делами Президента Российской Федерации⁶⁹.

Информационное обеспечение деятельности главы государства и оповещение о направлениях его деятельности осуществляет Управление прессы и информации Президента Российской Федерации⁷⁰. Если указанное управление отвечает преимущественно за организацию мероприятий с участием главы государства, то предложения по опубликованию новостей о деятельности главы государства оно осуществляет во взаимодействии с Управлением Президента Российской Федерации по общественным связям и коммуникациям, учрежденном главой государства для содействия в реализации государственной информационной политики в целом, в том числе путем сбора информации о

⁶⁹ Управление информационных и коммуникационных технологий. URL: <https://udprf.ru/content/upravlenie-informacionnyh-i-kommunikacionnyh-tehnologii> (дата обращения: 05.03.2023).

⁷⁰ Указ Президента РФ от 18.06.2012 № 874 «Об утверждении Положения об Управлении прессы и информации Президента Российской Федерации» // Собрание законодательства РФ, 25.06.2012, № 26, ст. 3497.

мнениях о проведении государственной политики в различных сферах и координации информационной работы федеральных органов исполнительной власти⁷¹.

Для целей содействия главе государства в реализации государственной политики в области цифровых технологий Президентом учреждено Управление Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи⁷², в задачи которого входит как подготовка предложений по вопросам цифровизации государственного управления, так и реализация этих предложений. Представители Администрации Президента содействуют главе государства в реализации его политики и подготовке документов, в том числе участвуют в реализации государственной политики совместно с представителями органов исполнительной власти⁷³.

Помимо Администрации Президента, содействие в его реализации государственной политики в информационной сфере осуществляют и иные органы.

В частности, в 2018 году был создан Совет при Президенте по стратегическому развитию и национальным проектам⁷⁴, утвердивший паспорт национальной программы «Цифровая экономика» в 2019 году⁷⁵. До 2019 года

⁷¹ Указ Президента Российской Федерации от 18.06.2012 № 876 «Об Управлении Президента Российской Федерации по общественным связям и коммуникациям» // Собрание законодательства РФ от 2012 г., № 26, ст. 3498.

⁷² Указ Президента Российской Федерации от 14.06.2018 № 334 «О мерах по оптимизации структуры Администрации Президента Российской Федерации» (вместе с «Положением об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи») // Собрание законодательства РФ, 18.06.2018, № 25, ст. 3646.

⁷³ Протокол заседания совета по вопросам распространения социальной рекламы в информационно-телекоммуникационной сети «Интернет» от 22.12.2022. URL: <https://digital.gov.ru/ru/documents/8623/> (дата обращения: 05.03.2023).

⁷⁴ Указ Президента РФ от 19.07.2018 № 444 «Об упорядочении деятельности совещательных и консультативных органов при Президенте Российской Федерации» (вместе с Положением о Совете при Президенте Российской Федерации по стратегическому развитию и национальным проектам) // Собрание законодательства РФ, 23.07.2018, № 30, ст. 4717.

⁷⁵ Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). URL: <http://government.ru/info/35568/> (дата обращения: 05.03.2023).

предыдущие национальные программы («Электронная Россия», «Информационное общество») утверждались Правительством РФ⁷⁶.

С изменением Конституции Российской Федерации в 2020 г. в Российской Федерации был конкретизирован правовой статус Государственного Совета Российской Федерации. В правовой литературе, посвященной Государственному Совету, уже отмечается его рассмотрение в качестве координационного органа⁷⁷, а также общее расширение его полномочий⁷⁸. Государственный Совет, объединяя множество различных представителей публичной власти и позволяя согласовать единые позиции по вопросам внешней и внутренней политики, исходя из различных интересов на разных уровнях власти⁷⁹, в будущем сможет занять новое главенствующее место в качестве органа, определяющего общие направления цифровизации государственного управления и цифровой экономики в системе публичной власти в целом.

В составе Государственного Совета в соответствии с Указом Президента Российской Федерации от 21.12.2020 № 800 «Вопросы Государственного Совета Российской Федерации»⁸⁰ сформированы следующие комиссии по социально-экономическим направлениям, деятельность которых затрагивает регулирование информационной сферы: комиссия по направлению «Государственное и муниципальное управление», комиссия по направлению «Коммуникации, связь,

⁷⁶ Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)» // Собрание законодательства РФ, 04.02.2002, № 5, ст. 531; Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // Собрание законодательства РФ", 05.05.2014, № 18 (часть II), ст. 2159.

⁷⁷ Михеева Т.Н. Государственный Совет Российской Федерации: история и современность // Государственная власть и местное самоуправление. 2021. N 4. С. 51–55.

⁷⁸ Алпаткина Е.С. Государственный Совет Российской Федерации: мифы и реальность // Государственная власть и местное самоуправление. 2021. N 5. С. 55–60.

⁷⁹ Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти». Москва: Норма, ИНФРА-М, 2020.

⁸⁰ Указ Президента Российской Федерации от 21.12.2020 № 800 «Вопросы Государственного Совета Российской Федерации». URL: <http://publication.pravo.gov.ru/Document/View/0001202012210077?index=0&rangeSize=1> (дата обращения: 05.03.2023).

цифровая экономика». Наиболее активную деятельность на период 2021–2022 годов, однако, ведут комиссии другой направленности – например, по направлениям «Энергетика», «Наука»⁸¹.

Для содействия Президенту Российской Федерации в определении и реализации политики информационной безопасности действует Совет безопасности⁸². Совет безопасности содействует главе государства в реализации его политики, в том числе в соответствии с его обращениями⁸³. В его составе учреждена Межведомственная комиссия по информационной безопасности⁸⁴, которая обеспечивает сбор информации об особенностях реализации мер информационной безопасности в различных отраслях и федеральных округах России⁸⁵. Председателем комиссии является заместитель Секретаря Совета безопасности. В комиссии участвуют как представители различных федеральных министерств и ведомств, так и представители крупных компаний и государственных корпораций.

Таким образом, для реализации полномочий главы государства в определении и реализации государственной политики в информационной сфере в аппарате Президента Российской Федерации действуют различные органы. Регулирование информационной сферы осуществляется путем взаимодействия отдельных управлений Администрации Президента Российской Федерации,

⁸¹ Новости Государственного Совета Российской Федерации. URL: <http://www.kremlin.ru/events/state-council/page/2> (дата обращения: 05.03.2023).

⁸² Пункт ж) статьи 83 Конституции Российской Федерации; статья 13 Федерального закона «О безопасности» от 28.12.2010 № 390-ФЗ // Российская газета, № 295, 29.12.2010; Указ Президента РФ от 07.03.2020 № 175 «О некоторых вопросах Совета Безопасности Российской Федерации» (вместе с Положением о Совете Безопасности Российской Федерации, Положением об аппарате Совета Безопасности Российской Федерации) // Собрание законодательства РФ, 09.03.2020, № 10, ст. 1323.

⁸³ Напр.: Президент РФ. О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства. 20 мая 2022 года. URL: <http://www.scrf.gov.ru/council/session/3241/> (дата обращения: 05.03.2023).

⁸⁴ Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (утверждено Указом Президента РФ от 06.05.2011 № 590) // Собрание законодательства РФ, 09.05.2011, № 19, ст. 2721.

⁸⁵ Состоялось заседание Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности. URL: <http://www.scrf.gov.ru/news/allnews/3476/> (дата обращения: 05.03.2023). Дата опубликования: 19.04.2023.

Государственного Совета Российской Федерации и Совета безопасности Российской Федерации.

Во Франции глава государства также, как и Президент России, определяет структуру своего аппарата самостоятельно, однако правовой статус его аппарата не закрепляется в законодательстве, что отличает французский подход. Аппарат главы государства состоит из назначаемых должностных лиц, ответственных за различные направления. В составе аппарата главы государства (секретариата Президента Франции) Президентом учреждено несколько должностей, которые могут отвечать за регулирование информационной сферы⁸⁶: советник в сфере индустрии, исследований, инноваций и цифровизации; советник по публичной деятельности и цифровизации; специальный советник по коммуникации и стратегии⁸⁷. Указанные лица участвуют в подготовке документов главы государства. В частности, в рамках осуществления своих полномочий глава государства может давать поручения Премьер-министру и иным министрам, обеспечивающие политическую координацию цифровизации государственного управления⁸⁸. Указанные поручения также готовятся аппаратом главы государства.

Президент Франции также председательствует в Совете национальной безопасности, определяющем общие направления развития безопасности в государстве, включая информационную безопасность⁸⁹.

⁸⁶ Секретариат Президента Франции не урегулирован законодательством и формируется по собственному усмотрению главы государства. Полномочия советников и иных должностных лиц, входящих в аппарат Президента Франции также не установлены законодательством.

⁸⁷ Cabinet du Président de la République. URL: <https://www.elysee.fr/la-presidence/cabinet-du-president-de-la-republique-et-services-de-l-elysee> (дата обращения: 05.03.2023).

⁸⁸ Напр.: Intervention du Président de la République à l'occasion de la convention managériale de l'Etat. URL: <https://www.elysee.fr/emmanuel-macron/2021/04/08/intervention-du-president-de-la-republique-emmanuel-macron-a-loccasion-de-la-convention-managériale-de-letat> (дата обращения: 05.03.2023).

⁸⁹ Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000021542333/2010-01-13/> (дата обращения: 05.03.2023).

С развитием информационной сферы и в структуре аппарата Президента США увеличивается количество органов, ответственных за реализацию государственной политики в разных областях информационной сферы. Однако в отличие от смешанных республик, в США структурные единицы аппарата главы государства осуществляют одновременно и координационные функции в отношении федеральных исполнительных агентств, а также независимых агентств (в случаях, предусмотренных законом).

В отличие от России и Франции, в США глава государства вправе назначать руководителей органов по совету и с согласия Сената. Нижестоящие руководители отдельных агентств (*inferior officers*) могут назначаться главой государства без согласования Сената на основании закона⁹⁰, который может устанавливать дополнительные критерии к соответствующей должности⁹¹. Глава государства может сменить руководителя или изменить направление его политики, однако не может изменить функции, возложенные на соответствующий орган законом. В результате принятия множества законов для регулирования информационной сферы в аппарате главы государства учреждаются различные органы, функции которых могут совпадать (в частности, такая тенденция наблюдается в сфере информационной безопасности).

Ключевую роль в регулировании деятельности федеральных агентств в информационной сфере играют агентства, образованные в составе Административно-бюджетного управления (*Office of management and budget*) Исполнительного офиса (*Executive office*) Президента США.

⁹⁰ Article II, section 2, USA Constitution: «...shall appoint Ambassadors, other public Ministers and Consuls, Judges of the supreme Court, and all other Officers of the United States, whose Appointments are not herein otherwise provided for, and which shall be established by Law: but the Congress may by Law vest the Appointment of such inferior Officers, as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments». URL: <https://www.archives.gov/founding-docs/constitution-transcript> (дата обращения: 05.03.2023).

⁹¹ Volokh H.M. The Two Appointments Clauses: Statutory Qualifications for Federal Officers // *Journal of Constitutional Law*. 2008. Vol. 10. № 4. P. 745–789.

Наиболее значимым в регулировании деятельности федеральных агентств в целом является Управление вопросов информации и регулирования (OIRA)⁹², координирующее нормотворческую деятельность агентств, включая независимые агентства, в пределах, установленных законом, а также отвечающее за защиту приватности в деятельности агентств. Получая проект нормативного акта, управление запрашивает информацию у других агентств и таким образом координирует интересы всей разветвленной системы органов исполнительной власти США при издании нормативных актов, а также осуществляет сбор общественного мнения⁹³.

Для целей развития электронного государства в США в составе Административно-бюджетного управления было учреждено Управление электронного государства и информационных технологий⁹⁴, которое координирует цифровизацию агентств США, включая вопросы информационной безопасности (издавшее с 2021 по 2022 годы семь меморандумов, посвященных информационной безопасности в деятельности агентств США⁹⁵). Руководитель

⁹² USA. The Paperwork Reduction Act of 1980. URL: <https://www.govtrack.us/congress/bills/96/hr6410/text> (дата обращения: 05.03.2023).

⁹³ Sunstein C. R. The Office of Information and Regulatory Affairs: Myths and Realities Article // Harvard Law Review. Vol. 126. №. 7. 2013. P. 1838–1878.

⁹⁴ USA. E-Government Act of 2002. URL: <https://www.govinfo.gov/app/details/PLAW-107publ347> (дата обращения: 05.03.2023).

⁹⁵ M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices September 14, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf> (дата обращения: 05.03.2023); M-22-16 Administration Cybersecurity Priorities for the FY 2024 Budget. July 22, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf> (дата обращения: 05.03.2023).; M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. January 26, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf> (дата обращения: 05.03.2023); M-22-05 Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements. December 6, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf> (дата обращения: 05.03.2023).; M-22-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response. October 8, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf> (дата обращения: 05.03.2023); M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident. August 27, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf> (дата обращения: 05.03.2023); M-21-30 Protecting Critical Software Through Enhanced Security Measures. August 10, 2021. URL:

управления электронного государства и информационных технологий назначается главой государства без согласования Сената.

Указанные агентства в составе Административно-бюджетного управления часто совместно определяют политику развития электронного государства в США. Это заметно в рамках деятельности многочисленных советов, в которых участвуют представители указанных управлений, объединяющих представителей различных агентств США. В частности, при Административно-бюджетном управлении США действуют: Федеральный совет главных управляющих данными⁹⁶, назначаемых в агентства на основании Закона об основах политических решений, основанных на доказательствах, от 2018 года⁹⁷ и отвечающих за оборот данных внутри агентства, стандартизацию и управление данными как активами (data assets); Совет главных управляющих информацией, созданный в соответствии с Законом об электронном государстве от 2002 года⁹⁸ и в его составе (секции) - Совет главных управляющих информационной безопасностью, которым руководит Федеральный главный управляющий информационной безопасностью⁹⁹; Федеральный совет приватности, объединяющий старших управляющих приватностью агентств, сформированный на основании указа президента США Б. Обамы от 12.02.2016 № 13719¹⁰⁰.

Наконец, в регулировании информационной сферы не малую роль играют и органы Исполнительного офиса Президента США, отвечающие за развитие сферы исследований и разработок. В частности, Управление политики в сфере науки и

<https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf> (дата обращения: 05.03.2023).

⁹⁶ Официальный сайт FCDO. URL: <https://www.cdo.gov/about-agency-cdos/> (дата обращения: 05.03.2023).

⁹⁷ H.R.4174 - Foundations for Evidence-Based Policymaking Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4174/text> (дата обращения: 05.03.2023).

⁹⁸ E-Government Act of 2002. URL: <https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf> (дата обращения: 05.03.2023).

⁹⁹ CIO Council - CISO Committee. URL: <https://www.cio.gov/about/members-and-leadership/ciso-council/> (дата обращения: 05.03.2023).

¹⁰⁰ Executive Order 13719 of February 9, 2016. Establishment of the Federal Privacy Council. URL: <https://www.govinfo.gov/content/pkg/FR-2016-02-12/pdf/2016-03141.pdf> (дата обращения: 05.03.2023).

технологий обеспечивает главе государства содействие по вопросам развития исследований и разработок, а также координирует вопросы технического сопровождения информационной безопасности¹⁰¹. В период правления Б. Обамы в составе управления была учреждена должность Главного управляющего технологий¹⁰². Главный управляющий технологиями назначается на должность главой государства и является ассоциированным руководителем Управления политики в сфере науки и технологий. Главный управляющий технологиями ежегодно по консультации с Административно-бюджетным управлением направляет Президенту США отчет, который включает сведения о состоянии информационных систем федеральных агентств, их Интернет-сайтов, включая потенциальные угрозы безопасности.

В 2021 году в составе Исполнительного офиса Президента США была также учреждена должность Директора национальной киберполитики (National Cyber Director)¹⁰³. Директор национальной киберполитики является советником Президента по вопросам кибербезопасности, консультирует в пределах своей компетенции Совет национальной безопасности и Совет внутренней безопасности США, а также координирует реализацию национальной киберполитики и развитие системы уведомления об инцидентах в федеральных агентствах. Таким образом, если управления Исполнительного офиса Президента США преимущественно регулируют более конкретные вопросы обеспечения федеральными агентствами информационной безопасности, Директор национальной киберполитики играет более весомую роль в определении стратегии национальной кибербезопасности в целом.

Таким образом, развитие полномочий главы государства в информационной сфере приводит к расширению его аппарата и появлению новых органов,

¹⁰¹ National Science and Technology Policy, Organization, and Priorities Act of 1976. URL: <https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg459.pdf> (дата обращения: 05.03.2023).

¹⁰² United States Chief Technology Officer Act. URL: <https://www.congress.gov/bill/114th-congress/house-bill/1764/text> (дата обращения: 05.03.2023).

¹⁰³ William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. URL: <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf> (дата обращения: 05.03.2023).

координирующих развитие электронного правительства либо сферу информационной безопасности.

Необходимые для регулирования информационной сферы структурные изменения происходят и в Правительстве Российской Федерации. В целях организации деятельности Правительства Российской Федерации в составе Аппарата Правительства Российской Федерации образуются различные департаменты. В частности, в составе Аппарата Правительства Российской Федерации действуют Департамент информационных технологий, Департамент пресс-службы и референтуры, Сводно-аналитическое управление¹⁰⁴.

Для реализации государственной политики в информационной сфере учреждаются различные координационные комиссии. Особо значимая роль отведена комиссиям, координирующим сферу связи и информационных технологий. Анализ изменений правового статуса правительственных комиссий, координирующих вопросы развития информационных технологий в деятельности органов исполнительной власти, показывает увеличение полномочий комиссий. Если изначально в комиссиях председательствовал министр связи, а их решения были обязательны только для органов исполнительной власти, представители которых входили в соответствующую комиссию¹⁰⁵, то с 2013 года подход изменился. Была создана Правительственная комиссия по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (далее – Правительственная комиссия по

¹⁰⁴ Распоряжение Правительства РФ от 22.01.2020 № 56-р «Об утверждении структуры Аппарата Правительства Российской Федерации и о признании утратившими силу некоторых актов Правительства Российской Федерации» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 440.

¹⁰⁵ Постановление Правительства Российской Федерации от 28.03.2008 № 215 «О Правительственной комиссии по федеральной связи и информационным технологиям // Собрание законодательства РФ, 31.03.2008, № 13, ст. 1315; Постановление Правительства Российской Федерации от 28.03.2008 № 215 «О Правительственной комиссии по федеральной связи и технологическим вопросам информатизации (в редакции постановлений Правительства Российской Федерации от 10.03.2009 г. № 219; от 04.05.2010 г. № 304). URL: <http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102105985&backlink=1&&nd=102120707> (дата обращения: 05.03.2023).

цифровому развитию)¹⁰⁶. Председателем комиссии уже был назначен Председатель Правительства Российской Федерации¹⁰⁷, а решения комиссии приобрели обязательную силу не только для федеральных органов, участвующих в составе комиссии, но для всех федеральных органов исполнительной власти в целом.

Дополнительными полномочиями наделён также Президиум Комиссии. Решения Президиума обязательны для органов, принимающих в нем участие. Оба органа играют существенную роль в развитии цифровой экономики, однако осуществляют разные виды координации. Например, Президиум может принимать решение о подключении информационной системы организации к единой информационной инфраструктуре государственных информационных систем¹⁰⁸, а равно принимает решение о присоединении информационной системы организации к единой информационной системе здравоохранения по направлению заявки от Министерства здравоохранения Российской Федерации¹⁰⁹. При этом

¹⁰⁶ Постановление Правительства Российской Федерации от 26.08.2013 № 735 «О Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности» // Собрание законодательства РФ, 02.09.2013, № 35, ст. 4521.

¹⁰⁷ Распоряжение Правительства Российской Федерации от 03.09.2013 г. № 1578-р. URL: <http://static.government.ru/media/files/41d489d9ad294a026279.pdf> (дата обращения: 05.03.2023).

¹⁰⁸ П. 7 Правил присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, утверждённых Постановлением Правительства РФ от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» // Собрание законодательства РФ, 31.12.2012, № 53 (ч. 2), ст. 7938.

¹⁰⁹ П. 14 Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями, утверждённых Постановлением Правительства Российской Федерации от 12 апреля 2018 г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102487569&backlink=1&&nd=102466887> (дата обращения: 05.03.2023).

состав сведений, получаемых и передаваемых организацией при подключении к единой информационной инфраструктуре государственных информационных систем, например, уже определяется Правительственной комиссией по цифровому развитию или Правительством Российской Федерации¹¹⁰.

Соответствующие структурные изменения можно отметить и в аппарате правительства Франции. При Премьер-министре Франции учрежден Генеральный секретариат национальной безопасности, который обеспечивает сопровождение деятельности Совета национальной безопасности, а также оперативную координацию для реализации принятых им решений.

Необходимость развития общей информационной инфраструктуры взаимодействия постепенно привела к возникновению в аппарате Премьер-министра Франции органа, осуществляющего координацию развития информационных технологий органов исполнительной власти.

В 2019 г. при Премьер-министре была создана Межминистерская дирекция по цифровизации (DINUM) в ведении Генерального секретаря государства¹¹¹. Дополнительно каждое министерство формирует структурное подразделение, отвечающее за цифровизацию, в том числе за цифровую трансформацию публичной политики, развитие использования цифровых технологий, создание и организацию цифровых сервисов, цифровую инновацию, использование потенциала данных и за информационные системы. Указанные структурные подразделения обязаны направлять в DINUM планы инвестирования или иную бюджетную документацию в сфере цифровизации и предоставлять DINUM любую иную информацию.

¹¹⁰ П. 11 Правил присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

¹¹¹ Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039281619/2021-07-14/> (дата обращения: 05.03.2023).

Развитие аппарата правительства наблюдается и в других странах. В Сингапуре политическая, оперативная и техническая координация развития электронного правительства осуществляются непосредственно службами премьер-министра: Управлением умной нации и цифрового правительства (Smart Nation and Digital Government Office (SNDGO)), выполняющим функции политической и оперативной координации, Агентством государственных технологий Сингапура (Government Technology Agency of Singapore (GovTech)), выполняющим функции технической координации развития электронного правительства¹¹².

Сравнительный анализ позволяет заключить об усилении роли координационных органов аппаратов главы государства и правительства в регулировании информационной сферы.

В целом структурные связи внутри государственного аппарата можно разделить на субординационные, устанавливающие связь сверху вниз, реординационные, характеризующие связь обратного порядка, и координационные, характеризующие связи между равными звеньями аппарата¹¹³. Координационные связи могут устанавливаться как путем наделения одного из органов исполнительной власти координационными полномочиями, так и иными способами, в том числе путем обмена информацией, совместных действий, проведения совещаний¹¹⁴, а равно заключения административных договоров¹¹⁵.

Координационная функция предполагает вертикальную связь, обеспечивающую централизованную организацию инфраструктуры взаимодействия. Горизонтальные сетевые связи обеспечиваются координационным органом для информационного обмена, но не исключают сохранение вертикали власти. В условиях формирования цифровой экономики

¹¹² The Prime Minister's Office. Singapore. URL: <https://www.pmo.gov.sg/About-Us> (дата обращения: 05.03.2023).

¹¹³ Формы государственного управления / Отв. ред. Б.М. Лазарев. М.: ИГПАН, 1983. С. 17–24.

¹¹⁴ Указ. соч. С. 23 -24.

¹¹⁵ Бучакова М.А. Административно-правовое регулирование координации как функции государственного управления // Вестник Омского университета. Серия «Право». 2014. № 2 (49). С. 60–64.

координация, осуществляемая органами исполнительной власти, позволяет развивать сетевые горизонтальные связи между органами публичной власти и стимулировать оборот данных органами разных уровней публичной власти.

Правовой статус координационных органов и особенности координационных процедур получили небольшое рассмотрение в литературе¹¹⁶, однако в рамках цифровизации государственного управления именно координационные органы обеспечивают централизацию принятия решений и создают условия для горизонтального взаимодействия между различными заинтересованными ведомствами.

Вертикальный характер отношений координации позволяет координационным органам дублировать полномочия других органов в случаях, когда система органов исполнительной власти расширяется и стремится к поиску новых оперативных решений управленческих вопросов. Например, в ходе реформирования системы органов исполнительной власти в 2000-х годах отмечалось именно увеличение таких комиссий, фактически опосредовавших делегирование органом своих полномочий в определенной сфере выделяемой им комиссии¹¹⁷. Однако несмотря на возможные риски дублирования полномочий, координация позволяет обеспечить единое и устойчивое развитие государственной политики в сфере применения информационных технологий органами исполнительной власти.

Координационные органы следует отличать от совещательных комиссий, комитетов и организаций. Координационный орган, во-первых, сохраняет властные полномочия, а равно обладает контрольными полномочиями в отношении органов исполнительной власти, которые находятся ниже его в вертикали власти. Во-вторых, координационные органы обладают полномочиями

¹¹⁶ Максуров А.А. Координационная юридическая технология в Соединенном Королевстве (на примере отдельных регионов) // Вестник Санкт-Петербургского университета. 2018. Т. 9. № 3. С. 278–290; Цветков В.В. Правовая природа открытого метода координации в сфере социального права Европейского союза // Вестник Санкт-Петербургского университета. 2016. № 4. С. 29–35.

¹¹⁷ Исполнительная власть в Российской Федерации. Проблемы развития / отв. ред. И.Л. Бачило. М.: Юрист, 1998. С. 141.

утверждать административные акты по предмету ведения, которые являются обязательными для координируемых ими органов, а также могут носить нормативный правовой характер.

Координационные органы в Российской Федерации часто формируются и функционируют в рамках проектной деятельности государства¹¹⁸. В определенном смысле деятельность проектных органов сопоставима с деятельностью координационных органов. Однако координационный орган может сохраняться в рамках реализации различных государственных проектов, приобретая в конкретном направлении государственной политики отдельную проектную роль.

Под координационным органом исполнительной власти можно понимать орган исполнительной власти, осуществляющий сбор и организующий обмен информацией между нижестоящими органами исполнительной власти одного или нескольких уровней подчинения, наделенный контрольными полномочиями в отношении таких органов, а также обладающий полномочиями утверждать правовые акты по предмету ведения, обязательные для исполнения координируемыми им органами исполнительной власти.

Координационный орган непосредственно реализует аналитические информационные процессы в рамках осуществления им информационной функции государственного управления, реализует несколько основных групп полномочий: сбор и анализ информации, в том числе посредством реализации контрольных полномочий, а также осуществление планирования, включая подготовку проектов технических и правовых документов, в том числе новых стратегий информатизации государственного управления. Дополнительно координационный орган в сфере информатизации также может осуществлять функцию обеспечения технической реализации и поддержки взаимодействия информационных систем и межминистерских проектов.

Можно выделить следующие виды координации в структуре управления информатизацией государственного аппарата: политическая координация,

¹¹⁸ См.: Калмыкова А.В., Кабытов П.П. «Гибкие» структуры государственного управления // Журнал российского права. 2019. № 8. С. 107–120.

осуществляемая в отношении общего формирования политики цифровизации государственного управления, оперативная координация, осуществляемая в отношении отдельных проектов в рамках реализации установленной политики цифровизации, которая в странах со смешанной формой правления (Россия, Франция) реализуется правительством, а также техническая координация, выражающаяся в обеспечении технического обслуживания и функционирования информационных систем и сервисов, используемых несколькими органами исполнительной власти одновременно.

Координационный орган может сочетать в себе каждую из указанных форм координации или специализироваться только на отдельных видах координации. Прикладное значение выделенных видов координации состоит в возможности проанализировать тенденции к централизации либо децентрализации развития информационных технологий в деятельности органов исполнительной власти.

Сравнительный анализ позволяет выделить несколько различных моделей в зависимости от сочетания выделенных видов координации.

Российская модель координации развития информационных технологий в деятельности органов исполнительной власти характеризуется наиболее усиленной централизацией.

Основной отличительной чертой российского подхода является наличие отдельного министерства, отвечающего за техническое сопровождение информатизации государственного управления, и выделение отдельных структурных подразделений и органов внутри органов общей компетенции для реализации политической и оперативной координации.

В Российской Федерации основные полномочия по политической координации развития информационных технологий в деятельности органов исполнительной власти реализуются главой государства, а полномочия по оперативной координации и определению состава и структуры координационных органов в информационной сфере реализуются Правительством Российской Федерации. Техническую координацию, состоящую в непосредственном

присоединении информационных сетей, осуществляет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Во Франции необходимость развития общей информационной инфраструктуры взаимодействия постепенно привела к возникновению органа, осуществляющего все виды координации в сфере развития информационных технологий органов исполнительной власти — Межминистерской дирекции по цифровизации (DINUM) в составе служб Премьер-министра Франции. Однако современный технологический функционал единой инфраструктуры межведомственного взаимодействия во Франции развит более слабо, чем в России.

В США координация развития информационных технологий в деятельности федеральных агентств осуществляется органами в составе аппарата главы государства, руководящего исполнительной властью. Дополнительно отдельные координационные полномочия предоставляются законодателем таким органам для обеспечения регулирования деятельности не только исполнительных, но также независимых агентств. Координационные органы выполняют функции политической координации, регулируя политику использования информационных технологий федеральными агентствами.

Сформированная в США модель сохраняет условия для централизации именно в сфере определения общей политики развития информационных технологий в деятельности федеральных агентств, однако принятие решений о необходимости внедрения тех или иных информационных технологий и организации информационного обмена осуществляется агентствами самостоятельно. В указанном контексте модель развития информационных технологий в деятельности органов исполнительной власти в США можно охарактеризовать как модель «умеренной централизации».

Выделенные модели координации показывают различные уровни централизации использования информационных технологий в деятельности органов исполнительной власти. Если в США, где не развивается единая инфраструктура взаимодействия, централизация реализуется только на уровне определения общей политики, во Франции и России централизация более

характерна. В случае, если Франция продолжит развитие единой инфраструктуры взаимодействия, во Франции, как и в России, координационные органы разделятся в зависимости от вида координации. Это объясняется необходимостью распределения полномочий между различными органами исполнительной власти, осуществляющими одну функцию в одной предметной сфере. Усиление централизации регулирования информационной сферы приводит к распределению полномочий между различными органами.

1.2. Министерства и иные ведомства¹¹⁹

Понимание министерства может отличаться в зависимости от страны и национального подхода к формированию структуры органов исполнительной власти. В Российской Федерации министерство представляет собой обособленную единицу государственного аппарата, руководство которой осуществляет министр. Схожий подход характерен для США. Другой подход к пониманию министерства применяется во Франции, где ключевую роль играет личность министра, а структура министерства может изменяться. Возможно назначение нескольких министров (например, в Министерстве экономики и финансов). Дополнительно во Франции существуют также должности делегированных министров, допускается возложение отдельных функций на государственных секретарей.

Министерства осуществляют функции по прогнозированию и планированию в рамках отрасли в их ведении. Однако если органы общей компетенции реализуют координационную функцию в рамках регулирования информационной сферы, министерства могут осуществлять непосредственное руководство подведомственными им органами исполнительной власти нижестоящего уровня.

Государственное управление в информационной сфере может осуществляться путем образования новых отраслевых министерств в

¹¹⁹ В рамках проводимого сравнительного исследования термин «ведомство» используется для обозначения органов исполнительной власти центрального аппарата.

информационной сфере. Такой подход характерен, например, для азиатских стран (Сингапур, Китай, Индия) и реализуется также в Российской Федерации.

В Российской Федерации Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры)¹²⁰, в функции которого входит выработка и реализация государственного регулирования в сферах использования информационных технологий, связи, а также персональных данных¹²¹. Деятельность министерства охватывает регулирование всей информационной сферы в целом. Можно отметить, что, осуществляя техническую координацию развития электронного правительства, министерство начинает активно участвовать в процессе оказания государственных услуг и управления государственным имуществом для этих целей, являясь оператором ключевых государственных информационных систем.

В Китае действует Министерство индустрии и информационных технологий, в основные полномочия которого входит обеспечение индустриального развития, включая развитие коммуникаций, а также обеспечение информационной безопасности¹²². Министр назначается по представлению премьер-министра Государственного Совета Всекитайским Собранием Народных Представителей¹²³. Законодательные полномочия в Китайской Народной Республике осуществляются Всекитайским Собранием Народных Представителей, однако и Государственный Совет, в который входит министр индустрии и информационных технологий, наделен нормотворческими полномочиями¹²⁴.

¹²⁰ Указ Президента РФ от 21.01.2020 № 21 «О структуре федеральных органов исполнительной власти» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 346.

¹²¹ Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // Собрание законодательства РФ, 09.06.2008, № 23, ст. 2708.

¹²² China. Ministry of Industry and Information Technology. URL: http://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm (дата обращения: 05.03.2023).

¹²³ Дугаржапов А.Г. Полномочия Госсовета КНР // Проблемы современной науки и образования. 2015. № 2. С. 81–85.

¹²⁴ Цюэнь Л. Система и развитие законодательства Китайской Народной Республики // Вестник СПбГУ. Право. 2020. Т. 11. Вып. 3. С. 666–678.

В Сингапуре министры назначаются главой государства из числа представителей парламента по представлению премьер-министра. Регулирование информационной сферы осуществляет Министерство коммуникаций и информации, в ведении которого находятся Агентство по кибербезопасности, Ведомство по развитию инфокоммуникационных медиа, Национальный библиотечный совет и Комиссия по защите персональных данных¹²⁵. Однако к ведению указанного министерства не относятся вопросы развития государственной информационной инфраструктуры, которые реализуются непосредственно службами премьер-министра.

В Индии, хотя планы развития электронного правительства утверждаются правительством, оперативная и техническая координация отнесены к ведению профильных министерств¹²⁶. В Индии действуют несколько министерств в информационной сфере. Министры назначаются главой государства по представлению премьер-министра. Образованные в результате разделения единого Министерства коммуникаций и информационных технологий в 2016 году Министерство коммуникаций, отвечающее за организацию систем связи, включая почтовую связь¹²⁷, а также Министерство электронных и информационных технологий¹²⁸, занимающееся вопросами цифровизации государственного управления, фактически возглавляет один и тот же министр. Дополнительно при Министерстве электронных и информационных технологий назначен государственный министр (minister of the state) – министр нижестоящего уровня. В Индии также действует Министерство информации и телевидения, которое совместно с Министерством по вопросам молодежи и спорта возглавляет один

¹²⁵ Singapore. Ministry of communications and information. Agencies. URL: <https://www.mci.gov.sg/agencies> (дата обращения: 05.03.2023).

¹²⁶ Мартынова Н.А., Хмельков А.Б. Цифровые технологии в государственном управлении: опыт России и Республики Индия // Среднерусский вестник общественных наук. 2019. № 1. С. 127–144.

¹²⁷ India. Ministry of communications. URL: <https://dot.gov.in/vision-mission> (дата обращения: 05.03.2023).

¹²⁸ India. Ministry of electronics & information technology. URL: <https://www.meity.gov.in> (дата обращения: 05.03.2023).

министр¹²⁹. Увеличение числа министерств с сохранением меньшего количества министров можно отметить в качестве одной из форм укрупнения министерств, реализуемой Индией в самобытной манере¹³⁰.

Во Франции и США отсутствует профильное министерство, занимающееся вопросами цифровизации. Основные полномочия в информационной сфере распределяются между отдельными министерствами по предметам их ведения, а также посредством формирования соответствующих ведомств, осуществляющих регулирование в отдельных сферах.

Во Франции техническая координация единой информационной инфраструктуры отнесена к ведению Премьер-министра. Однако полномочия по определению и реализации регулирования в информационной сфере осуществляет Министр экономики, финансов, индустриального и цифрового суверенитета, при котором назначен Делегированный Министр по цифровому развитию и телекоммуникациям¹³¹. Хотя делегированный министр находится в ведении вышестоящего министра, он обладает самостоятельным правом участия на Совете министров в пределах компетенции. Однако назначение делегированного министра нельзя рассматривать равнозначным к учреждению отдельных профильных министерств, регулирующих информационную сферу.

Учреждение отдельного профильного министерства или нескольких министерств отражает большую склонность государства к централизации процессов по цифровизации государственной деятельности и государственному управлению информационной сферой. Оно способствует единому выстраиванию различных информационных процессов в деятельности исполнительной власти. Модель, в которой не создается отдельное министерство для регулирования информационной сферы, нацелена на регулирование информационной сферы с

¹²⁹ India. Council of Ministers. URL: <https://www.india.gov.in/my-government/whos-who/council-ministers> (дата обращения: 05.03.2023).

¹³⁰ Штатина М.А. Административные реформы в Индии // Труды Института государства и права РАН. 2019. Том 14. № 1. С. 166–190.

¹³¹ Décret du 4 juillet 2022 relatif à la composition du Gouvernement. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046013941> (дата обращения: 05.03.2023).

учетом особенностей соответствующей отрасли либо экономических возможностей государства.

Помимо министерств, в системе органов исполнительной власти в рамках регулирования информационной сферы действуют также отдельные органы, осуществляющие функции контроля в определенной области информационной сферы (далее – специализированные ведомства).

В Российской Федерации сохраняются принцип единоначалия и вертикальная иерархия. Органом по контролю и надзору в сфере соблюдения законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)¹³², находящаяся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры)¹³³.

Ключевые полномочия министерства в отношении подведомственных ему федеральных служб и агентств определены в Постановлении Правительства РФ от 2 июня 2008 г. № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» (далее – Постановление о Минцифры)¹³⁴. Министерство осуществляет координационные и контрольные полномочия в отношении Роскомнадзора (п. 5.2, 5.12, 5.14 Постановления о Минцифры). Полномочия министерства дополняются контрольными полномочиями министра. В частности, министр утверждает ежегодный план деятельности Роскомнадзора (п. 10.7 Постановления о Минцифры), вносит в Министерство финансов Российской Федерации предложения по бюджетному финансированию службы (п. 10.9 Постановления о Минцифры). Министр вправе приостанавливать или отменять

¹³² Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций) // Российская газета, № 49, 24.03.2009.

¹³³ Указ Президента РФ от 21.01.2020 № 21 «О структуре федеральных органов исполнительной власти» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 346.

¹³⁴ Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // Собрание законодательства РФ, 09.06.2008, № 23, ст. 2708.

решения Роскомнадзора, если иной порядок отмены не установлен федеральным законом (п. 10.13 Постановления о Минцифры).

Министерство осуществляет нормотворческие полномочия в сфере ведения Роскомнадзора (пункты 5.1, 5.2.26 указанного постановления). Однако если в соответствии с пунктом 8 части 2 статьи 23 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» Роскомнадзор вправе только обращаться с предложениями по усовершенствованию регулирования в сфере защиты персональных данных, Минцифры вправе также предлагать проекты нормативно-правовых актов в сфере ведения Роскомнадзора.

Таким образом, регулирование информационной сферы в России осуществляется на основе иерархического подчинения специализированного ведомства профильному министерству, что обеспечивает единую политику регулирования различных направлений информационной сферы в ведении указанных органов: персональных данных, связи, средств массовой информации.

Зарубежные страны с более длительной историей развития административного аппарата были вынуждены искать более гибкие подходы к определению правового статуса органов, регулирующих информационную сферу. В США и Франции можно отметить тенденцию к формированию специализированных независимых органов¹³⁵. Независимость реализуется благодаря взаимодействию законодательной и исполнительной власти при формировании коллегиального органа, осуществляющего регулирующие функции в отдельной сфере, и состоит в уменьшении влияния главы исполнительной власти на деятельность независимого органа исполнительной власти путем определения законодателем особенностей функционирования и формирования такого органа. Такая функциональная децентрализация внутри центрального государственного аппарата может не снижать общей тенденции к централизации управленческих функций с позиций соотношения с регионами.

¹³⁵ Децентрализованные органы и учреждения в системе исполнительной власти зарубежных государств: научно-практическое пособие / Н. М. Касаткина, Ф. А. Лещенков, А. Н. Пилипенко и др.; отв. ред. А. Н. Пилипенко. М.: ИЗиСП: Норма: ИНФРА-М, 2018.

Есть несколько общих черт у независимых агентств США и независимых административных ведомств Французской Республики. В обеих юрисдикциях органы учреждались для преодоления сложности бюрократической системы, независимость обеспечена коллегиальностью, представительством, срочностью полномочий и ограничением на отстранение от должности.

Одновременно, с точки зрения компетенции наблюдаются различия. Независимость агентств США сопровождалась передачей им квазисудебных и нормотворческих функций. Это породило многочисленные споры в правовой литературе о правомерности независимых агентств, их соотношении с системой сдержек и противовесов и конституцией. Основными независимыми агентствами США, регулирующими информационную сферу, являются Федеральная торговая комиссия США и Федеральная комиссия связи США.

Во Франции, напротив, независимые административные ведомства стали рассматриваться как гарантия соблюдения прав человека и одно из средств правового государства¹³⁶. Схожее с США увеличение количества образуемых независимых административных ведомств привело к принятию законодательства¹³⁷, унифицирующего и гармонизирующего правовой статус независимых административных ведомств и уменьшение их количества, что позволило скорректировать потенциальную возможность нарушения конституционной системы распределения власти в государстве.

¹³⁶ Chevallier J. Autorités administratives indépendantes et État de droit // Civitas Europa. 2016. Vol. 37. № 2. P. 143-154; Autin J.L. Autorités administratives indépendantes, démocratie et État de droit // Droit et société. 2016. № 93. P. 285–295.

¹³⁷ Mézard J. Un État dans l'État : canaliser la prolifération des autorités administratives indépendantes pour mieux les contrôler. Rapport № 126 (2015-2016), fait au nom de la CE Autorités administratives indépendantes, déposé le 28 octobre 2015. URL : <http://www.senat.fr/rap/r15-126-1/r15-126-1.html> (дата обращения: 05.03.2023); Loi organique n° 2017-54 du 20 janvier 2017 relative aux autorités administratives indépendantes et autorités publiques indépendantes. URL : <https://www.legifrance.gouv.fr/eli/loi/2017/1/20/PRMX1604073L/jo/texte> (дата обращения: 05.03.2023); Loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendante. URL : <https://www.legifrance.gouv.fr/eli/loi/2017/1/20/PRMX1604064L/jo/texte> (дата обращения: 05.03.2023).

Независимые ведомства Франции редко наделяются нормотворческими полномочиями. Основной формой их деятельности является направление мнений на отдельные проекты нормативных актов, опубликование разъяснений и обращений. В некоторых случаях независимые ведомства наделяются также полномочиями по принятию решения о применении мер административного принуждения.

Независимыми административными ведомствами, осуществляющими полномочия в информационной сфере, во Франции являются, например, Национальная комиссия по информатике и свободам (CNIL), регулирующая сферу персональных данных, Комиссия по доступу к административным документам (CADA), отвечающая за разрешение споров о возможности предоставления гражданам информации о деятельности органов исполнительной власти, Комиссия тайны национальной безопасности (CSDN), рассматривающая вопросы снятия правового режима государственной тайны с планируемой к передаче органом исполнительной власти информации, Ведомство по регулированию электронных коммуникаций, почтовой связи и распространения прессы (ARCEP), регулирующее сети связи, Ведомство по регулированию аудиовизуальной и цифровой коммуникации (ARCOM)¹³⁸, регулирующее радиосвязь и телевизионное вещание, Высшее ведомство транспарентности публичной жизни (HATVP), отвечающее за опубликование сведений о доходах отдельных должностных лиц и реализацию антикоррупционной политики.

Несмотря на реформу независимых административных ведомств и уменьшение их количества, во Франции сохраняется значительное число независимых органов, регулирующих отдельные аспекты информационной сферы.

Различие можно отметить и в способе формирования коллегиального органа. Коллегиальность обеспечивает более взвешенное принятие решений, учитывающих различные интересы. В США это достигается путем обязательного требования к бипартийности состава независимого агентства. Во Франции – путем

¹³⁸ Публичное независимое ведомство, наделенное юридической личностью.

участия представителей различных ветвей власти (обеих палат парламента, Кассационного суда Франции и Государственного совета Франции) в составе коллегиального органа, а также привлечения специалистов, обладающих определенной профессиональной компетенцией в информационной сфере (*personnalité qualifiée*).

На основании сравнительного анализа независимость органа исполнительной власти можно определить как специальный правовой статус органа исполнительной власти, при котором исключается возможность прямого иерархического влияния на его деятельность вышестоящих органов исполнительной власти, а также главы государства и законодательных органов, с одновременным установлением сбалансированных механизмов контроля за деятельностью таких органов каждой из ветвей власти. С организационной точки зрения предоставление такой независимости требует принятия дополнительных мер, направленных на пресечение возможности злоупотребления полномочиями со стороны органа. В числе таких мер можно отметить: коллегиальность органа, срочность полномочий назначаемых коллегиальных руководителей органа, введение дополнительных гарантий для невозможности отстранения таких лиц от должности раньше срока полномочий.

В Российской Федерации схожие независимые коллегиальные органы, функционально децентрализованные в центральном аппарате исполнительной власти, отсутствуют. Независимость органа в системе исполнительной власти предполагает его учреждение законодателем. Однако в соответствии со статьей 83 Конституции Российской Федерации¹³⁹ именно Президент Российской Федерации определяет структуру федеральных органов исполнительной власти.

Децентрализация полномочий может осуществляться и с помощью косвенных средств: расширения полномочий соответствующего органа исполнительной власти в отношении органов исполнительной власти одного

¹³⁹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: <http://publication.pravo.gov.ru/Document/View/0001202007040001> (дата обращения: 05.03.2023).

уровня (например, предоставление полномочий по вынесению мнения относительно соответствующего проекта нормативно-правового акта); отнесения органа исполнительной власти к ведению президента или правительства напрямую, что дает больше гарантий к независимости осуществления полномочий органом исполнительной власти; создание коллегиальных органов исполнительной власти, позволяющее обеспечить учет нескольких мнений при формировании регулирования по предмету ведения.

Близким примером такого независимого органа является Уполномоченный по правам человека в Российской Федерации, назначаемый и отстраняемый от должности Государственной Думой Российской Федерации¹⁴⁰. Однако национальный институт защиты прав человека, обладая необходимой независимостью от органов исполнительной власти, в указанном случае не входит в систему органов исполнительной власти в целом и не обладает полномочиями, которыми наделены федеральные органы исполнительной власти.

Дискуссионным в российской правовой литературе является вопрос о создании независимого органа по защите персональных данных. Некоторые исследователи предлагают передать орган по защите персональных данных в ведение Правительства Российской Федерации¹⁴¹, другие склоняются к утверждению о наличии всех необходимых условий независимости такого органа¹⁴².

Однако независимость органа по защите персональных данных должна быть обеспечена не только отнесением его к ведению Правительства Российской Федерации. Важным условием независимости является коллегиальность органа и особый порядок формирования его состава, включающий назначение специалистов, обладающих профессиональными познаниями в информационной

¹⁴⁰ Федеральный конституционный закон от 26.02.1997 № 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации» // Российская газета, № 43-44, 04.03.1997.

¹⁴¹ Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении: автореферат дис. ... д.ю.н. Саратов, 2014.

¹⁴² Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... к.ю.н. Челябинск, 2010.

сфере. Усиление независимости может повлечь за собой и пересмотр процедур принятия органом решений о привлечении к ответственности за нарушения в сфере персональных данных. Хотя современное законодательство предоставляет Роскомнадзору дополнительные полномочия напрямую предлагать Правительству изменения в законодательство о персональных данных, усиливающие его независимость, сохраняется принцип единоначалия.

Независимые органы исполнительной власти – результат модернизации системы государственного управления на предыдущих этапах развития публичной администрации. Особенностью их учреждения была необходимость преодолеть сложности коммуникаций в сложившейся системе управления с целью обеспечения гарантии прав и свобод граждан (Франция) или интересов бизнеса (США). Независимые органы – вынужденная реакция государства для реформирования управленческого аппарата. Анализ деятельности независимых органов исполнительной власти обнажает их негативные стороны: повышение бюджетных затрат на содержание такого органа, необходимость дополнительного контроля за соблюдением разделения властей с учетом расширяющихся полномочий независимых органов.

Российская модель организации публичной администрации – более молодая по сравнению с Францией и США, сохраняющая способность к централизованному разрешению вопросов управления информационной сферой без необходимости учреждения более гибких независимых органов. Сложившаяся в России в отличие от большинства зарубежных стран обособленная система административных правонарушений и отсутствие дискуссии о разделении властей для наделения органа исполнительной власти полномочиями по назначению административного наказания во внесудебном порядке позволили избежать необходимости учреждения отдельных независимых органов исполнительной власти.

В связи с изложенным вопрос обеспечения независимости органа по защите персональных данных по образцу зарубежных стран представляется нецелесообразным. Однако для России характерна другая проблема в части

регулирования информационной сферы. Полномочия Минцифры и Роскомнадзора расширяются и охватывают различные аспекты регулирования информационной сферы. Минцифры как оператор ключевых государственных информационных систем одновременно участвует в нормотворческой деятельности в сфере персональных данных. Такое укрупнение полномочий препятствует развитию регулирования персональных данных в публичной сфере. Укрупнение полномочий профильных министерства и ведомства России в информационной сфере свидетельствуют о необходимости поиска новых структур и способов распределения функций в центральном аппарате. С одной стороны, необходимо перераспределение части полномочий к другим профильным органам исполнительной власти. В частности, реализуемые Роскомнадзором меры по ограничению доступа к информационным ресурсам могут быть отнесены к ведению правоохранительных органов (что характерно, например, для Франции). С другой стороны, необходимо обособление органа исполнительной власти, непосредственно занимающегося только вопросами защиты персональных данных. Соответствующая служба может быть учреждена в ведении Министерства юстиции Российской Федерации. В таком случае, во-первых, полномочия по регулированию сферы связи и цифровизации государственного управления будут отделены от полномочий в сфере защиты персональных данных. Во-вторых, регулирование персональных данных будет осуществляться органами в ведении Президента Российской Федерации, а сферы связи и цифровизации государственного управления – органами в ведении Правительства Российской Федерации.

Если в США и Франции в отдельных областях информационной сферы учреждаются преимущественно независимые органы, в регулировании вопросов информационной безопасности во всех сравниваемых странах (Россия, Франция, США) сохраняется централизованный подход.

В Российской Федерации полномочия в сфере информационной безопасности осуществляются несколькими органами исполнительной власти – Федеральной службой безопасности Российской Федерации, Федеральной

службой по техническому и экспортному контролю, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации. В аппарате Правительства Российской Федерации отсутствует специализированный орган, координирующий вопросы информационной безопасности.

Во Франции сбор информации об инцидентах и взаимодействие с другими участниками системы информационной безопасности осуществляет Национальное агентство безопасности информационных систем, учрежденное в 2009 году при Генеральном секретариате национальной безопасности¹⁴³.

Полномочия в сфере информационной безопасности в США осуществляет Агентство кибербезопасности и безопасности инфраструктуры (CISA), учрежденное при Министерстве внутренней безопасности США в 2018 году¹⁴⁴. Агентство обеспечивает централизованный обмен информацией об инцидентах информационной безопасности между различными органами публичной власти и организациями частного сектора. С 2022 года Центр национальной кибербезопасности и коммуникационных интеграций, действующий в составе Агентства, получил возможность собирать информацию об инцидентах также на вертикальном уровне, включая органы штатов¹⁴⁵.

Сравнительный анализ рассматриваемых стран показывает, что полномочия в сфере информационной безопасности осуществляются специально создаваемыми органами исполнительной власти в ведении отраслевых органов безопасности. Российская Федерация позже начала реагировать на вопросы информационной безопасности и выстраивать систему уведомлений об инцидентах информационной безопасности. Исходя из необходимости

¹⁴³ Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212/> (дата обращения: 05.03.2023).

¹⁴⁴ H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/3359/text> (дата обращения: 05.03.2023).

¹⁴⁵ S.2520 - State and Local Government Cybersecurity Act of 2021. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/2520/text> (дата обращения: 05.03.2023).

всестороннего подхода к вопросам национальной безопасности в целом, полномочия по регулированию информационной безопасности в Российской Федерации преимущественно реализуются Федеральной службой безопасности Российской Федерации в ведении Президента Российской Федерации.

1.3. Органы исполнительной власти субъектов федеративных государств в информационной сфере

Развитие информационной сферы на нижестоящих уровнях публичной власти осуществляется в следующих направлениях. Развиваются технологии Интернета вещей, позволяющие объединять различные объекты местной и региональной инфраструктуры. Как следствие, в распоряжение органов нижестоящего уровня поступают различные данные о деятельности региона, включая пространственные данные и различные статистические сведения, которые могут быть вторично использованы для развития региона (например, исходя из статистики парковочных мест можно определить, в каком месте лучше открыть магазин). Имея локальное значение, такие данные, тем не менее, представляют ценность для центральной администрации и других органов нижестоящего уровня, поскольку позволяют создавать более детальную статистику для выявления проблем и потребностей регулирования. Возникает необходимость централизованного информационного обмена по вертикали и по горизонтали между различными органами в системе публичной власти в целом.

Организация взаимодействия и распределение полномочий между центром и регионами зависит от территориального устройства государства. В федеративных государствах конституционно решается вопрос разграничения полномочий между центром и регионами. В унитарных государствах также реализуются процессы децентрализации, перераспределяющие часть полномочий центра местным органам.

Разграничение предметов ведения между центральными и региональными государственными органами в рамках регулирования информационной сферы в федеративных государствах пока что находится в стадии развития.

В Российской Федерации разграничение предметов ведения между субъектами и Российской Федерацией может осуществляться в административном или договорном порядке¹⁴⁶, однако приоритетным является административное разграничение предметов ведения в Конституции. В свете реформы Конституции в 2020 году к ведению федерации были отнесены вопросы безопасности в сфере оборота данных¹⁴⁷. Вопросы регулирования информации, информационных технологий и связи отнесены к ведению Российской Федерации в первоначальной редакции пункта и) статьи 71 Конституции Российской Федерации. Однако такое разграничение предметов ведения не позволяет в полной мере учесть особенности управления информацией на уровне субъектов Российской Федерации. В результате вопрос полномочий субъектов Российской Федерации в отношении информации сохраняет дискуссионный характер как на практике, так и в теории.

В частности, в Договоре о разграничении предметов ведения и полномочий между органами государственной власти Российской Федерации и органами государственной власти города федерального значения Москвы от 16.06.1998¹⁴⁸ вопросы развития и функционирования федеральных и городских систем энергетики, информации и связи были отнесены к совместному ведению Российской Федерации и Москвы.

В правовой литературе 90-х – 2000-х годов можно также встретить упоминание «федеральной информации» в контексте предмета ведения Российской Федерации¹⁴⁹. Однако указанный термин не получил дальнейшего развития.

¹⁴⁶ Манохин В.М. Правотворческая деятельность в субъектах Российской Федерации: Вопросы методики. Саратов: СГАП, 2000.

¹⁴⁷ Пункт м) статьи 71 Конституции Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: <http://publication.pravo.gov.ru/Document/View/0001202007040001> (дата обращения: 05.03.2023).

¹⁴⁸ Договор о разграничении предметов ведения и полномочий между органами государственной власти Российской Федерации и органами государственной власти города федерального значения Москвы от 16.06.1998 // Российская газета. № 116. 23.06.98.

¹⁴⁹ См., напр.: Тихомиров Ю.А. Публичное право. Учебник. М.: Издательство БЕК, 1995. С. 199; Информационные ресурсы развития Российской Федерации: Правовые проблемы / Институт государства и права. М.: Наука, 2003. С. 366.

По смыслу части 1 статьи 4 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁵⁰ информационное законодательство состоит только из федеральных законов, а законы субъектов не упоминаются. При этом в некоторых субъектах Российской Федерации действуют законы об информационных ресурсах¹⁵¹.

В правовой литературе обращалось внимание на наличие у субъектов Российской Федерации права собственности на информационные ресурсы¹⁵². Категория собственности в отношении информационных ресурсов была возможна в рамках упоминания информации в качестве объекта гражданских прав в законодательстве. В связи с исключением информации из числа объектов гражданских прав, хотя в современной литературе сохраняется полемика по данному вопросу¹⁵³, такой вопрос утратил целесообразность.

В информационном законодательстве были выработаны более гибкие подходы, описывающие полномочия в отношении информации. Более подходящим было бы упоминание о субъектах Российской Федерации как отдельных обладателях информации. Право субъекта Российской Федерации как обладателя информации устанавливать отдельные особенности регулирования находящейся в его распоряжении информацией следует из статьи 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁵⁴.

¹⁵⁰ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

¹⁵¹ Напр.: Закон Москвы от 24.10.2001 № 52 «Об информационных ресурсах и информатизации города Москвы». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&vkart=card&nd=120029610&rdk=&backlink=1> (дата обращения: 05.03.2023); Закон Республики Татарстан от 13 ноября 2007 г. № 58-ЗРТ «Об информационных системах и информатизации Республики Татарстан». URL: <https://digital.tatarstan.ru/zakon-rt-ob-informatsionnih-sistemah-i.htm> (дата обращения: 05.03.2023).

¹⁵² Информационные ресурсы развития Российской Федерации: Правовые проблемы / Институт государства и права. М.: Наука, 2003. С. 367.

¹⁵³ Александрова Н.С. Информация как родовое понятие некоторых объектов гражданских прав (на примере цифровых прав) // Legal Concept - Правовая парадигма. 2020. Т. 19. № 1. С. 64-68.

¹⁵⁴ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

Вопрос разграничения полномочий между Российской Федерацией и ее субъектами нуждается в отдельном уточнении непосредственно в Конституции Российской Федерации. Если к ведению Российской Федерации относится информация в целом и безопасность оборота данных, то вопросы управления информацией и информационными системами субъектов Российской Федерации должны быть закреплены в совместном ведении федерации и ее субъектов. Такой подход позволит субъектам Российской Федерации в том числе определять направления развития информационной сферы с учетом потребностей в субъекте и бюджетных возможностей¹⁵⁵.

Контрастирующим к российскому опыту в этом отношении можно привести опыт США. Политика Р. Рейгана и Р. Никсона, направленная на усиление самостоятельности штатов, со временем привела к усилению «политической дифференциации» между различными штатами¹⁵⁶. В результате для США характерно активное развитие информационного законодательства на уровне штатов.

Дифференциация осуществляется в разных направлениях. С одной стороны, можно отметить принятие актов, регулирующих отдельные особенности оборота персональной информации, такими штатами как Нью-Йорк, Калифорния. Такое развитие обусловлено в том числе медлительностью Конгресса США в принятии единого закона, регулирующего особенности обработки персональных данных в публичном секторе.

Другое направление – регулирование технологий искусственного интеллекта. Каждый из штатов в настоящий момент самостоятельно устанавливает правила использования технологий распознавания лиц. Если ряд штатов изначально запрещали использование технологий распознавания лиц органами исполнительной власти, подход меняется, устанавливаются отдельные

¹⁵⁵ Необходимость оптимизации соотношения полномочий и финансов субъектов Российской Федерации точно подмечена С.В. Нарутто. См.: Нарутто С.В. Конституция, федерализм и единство государственно-правовой системы России // *Lex Russica*. 2018. № 11. С. 83-92.

¹⁵⁶ Гуляков А.Д. Логика развития федерализма в США (историко-государствоведческая и историко-правовая оценка) // *Lex Russica*. 2016. № 7. С. 116–129.

ограничения (Калифорния, Вирджиния). На федеральном уровне обсуждаются законопроекты, однако до настоящего времени регулирование осуществляется штатами¹⁵⁷.

Таким образом, вопрос разграничения полномочий в федеративных государствах между субъектами и федерацией в информационной сфере остается открытым. В России регулирование информации отнесено к ведению федерации, однако сложившаяся модель нуждается в уточнении. В США отмечается более активная роль штатов в поиске регулирования информационной сферы.

В системе органов исполнительной власти субъектов федеративных государств также учреждаются отдельные органы, регулирующие информационную сферу.

Для управления информационной сферой в субъектах Российской Федерации учреждаются министерства или департаменты информации и цифровизации¹⁵⁸, которые не подчиняются федеральному министерству и не являются его территориальными подразделениями. Указанные органы осуществляют функцию распорядительства в отношении государственных информационных систем соответствующего субъекта Российской Федерации. В частности, Департамент информационных технологий города Москвы определяет правила использования информационных ресурсов субъекта в рамках различных проектов¹⁵⁹, устанавливает порядок предоставления доступа к наборам городских данных¹⁶⁰.

¹⁵⁷ Rabinowicz C. Approaches to Regulating Government Use of Facial Recognition Technology // Harvard Journal of Law and Technology Digest. URL: <https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology> (дата обращения: 05.05.2023). Дата опубликования: 04.05.2023.

¹⁵⁸ Напр.: Департамент информационных технологий города Москвы. URL: <https://www.mos.ru/dit/> (дата обращения: 05.03.2023); Министерство информационного развития и связи Пермского края. URL: <https://mirs.permkrai.ru> (дата обращения: 05.03.2023).

¹⁵⁹ Распоряжение Департамента информационных технологий города Москвы от 13.03.2023 № 64-16-120/23 «Об утверждении Правил использования информационных систем и ресурсов города Москвы при реализации проекта «Электронный дом». URL: <https://www.mos.ru/dit/documents/normativnye-pravovye-akty-departamenta/view/283481220/> (дата обращения: 05.03.2023).

¹⁶⁰ Распоряжение Департамента информационных технологий города Москвы от 31.03.2023 № 64-16-168/23 «Об установлении порядка направления и рассмотрения заявок о предоставлении

В США в отдельных штатах дополнительно также создаются и действуют отдельные министерства (департаменты), осуществляющие в первую очередь функцию распорядительства в отношении информационных технологий и информационных систем штата¹⁶¹. Например, Управление услуг в сфере информационных технологий штата Нью-Йорк (Office of Information Technology Services) разрабатывает политики и стандарты в сфере применения информационных технологий в штате Нью-Йорк¹⁶² в соответствии с установленной таким управлением процедурой¹⁶³, а также обеспечивает информирование граждан об электронных услугах штата на своем портале.

Хотя в отдельных направлениях регулирования информационной сферы наблюдается более централизованный подход (например, информационная безопасность), органы исполнительной власти в субъектах федеративных государств обеспечивают реализацию электронного правительства в пределах своей территории. Разграничение полномочий между федерацией и субъектами в рамках регулирования информационной сферы еще находится в стадии развития.

Помимо регионального уровня в федеративных государствах, в любом государстве действует также система органов, решающих вопросы местного значения. В случае с федеративными государствами зачастую регионы самостоятельно определяют особенности существования и функционирования

доступа к наборам городских данных». URL: <https://www.mos.ru/dit/documents/normativnye-pravovye-akty-departamenta/view/285419220/> (дата обращения: 05.03.2023).

¹⁶¹ The New York State Office of Information Technology Services (ITS). URL: <https://its.ny.gov/about-us> (дата обращения: 05.03.2023); Washington Technology Solutions. URL: <https://watech.wa.gov> (дата обращения: 05.03.2023); The California Department of Technology (CDT). URL: <https://cdt.ca.gov> (дата обращения: 05.03.2023).

¹⁶² The New York State Office of Information Technology Services (ITS). Policies. URL: <https://its.ny.gov/policies> (дата обращения: 05.03.2023).

¹⁶³ The New York State Office of Information Technology Services. Process for Establishing Information Technology Policies, Standards, and Guidelines. № NYS-P09-003. Updated: 05.04.2021. URL: https://its.ny.gov/system/files/documents/2022/10/nys-p09-003_process_for_establishing_information_technology_policies.pdf (дата обращения: 05.03.2023).

муниципальных образований и обеспечивают их поддержку. В первую очередь цифровизация осуществляется в рамках развития «умных городов»¹⁶⁴.

Стоит отметить, что развитие «умного города» не всегда относится к сфере компетенции органов местного самоуправления. Многие города, лидирующие в развитии электронного правительства, являются автономными государственными субъектами – Берлин (1 место), Москва, Париж (совместное 5 место). Некоторые города представляют собой отдельные государства – Сингапур (9 место)¹⁶⁵. В целом из первых 38 лидирующих городов 20 расположены в Европе, 10 в Азии, 6 в Америке и 2 в Океании.

Однако страны стремятся поддерживать развитие не только в крупных городах. В частности, в России в рамках проекта «Умный город» в индексе цифровизации городов за 2021 год выделено 203 города¹⁶⁶. Поддержка цифровизации осуществляется не только в отношении городских округов и городских поселений. В рейтинге лучших муниципальных практик за 2021 год, например поселение Сингапай Ханты-Мансийского автономного округа – Югра внедрило систему видеонаблюдения на улицах, в то время как в поселении Нововеличковское Краснодарского края освещенность улиц была повышена до 80 процентов¹⁶⁷. Победители получают от Минстроя России дотации на развитие цифровизации, однако по содержанию поданных проектов очевидно, что потребности муниципальных образований в цифровизации неоднородны.

Во Франции централизованное содействие территориальным общностям в цифровизации осуществляет Банк территорий, действующий в составе Фонда депозитов и консигнаций (Caisse des Dépôts et Consignations). Банк территорий

¹⁶⁴ См. Минстрой России. Базовые и дополнительные требования к умным городам (стандарт «Умный город»). URL: <https://minstroyrf.gov.ru/docs/18039/> (дата обращения: 05.03.2023). Дата опубликования: 04.03.2019.

¹⁶⁵ UN E-Government Survey 2022. P. 88. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%203.pdf> (дата обращения: 05.03.2023).

¹⁶⁶ IQ городов. Проект «Умный город». URL: <https://russiasmartcity.ru/iq#statistics> (дата обращения: 05.03.2023).

¹⁶⁷ Сборник лучших муниципальных практик по итогам 2021 года. URL: <https://russiasmartcity.ru/documents> (дата обращения: 05.03.2023).

осуществляет содействие как в виде выделения финансирования (инвестиции или займы), так и посредством предоставления иной помощи заинтересованным территориальным общностям¹⁶⁸. Французская модель цифровизации местного самоуправления ориентирована в сторону развития экономики данных и организации оборота данных местного самоуправления. Например, в департаменте Луаре путем объединения более чем 24 тысяч данных была создана более детальная статистика несчастных случаев на дорогах¹⁶⁹, а сообщество агломераций Страны Басков организовало портал открытых данных агрикультуры¹⁷⁰.

В США правовой статус муниципальных образований и пределы их компетенции полностью определяется соответствующим штатом¹⁷¹. Цифровизация муниципалитетов централизованно не координируется на федеральном уровне и в большей степени основана на участии частного сектора и обмене лучшими практиками. В частности, Фонд Блумберга организовал создание проекта «What Works Cities», который предоставляет городам с населением более 30 тысяч человек возможность обмениваться опытом цифровизации и получать сертификацию соответствия¹⁷². Согласно отчету компании Deloitte более 200 городов участвуют в проекте, из которых 32.7 % составляют города с населением менее 100 тысяч человек¹⁷³.

¹⁶⁸ Collectivités locales : bénéficiez d'outils digitaux de diagnostics pour la réalisation de vos projets. URL: <https://www.banquedesterritoires.fr/solutions-diagnostic-gestion-territoriale-collectivites> (дата обращения: 05.03.2023).

¹⁶⁹ En croisant les données, le Loiret identifie les zones accidentogènes de son réseau routier. Publié le 9 mars 2021. URL: <https://www.banquedesterritoires.fr/en-croisant-les-donnees-le-loiret-identifie-les-zones-accidentogenes-de-son-reseau-routier> (дата обращения: 05.03.2023).

¹⁷⁰ Une plateforme open data au service des agriculteurs en Pays basque. URL: <https://www.banquedesterritoires.fr/une-plateforme-open-data-au-service-des-agriculteurs-en-pays-basque-64> (дата обращения: 05.03.2023). Дата опубликования: 18.10.2021.

¹⁷¹ Vanlandingham K.E. Municipal Home Rule in the United States // William & Mary Law Review. 1968. Vol. 10. Issue 2. P. 269–314.

¹⁷² About What Works Cities. URL: <https://whatworkscities.bloomberg.org/about/> (дата обращения: 05.03.2023).

¹⁷³ Closing the Data Gap: How Cities Are Delivering Better Results for Residents. June 30, 2021. URL: <https://results4america.org/tools/closing-the-data-gap-how-cities-are-delivering-better-results-for-residents/#:~:text=Public%20engagement%3A%20The%20percentage%20of,from%2018%25%20to%2067%25> (дата обращения: 05.03.2023).

Для управления информационными ресурсами в составе местной администрации некоторых городов также могут образовываться отдельные органы, курирующие вопросы развития технологий и цифровизации. В частности, в Казани действует Управление информационных технологий и связи в составе Исполнительного комитета¹⁷⁴. В городе Нью-Йорке в составе местной администрации действует Управление технологий и инноваций, включившее в себя предшествующие управления, занимающиеся вопросами управления данными, кибербезопасности, информационной приватности¹⁷⁵.

Усиление федерализма в развитии информационных технологий местного уровня может приводить и к излишней децентрализации, препятствующей более оперативному и эффективному внедрению информационных технологий в деятельность органов публичной власти. В Германии, где централизованно планировалось введение 575 сервисов на всех уровнях государственного управления к 2022 году, такое внедрение не удалось из-за отсутствия соответствующей координации¹⁷⁶.

Сравнительный анализ позволяет выделить две модели развития цифровизации муниципальных образований: модель централизованного регулирования, предполагающая участие центральных органов государственной власти в стимулировании и поддержке цифровизации муниципалитетов (Россия, Франция), и модель саморегулирования, предоставляющая возможность муниципалитетам самостоятельно обмениваться лучшими практиками и формировать стандарты цифровизации (США). Централизованная координация цифровизации муниципальных образований позволяет более эффективно организовать обмен данными между различными уровнями власти.

¹⁷⁴ Управление информационных технологий и связи Исполнительного комитета г. Казани. URL: <https://kzn.ru/meriya/ispolnitelnyy-komitet/uits/> (дата обращения: 05.03.2023).

¹⁷⁵ The City of the New York. Office of the Mayor. Executive order № 3. January 19, 2022 URL: <https://www.nyc.gov/assets/home/downloads/pdf/executive-orders/2022/eo-3.pdf> (дата обращения: 05.03.2023).

¹⁷⁶ Bartholomae F.W., Nam Ch.W., Steinhoff P. Does Federalism Affect E-Government in Germany? // CESifo Working Paper. 2023. № 10260.

Взаимоотношения центрального аппарата государственных органов исполнительной власти и органов нижестоящего уровня в рамках развития экономики данных основаны на формировании сетевого взаимодействия, позволяющего обмениваться данными, возникающими в деятельности органов местного самоуправления и органов субъектов Российской Федерации.

Таким образом, распределение функций государственного управления между органами публичной власти, регулирующими информационную сферу, осуществляется на основе сочетания централизации и децентрализации. Децентрализация необходима для обеспечения независимости принятия органом решений по вопросам регулирования с учетом профессиональной компетенции (децентрализация на одном уровне власти) либо с учетом интересов и потребностей населения (децентрализация по территориальному признаку), в то время как централизация позволяет осуществлять единое регулирование по значимым направлениям государственной политики в информационной сфере. Вместе с тем, заметна тенденция к укреплению полномочий и развитию роли федеральных органов исполнительной власти в системе публичной власти в рамках регулирования информационной сферы.

ГЛАВА 2. ПОЛНОМОЧИЯ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Не только рассмотренные ранее особенности организации системы органов исполнительной власти определяют их правовой статус в информационной сфере. Ключевым элементом правового статуса органов исполнительной власти является характеристика их полномочий в информационной сфере¹⁷⁷.

Для сравнительного исследования целесообразно выделить полномочия органов исполнительной власти в информационной сфере, в отношении которых может быть проведено сопоставление с зарубежным опытом.

В первую очередь, нормотворческая и правоприменительная деятельность органов исполнительной власти оказывают непосредственное воздействие на информационную сферу и определяют ее регулирование. В дополнение полномочия органов исполнительной власти в сфере оказания государственных услуг в электронной форме и электронных государственных услуг наиболее полно отражают характеристику деятельности органов исполнительной власти в информационной сфере в контексте их прав и обязанностей в отношении невластных субъектов. Значимым элементом правового статуса органа исполнительной власти в информационной сфере являются его обязанности в сфере информационной безопасности. Наконец, необходимость реагирования органов исполнительной власти на размещение противоправной информации приводит также к развитию новых полномочий органов исполнительной власти в части применения мер административного принуждения в информационной сфере.

¹⁷⁷ В нормативно-правовых актах и правовой литературе функции и полномочия органов исполнительной власти часто отождествляются (напр.: Смирнова А.А. О соотношении государственных услуг, функций и полномочий органов исполнительной власти // Журнал российского права. 2015. № 3. С. 120 - 130). Однако подходы к пониманию функций государственного управления и их классификации многообразны. В проводимом исследовании автор рассматривает полномочия органов исполнительной власти как их права и обязанности, не отождествляя полномочия органа исполнительной власти и функции государственного управления.

2.1. Нормотворческая деятельность

Страны следуют разным подходам в законодательном регулировании информационной сферы. В России действует федеральный закон, определяющий общий правовой режим информации – Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁷⁸. Разработанные правовой доктриной категории и основные положения, нашедшие отражение в указанном законе, позволяют более эффективно регулировать информационную сферу в целом. Однако указанный закон постоянно дополняется и уточняется – за период его действия было принято 65 федеральных законов, вносящих в него изменения. Что свидетельствует о расширении регулирования информационной сферы законодателем.

Во Франции можно выделить два ключевых закона, регулирующих информационную сферу – Закон об информатике и свободах 1978 года¹⁷⁹, посвященный персональным данным, и Закон о доверии в цифровой экономике 2004 года¹⁸⁰, посвященный различным аспектам информационного взаимодействия, включая особенности ограничения доступа к запрещенной информации.

В США количество законов, непосредственно регулирующих информационную сферу, сложно однозначно определить ввиду множества законодательных актов. Законы посвящаются отдельным сферам: доступу к информации о деятельности государственных органов, открытым данным в публичном секторе, электронным подписям. Многие принимаемые законы в США зачастую регулируют деятельность федеральных агентств, что необходимо для возложения новых полномочий на независимые агентства.

¹⁷⁸ Российская газета, № 165, 29.07.2006.

¹⁷⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article20> (дата обращения: 05.03.2023).

¹⁸⁰ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/> (дата обращения: 05.03.2023).

Другим показателем деятельности законодателя по регулированию информационной сферы является наличие в структуре соответствующих палат отдельных комитетов и комиссий, занимающихся вопросами регулирования информационной сферы.

В Российской Федерации вопросами цифровизации занимаются комитеты обеих палат парламента, однако специализированный комитет функционирует именно на уровне Государственной думы Российской Федерации. В Государственной думе Российской Федерации с 2012 года действует Комитет Государственной Думы по информационной политике, информационным технологиям и связи¹⁸¹, в рамках деятельности которого были подготовлены ключевые законопроекты в развитии правового регулирования информационной сферы¹⁸². В Совете Федерации отсутствует специализированный на цифровизации отдельный комитет и вопросы цифровизации рассматриваются каждым комитетом применительно к его сфере ведения. Работа в сфере правового регулирования цифровизации осуществляется Комитетом Совета Федерации по конституционному законодательству и государственному строительству¹⁸³.

Во Франции, в отличие от России, на уровне обеих палат не созданы постоянные комиссии по цифровизации. На уровне Сената действует специальная

¹⁸¹ Официальная страница Комитета Государственной Думы по информационной политике, информационным технологиям и связи. URL: <http://www.komitet4-4.km.duma.gov.ru/Polozhenie> (дата обращения: 05.03.2023).

¹⁸² В частности, указанный комитет разработал законопроект, предусматривающий обязанность оператора персональных данных локализовать персональные данные на территории Российской Федерации, а также законопроект, установивший специальную подсудность московскому городскому суду дел о нарушении авторских прав в сети Интернет в случае применения досудебных обеспечительных мер. См.: Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ. URL: <http://publication.pravo.gov.ru/Document/View/0001201407220042> (дата обращения: 16.05.2023); Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» от 24.11.2014 № 364-ФЗ. URL: <http://publication.pravo.gov.ru/Document/View/0001201411250005?index=12&rangeSize=1> (дата обращения: 16.05.2023).

¹⁸³ Официальная страница Комитета Совета Федерации по конституционному законодательству и государственному строительству. URL: <http://legislation.council.gov.ru> (дата обращения: 05.03.2023).

группа исследований – Цифровая группа¹⁸⁴. Отдельно также действует Комиссия по культуре, образованию и коммуникациям¹⁸⁵. Общие вопросы цифровизации государственного управления рассматриваются также Комиссией по конституционным законам, законодательству, всеобщему избирательному праву и общей администрации¹⁸⁶. В частности, указанная комиссия рассматривала необходимость предотвращения рисков биометрического распознавания лиц в публичном пространстве¹⁸⁷. На уровне Национальной Ассамблеи не образовано специальных постоянных комиссий по цифровизации. Цифровизация рассматривается различными комиссиями. Например, в составе Комиссии по экономическим делам образована рабочая группа, занимающаяся вопросами общего обслуживания электронных коммуникаций¹⁸⁸.

В США, как и во Франции, также не образованы отдельные специализированные комитеты, однако в составе комитетов более широкого профиля учреждаются профильные подкомитеты в информационной сфере. В Палате представителей отсутствуют специализированные на цифровизации комитеты, однако в составе комитета по энергетике и торговле действует подкомитет о коммуникациях и технологиях. В частности, в 2022 году комитет по энергетике и торговле подготовил пять законов в сфере телемедицины в интересах пациентов, страдающих лимфедемой¹⁸⁹. Комитет науки, космоса и технологий

¹⁸⁴ Sénat. Groupe Numérique. URL: https://www.senat.fr/groupe-etude/etu_1008.html (дата обращения: 05.03.2023).

¹⁸⁵ Sénat. Commission de la culture, de l'éducation et de la communication. URL: <https://www.senat.fr/commission/cult/index.html> (дата обращения: 05.03.2023).

¹⁸⁶ Sénat. Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale. URL: <https://www.senat.fr/commission/loi/index.html> (дата обращения: 05.03.2023).

¹⁸⁷ Daubresse M.-Ph., de Belenet A. et Durain J. La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance. Rapport d'information, fait au nom de la commission des lois. № 627 (2021-2022). 10 mai 2022. URL: <http://www.senat.fr/notice-rapport/2021/r21-627-notice.html> (дата обращения: 05.03.2023).

¹⁸⁸ Assemblée nationale. Commission des affaires économiques. URL: [https://www2.assemblee-nationale.fr/15/commissions-permanentes/commission-des-affaires-economiques/\(block\)/54070](https://www2.assemblee-nationale.fr/15/commissions-permanentes/commission-des-affaires-economiques/(block)/54070) (дата обращения: 08.08.2022).

¹⁸⁹ Pallone Applauds Committee Passage of Five Health and Telecommunication Bills. URL: <https://energycommerce.house.gov/newsroom/press-releases/pallone-applauds-committee-passage-of-five-health-and-telecommunication> (дата обращения: 08.08.2022).

также рассматривает отдельные специальные вопросы цифровизации – например, вопрос кибербезопасности пространственных систем¹⁹⁰. В Сенате в составе Комитета по торговле, науке и транспорту образованы два подкомитета – подкомитет коммуникаций, медиа и вещания и подкомитет защиты прав потребителей, безопасности продуктов и безопасности данных¹⁹¹. Указанный комитет взаимодействует с Федеральной торговой комиссией в том числе по вопросам обработки потребительских данных. На уровне представителей указанных комитетов Сената и Палаты представителей был разработан проект Американского закона о приватности и защите данных¹⁹².

Несмотря на активность законодательных органов в регулировании отдельных аспектов информационной сферы, нормотворческая деятельность органов исполнительной власти в рамках регулирования информационной сферы не теряет своей значимости, что обосновывается способностью более оперативно реагировать на возникающие изменения.

Централизованный или децентрализованный подходы к законодательному регулированию информационной сферы при этом не влияют на нормотворческую деятельность органов исполнительной власти и главы государства.

Нормотворческая деятельность главы государства и органов исполнительной власти в рамках регулирования информационной сферы реализуется в зависимости от конституции и сложившихся в стране особенностей функционирования центрального аппарата.

Нормативные акты могут носить характер «замещающего» законодательства, временно определяющего регулирование отдельного направления информационной сферы до принятия соответствующего

¹⁹⁰ Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems. URL: <https://science.house.gov/hearings/exploring-cyber-space-cybersecurity-issues-for-civil-and-commercial-space-systems> (дата обращения: 08.08.2022).

¹⁹¹ Senate. List of the committees for the 117th Congress. URL: <https://www.senate.gov/committees/> (дата обращения: 08.08.2022).

¹⁹² American Data Privacy and Data Protection Act. Draft Legislation. Section by section summary. URL: <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50> (дата обращения: 08.08.2022).

регулируемого законодателем, обладать автономным статусом, не требующим дополнительного регулирования законодателем, либо носить подзаконный характер.

В порядке автономного регулирования глава государства в США принимает акты, определяющие особенности оборота информации ограниченного доступа. В США правовой режим государственной тайны¹⁹³ и служебной тайны (контролируемой неклассифицированной информации)¹⁹⁴ определены исполнительными указами президента, имеющими автономный характер. Однако в целом акты, принимаемые главой государства в США или органами из его аппарата, направлены на регулирование деятельности федеральных или исполнительных агентств в информационной сфере¹⁹⁵. За период с 2017 по начало 2023 года главой государства в США принято 14 актов, регулирующих деятельность федеральных агентств в информационной сфере.

В Российской Федерации также указом Президента определен перечень конфиденциальной информации¹⁹⁶. Однако соответствующие меры можно охарактеризовать как временные, вводимые до принятия специального закона. Хотя глава государства в России, в отличие от США, не относится к исполнительной власти, автономное регулирование информационной сферы Президентом Российской Федерации также не осуществляется.

В отличие от России и США, правовая система Пятой Французской республики, усиливающая полномочия главы государства, допускает и иной

¹⁹³ Executive Order № 13526. Classified National Security Information. December 29, 2009. URL: <https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information> (дата обращения: 05.03.2023).

¹⁹⁴ Executive Order № 13556. Controlled Unclassified Information. URL: <https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information> (дата обращения: 05.03.2023).

¹⁹⁵ Вопрос о пределах полномочий главы государства носит дискуссионный характер в правовой доктрине США: сформированы как подходы, отрицающие дополнительные полномочия президента, не предусмотренные законом или конституцией, так и альтернативные подходы. См.: Chemerinsky E. Constitutional law: principles and policies. Fifth Edition. 2015.

¹⁹⁶ Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102046005> (дата обращения: 05.03.2023).

формат «замещающего» законотворчества главой государства. В соответствии со статьей 38 Конституции правительство вправе по согласованию с парламентом для реализации своей программы принимать ордонансы, относящиеся обычно к сфере законодателя, на ограниченный срок. За период с 2021 года по сентябрь 2022 года Президентом Франции приняты 10 ордонансов по вопросам регулирования информационной сферы, два из которых направлены на имплементацию в национальное законодательство актов Европейского союза.

Нормотворческая деятельность правительства в странах со смешанной формой правления (Россия, Франция) в рамках регулирования информационной сферы направлена на уточнение процедурных особенностей реализации правовых норм, закрепленных в законе. Реализация одного закона предполагает принятие множества подзаконных актов, более детально регулирующих процедуры его применения. К примеру, в России в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁹⁷ содержится около 70 отсылок к нормативным актам, принимаемым органами исполнительной власти. Во Франции Закон о доверии в цифровой экономике 2004 года¹⁹⁸ содержит около 19 отсылок к подзаконному регулированию.

Автономное регулирование информационной сферы нормативными актами правительства менее распространено и используется для устранения пробелов, возникших в ходе реализации положений закона. В частности, во Франции статья 6-1 Закона Франции о доверии в цифровой экономике предусматривала особый порядок внесудебной блокировки ресурсов, содержащих террористический контент и детскую порнографию. Статья не упоминала ограничение доступа к неправомерному контенту операторами поисковых сервисов, однако соответствующие требования были установлены отдельным декретом Премьер-министра¹⁹⁹.

¹⁹⁷ Российская газета, № 165, 29.07.2006.

¹⁹⁸ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/> (дата обращения: 05.03.2023).

¹⁹⁹ Décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à

В большинстве случаев законодатель делегирует полномочия по принятию подзаконного регулирования именно правительству. Таким образом, в рамках подзаконного регулирования информационной сферы сохраняется централизованный подход.

Нормотворческую деятельность министерств и ведомств можно охарактеризовать путем анализа актов в одной из наиболее значимых сфер регулирования общественных отношений с использованием информационных технологий – персональных данных. Анализ полномочий органов по защите персональных данных в рассматриваемых странах показывает, что непосредственно подзаконное нормотворчество указанных органов немногочисленно.

В Российской Федерации возможность отдельного органа принимать подзаконное регулирование по своему усмотрению за счет широких формулировок закона ограничена. Общий подход строится на подчиненном понимании подзаконного творчества по отношению к закону, ограниченности подзаконного творчества²⁰⁰. Роскомнадзор как орган по защите персональных данных самостоятельно издает подзаконные акты только в случаях, прямо предусмотренных соответствующим законом. Например, в соответствии с частью 9 статьи 9 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ Роскомнадзор утвердил требования к содержанию согласия на распространение персональных данных²⁰¹.

Аналогичный подход используется во Франции. Национальная комиссия по информатике и свободам Франции не принимает подзаконных актов в сфере

caractère pornographique. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000030315053/#LEGIARTI000030315053> (дата обращения: 05.03.2023).

²⁰⁰ Абрамова А.И. Подзаконное правотворчество в современном понимании: реалии и перспективы // Журнал российского права. 2019. № 8. С. 25–35.

²⁰¹ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». URL: <http://publication.pravo.gov.ru/Document/View/0001202104210039> (дата обращения: 05.03.2023).

персональных данных. Это можно объяснить гармоничным внедрением французскими юристами независимых ведомств в систему разделения властей. С одной стороны, акты Комиссии часто обжалуются в Государственный совет Франции и его участие в формировании устойчивых правовых позиций в отношении защиты персональных данных сохраняется. С другой стороны, в силу прямой имплементации норм европейского права в национальное в дополнительном подзаконном регулировании отсутствует необходимость. Более широкое развитие получает деятельность Комиссии по опубликованию разъяснений, представлению мнений по законопроектам и отдельным административным действиям.

В США Федеральная торговая комиссия не устанавливала отдельного регулирования для защиты персональных данных в потребительском секторе, хотя отдельные положения в части персональных данных содержатся в некоторых нормативных актах Федеральной торговой комиссии. Например, Федеральная торговая комиссия утвердила постановление в сфере телемаркетинга, которое запрещает перезванивать абоненту, если он отказался от получения маркетинговых звонков (§ 310.4, (b), (iii), (A))²⁰². Однако Федеральная торговая комиссия может издавать нормативные акты по предмету своего ведения, в том числе в части персональных данных в потребительском секторе. Нормативный акт агентства некоторые американцы рассматривают как более предпочтительный закону, поскольку законодательное регулирование представляет собой менее гибкий процесс. Например, осенью 2021 года сенаторы обращались к Федеральной торговой комиссии с просьбой разработать постановление о регулировании персональных данных в потребительском секторе²⁰³.

Малая доля нормативных актов, принимаемых органами по защите персональных данных, не свидетельствует об ослаблении их роли в регулировании

²⁰² FTC. Telemarketing Sales Rule. US Code of Federal Regulations. Aug. 10, 2010. URL: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-310> (дата обращения: 05.03.2023).

²⁰³ Senator Blumenthal, et al., Letter to Federal Trade Commission Chair Lina Khan (Sept. 20, 2021). URL: <https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf> (дата обращения: 05.03.2023).

информационной сферы. За счет снижения роли судов в установлении толкования принимаемых законов правоприменительная деятельность органов по защите персональных данных получает все большее нормативное значение²⁰⁴. Кроме того, особенность юридической техники формирующегося законодательства в информационной сфере зачастую требует дополнительного толкования, устраняющего очевидные пробелы и противоречия в регулировании²⁰⁵.

Административные процедуры принятия органами по защите персональных данных решений о применении мер административного принуждения различаются. В США и Франции, где действуют независимые органы, принятие решений осуществляется с соблюдением отдельной «квазисудебной процедуры». В России установлен судебный порядок назначения административного наказания за нарушения в сфере персональных данных, однако общая доля судебных решений немногочисленна по отношению к количеству предписаний, выдаваемых органом.

Отсутствие участия судебных органов в контроле за деятельностью органов по защите персональных данных приводит к усилению централизации в регулировании информационной сферы. Данная тенденция характерна для США и России, в то время как во Франции участие административного судьи в определении толкования применимого законодательства более распространено.

Само по себе формальное установление судебного порядка принятия решений о применении мер административного принуждения не является препятствием к централизации полномочий по регулированию персональных данных в деятельности органа исполнительной власти. В Российской Федерации

²⁰⁴ Уместно привести цитату известного немецкого юриста Г. Кельзена: «Если государство, чьи внутренние функции ограничиваются законодательной деятельностью, судопроизводством и реализацией санкций, характеризуется как судебное государство, то можно сказать, что с установлением непосредственного государственного управления оно превращается в судебно-административное государство». Кельзен Г. Чистое учение о праве. 2-е изд / пер. с нем. М.В. Антонова и С.В. Лёзова. СПб.: ООО Издательский Дом «Алеф-Пресс», 2015. С. 363.

²⁰⁵ См.: Архипов В.В. Семантические пределы права в условиях медиального поворота: теоретико-правовая интерпретация: дис. ... д.ю.н. Санкт-Петербург, 2019. С. 22: «...уже сейчас российское (и не только) законодательство содержит множество норм, в отношении которых можно ставить вопрос о пределах их применения с точки зрения здравого смысла, поскольку иное применение и толкование будет абсурдным».

для применения мер административного наказания, предусмотренных статьей 13.11 Кодекса об административных правонарушениях Российской Федерации²⁰⁶, используется судебная процедура в соответствии с частью 1 статьи 23.1 указанного кодекса. В рамках досудебной процедуры должностные лица органа по защите персональных данных составляют протокол по факту выявления нарушения, в том числе в рамках контрольно-надзорных мероприятий, на основании которого возбуждается административное производство по делам об административных правонарушениях.

Однако фактически, несмотря на судебную процедуру применения мер наказания, в Российской Федерации судебная практика по персональным данным немногочисленна, а основная деятельность по регулированию осуществляется Роскомнадзором в рамках проведения профилактических и контрольно-надзорных мероприятий. Анализ статистики правоприменительной практики, проведенный Роскомнадзором за 2020-2021 годы, показывает, что в большинстве случаев суды отказывают в применении мер административного наказания по причине пропуска срока привлечения к ответственности либо малозначительности.

Например, согласно статистике Роскомнадзора в 2017 году²⁰⁷ органом было составлено 7103 протокола об административных правонарушениях в сфере персональных данных, из которых было составлено всего 65 протоколов непосредственно по статье 13.11 КоАП РФ, а большая часть протоколов была составлена по факту непредоставления или неполного предоставления сведений Роскомнадзору (6988 протоколов по статье 19.7 КоАП РФ). В 2019 году по статье 13.11 КоАП РФ Роскомнадзором было составлено 215 протоколов об административном правонарушении, при этом по статье 19.7 КоАП РФ было возбуждено 5191 дело²⁰⁸. В 2020 году Роскомнадзор составил 162 протокола о

²⁰⁶ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 1.

²⁰⁷ Обзор правоприменительной практики контрольно-надзорной деятельности в 2017 году (утвержден Приказом Роскомнадзора от 19.02.2018 № 31). URL: <https://rkn.gov.ru/p582/p984/> (дата обращения: 05.03.2023).

²⁰⁸ Обзор правоприменительной практики контрольно-надзорной деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за

нарушениях по статье 13.11 КоАП РФ, отмечая, что при этом было вынесено 4353 определения об отказе, в том числе в силу истечения сроков привлечения к ответственности²⁰⁹. В 2021 году Роскомнадзором было составлено в общей сложности 100 протоколов о нарушениях в сфере персональных данных, из которых протоколы по статье 19.7 КоАП РФ, по отчету органа, занимали наибольшую часть²¹⁰.

Наиболее распространенными индивидуальными юрисдикционными административными актами Роскомнадзора являются предписания, выдаваемые в рамках проведения контрольно-надзорных мероприятий. Например, в 2021 году территориальными органами Роскомнадзора выдано 475 предписаний об устранении нарушений законодательства о персональных данных²¹¹ при том, что непосредственно протоколов о выявлении нарушений было составлено 100 за указанный период.

Таким образом, несмотря на судебный порядок привлечения к ответственности за административные правонарушения в сфере персональных данных, Роскомнадзор сохраняет позицию в качестве основополагающего регулятора в сфере персональных данных за счет более распространенных мер досудебного административного принуждения в рамках контрольно-надзорной деятельности.

В США регулирование обработки персональных данных в потребительском секторе осуществляется Федеральной торговой комиссией. Пример США

2019 год (утвержден Приказом Роскомнадзора от 28.02.2020 № 25). URL: https://rkn.gov.ru/docs/obzor_2019_1.pdf (дата обращения: 05.03.2023).

²⁰⁹ Обзор правоприменительной практики контрольно-надзорной деятельности в 2020 году (утвержден Приказом Роскомнадзора от 26.02.2021 № 19). URL: https://rkn.gov.ru/docs/obzor_pravoprimereneniya_2020.pdf (дата обращения: 05.03.2023).

²¹⁰ Доклад о правоприменительной практике организации и проведения федерального государственного контроля (надзора) за обработкой персональных данных в 2021 году (Приложение № 2 к Приказу Роскомнадзора от 31.03.2022 № 55). URL: https://rkn.gov.ru/docs/doklad_po_pravoprimereniju_2022_PD.pdf (дата обращения: 05.03.2023).

²¹¹ Роскомнадзор. Доклад о видах государственного контроля (надзора) в 2021 году. URL: https://rkn.gov.ru/plan-and-reports/reports/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 05.03.2023).

показывает, что широкое толкование полномочий органа исполнительной власти позволяет такому органу самостоятельно определять регулирование информационной сферы, не принимая дополнительных нормативных правовых актов.

XX век в истории административного аппарата США характеризуется массовым созданием большого количества независимых агентств на основании законодательных актов Конгресса и усилением тенденций бюрократизации²¹². Поскольку независимые агентства получали свободу не только в сфере исполнительной деятельности по применению права, но фактически осуществляли квазисудебные и нормотворческие функции, самостоятельно создавая толкование права и вынося решение на его основе, для США осталась характерной проблема контроля за толкованием и нормотворческой деятельностью агентств²¹³.

Компетенция Федеральной торговой комиссии США в сфере регулирования защиты персональных данных в потребительских отношениях сформировалась в силу нескольких факторов. С появлением сети Интернет в 1990-х годах изначально в рамках осуществления коммуникаций в академической среде использование всемирной сети в коммерческих целях не предполагалось, пока администрация президента Дж. Буша не изменила подход²¹⁴. Коммерческое использование сети уже предполагало сбор данных пользователей с последующим использованием их в коммерческих целях. Поскольку законодательное регулирование отсутствовало, индустрия в рамках саморегулирования начала создавать и размещать политики конфиденциальности сайтов, следуя общему подходу необходимости уведомления пользователя об особенностях обработки его данных, выраженному в 1973г. Департаментом США в сфере здравоохранения, образования и общественного

²¹² История государства и права зарубежных стран: Учебник для вузов. В 2 ч. Ч. 2 / под общ. ред. д.ю.н. проф. О.А. Жидкова и д.ю.н. проф. Н.А. Крашенинниковой. 2-е изд. стер. М.: Норма, 2003. С. 248 – 251. 702 с.

²¹³ Barkow R.E. The Ascent of the Administrative State and the Demise of Mercy // Harvard Law Review. Vol. 121. 2008. P. 1332–1365.

²¹⁴ Hetcher S. The De Facto Federal Privacy Commission // J. Marshall J. Computer & Info. L. V. 19. Issue 1. 2000. P. 110. URL: поудаляйте везде лишние пробелы <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1152&context=jitpl> (дата обращения: 05.03.2023).

благополучия²¹⁵ и воспринятому в международном сообществе²¹⁶. С. Хетчер обратил внимание, что сформировавшийся подход к опубликованию политик конфиденциальности менее выгоден для пользователей, чем для самих компаний. Опубликование политик конфиденциальности, по мнению исследователя, было выгодно многим компаниям, во-первых, поскольку каждая из них заинтересована в том, чтобы у другой компании была политика конфиденциальности. Если бы компании не выкладывали политику конфиденциальности, могла бы появиться одна компания с более открытой политикой об использовании пользовательских данных, а другие были бы вынуждены разместить свои. Во-вторых, отсутствие политики конфиденциальности позволило бы пользователю сослаться на деликт в сфере приватности, поскольку без надлежащего разъяснения об особенностях использования его данных пользователь не мог иметь разумного ожидания приватности²¹⁷.

Появление политик конфиденциальности в сфере саморегулирования вызывало трудности в их правовой квалификации и выборе подходящего механизма защиты прав пользователя²¹⁸. Одним из возможных средств защиты в случае перепродажи собранных пользовательских данных могло быть применение компенсации за деликт присвоения, состоящий в использовании третьим лицом имени или внешности другого лица для получения собственной выгоды²¹⁹. Однако в деле *Shibley v. Time, Inc.* Апелляционный суд штата Охайо указал, что право на приватность не распространяется на передачу списков адресов для рекламной

²¹⁵ U.S. Dep't of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 41–42. 1973. URL: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> (дата обращения: 05.03.2023).

²¹⁶ OECD Recommendation of The Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 23 September 1980. URL: <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm> (дата обращения: 05.03.2023).

²¹⁷ Hetcher S. The De Facto Federal Privacy Commission. Op. cit. P. 119–120.

²¹⁸ Solove D.J., Hartzog W. The FTC and the New Common Law of Privacy // *Columbia Law Review*. Vol. 114. 2014. P. 583–676.

²¹⁹ Restatement of the Law, Second, Torts, § 652C. The American Law Institute. 1977. URL: https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (дата обращения: 05.03.2023); См.: Barbas S. From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption // *Buffalo Law Review*. 2013. Vol. 61. P. 1119–1189.

рассылки и деликт присвоения не применим²²⁰. Эта позиция была поддержана и в других штатах²²¹.

Другим возможным средством правовой защиты было бы признание политик конфиденциальности в качестве договоров. Однако возможность рассматривать политику конфиденциальности в качестве договора оставалась достаточно спорной, хотя в правовой литературе некоторые авторы высказывались в ее пользу²²². Договорные механизмы защиты, тем не менее, оказались неэффективными. Например, в деле *Dyer v. Northwest Airlines Corporations* в 2004г. Суд округа Северной Дакоты, рассматривая дело о передаче данных авиакомпанией о лицах, пользовавшихся услугами воздушной перевозки, государственным органам, указал, что политика конфиденциальности не может рассматриваться как договор, так же как и иные общие утверждения компаний о своей политике. Кроме того, даже если бы политика конфиденциальности была договором, заявитель не смог бы доказать убытки, возникшие вследствие передачи данных в его нарушение²²³.

Федеральная торговая комиссия в такой ситуации, еще в 1938г. получившая возможность рассматривать также дела о недобросовестных и вводящих в заблуждение практиках в сфере торговли²²⁴, оказалась подходящим органом для регулирования соблюдения компаниями размещенных ими политик конфиденциальности. Кроме того, принятый в 1998г. Закон о защите приватности

²²⁰ *Shibley v. Time, Inc.*, 45 Ohio App. 2d 69, 341 N.E.2d 337 (Ohio Ct. App. 1975). URL: https://casetext.com/case/shibley-v-time-inc/case-details?PHONE_NUMBER_GROUP=C (дата обращения: 05.03.2023).

²²¹ *Dwyer v. American Express Co.*, 273 Ill. App. 3d 742, 652 N.E.2d 1351 (Ill. App. Ct. 1995). URL: https://casetext.com/case/dwyer-v-american-express-co/case-details?PHONE_NUMBER_GROUP=C (дата обращения: 05.03.2023).

²²² Killingsworth S. *Minding Your Own Business: Privacy Policies in Principle and in Practice* // *Journal of Intellectual Property Law*. 1999. Vol. 7. Issue 1. P. 56–97.

²²³ *Dyer v. Northwest Airlines Corporations*, 334 F. Supp. 2d 1196 (D.N.D. 2004). URL: <https://law.justia.com/cases/federal/district-courts/FSupp2/334/1196/2520672/> (дата обращения: 05.03.2023).

²²⁴ The Wheeler-Lea Amendment to the Federal Trade Commission Act. 1938.

детей онлайн²²⁵ предоставлял комиссии право требовать размещения сайтами, нацеленными на работу с детьми, информации об использовании данных, и получения ими информированного согласия у родителей.

В условиях разрозненного регулирования для отдельных сфер полномочия комиссии оказывались недостаточно полными в общей сфере защиты персональных данных в США. Хотя комиссия могла требовать прямого соответствия у сайтов, направленных на детей, у нее не было полномочий предписывать организациям принятия политики конфиденциальности. Комиссия могла только выдать предписание, когда политика уже принята, но не соблюдается, поскольку такие действия подходили бы под недобросовестные и вводящие в заблуждение практики в сфере торговли²²⁶. В отчете Конгрессу от 2000г. комиссия указывала, что несмотря на активные действия по стимулированию компаний в порядке саморегулирования следовать добросовестным практикам в сфере информации, не все компании готовы следовать этому подходу²²⁷.

Прямое предписание раскрытия информации о передаче личных данных клиентов финансовыми организациями и принятия ими политик конфиденциальности было установлено также в Законе Грем-Лич-Блайли 1999г.²²⁸ Наконец, развитию саморегулирования и принятию организациями политик конфиденциальности способствовало принятие условий принципов защиты данных Safe Harbor, утвержденных Департаментом торговли США 21

²²⁵ Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. URL: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> (дата обращения: 05.03.2023).

²²⁶ Напр.: FTC. n the Matter of GEOCITIES, a corporation. File № 9823015. 1998. URL: <https://www.ftc.gov/sites/default/files/documents/cases/1998/08/geo-ord.htm> (дата обращения: 06.03.2023).

²²⁷ FTC. Privacy Online: Fair Information Practices in The Electronic Marketplace. A Report to Congress. May 2000. URL: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf> (дата обращения: 06.03.2023).

²²⁸ Gramm-Leach-Bliley Act. Public law 106–102. 106th Congress. Nov. 12, 1999. URL: <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf> (дата обращения: 06.03.2023).

июля 2000г.²²⁹ и пришедшим им на смену в 2016г. принципам Privacy Shield²³⁰. Хотя в 2020г. Европейский суд справедливости признал указанные принципы недействительными²³¹ для осуществления трансграничной передачи, использование европейскими компаниями других механизмов трансграничной передачи (например, стандартных условий передачи) сохранит обязанность для американских компаний в порядке саморегулирования придерживаться принципов, охватывающих уже сложившиеся принципы справедливых практик в сфере информации, попадая под компетенцию Федеральной торговой комиссии.

Подход США, в соответствии с которым допускается расширенное толкование агентством законодательства с осуществлением судебного контроля только в части обоснованности решения, если законодательство допускает такое широкое толкование, привел к возникновению нового правового регулирования, формируемого Федеральной торговой комиссией, в том числе на основании общей отсылки к осуществлению недобросовестных торговых практик. Компании также не заинтересованы в судебном оспаривании решений комиссии, предпочитая заканчивать административное дело соглашением с органом с обязательством по принятию надлежащих мер соблюдения прав субъектов персональных данных и выплатить штраф. В таком случае решения органа исполнительной власти становятся самостоятельной формой права, на которую ориентируются и практикующие юристы²³².

²²⁹ Safe Harbor Privacy Principles. Issued by the U.S. Department of Commerce on July 21, 2000. URL: <https://rm.coe.int/16806af271> (дата обращения: 06.03.2023).

²³⁰ EU-U.S. Privacy Shield Framework Principles. Issued by the U.S. Department of Commerce. URL: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> (дата обращения: 06.03.2023).

²³¹ CJUE. Arrêt de la Cour (grande chambre) du 16 juillet 2020. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems. Affaire C-311/18. URL: <https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgreg=fr&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=fr&avg=&cid=13413760> (дата обращения: 06.03.2023).

²³² Solove D.J., Hartzog W. Op. cit.

Например, в решении Федеральной торговой комиссии по делу компании Everalbum, Inc. от 06.05.2021²³³ административный орган предписал организации обеспечить получение согласий пользователей на использование технологий распознавания лица, а также подробно раскрыть пользователям информацию об особенностях использования их биометрических данных и удалить данные, в отношении которых согласие не было получено. Административный орган при этом ссылается на нарушение Закона о Федеральной торговой комиссии такими действиями, однако не приводит нормативного обоснования соответствия вменяемого деяния противоправному в силу положений указанного закона. Больше внимание уделено непосредственно содержанию предписания административного органа по устранению нарушения.

Обобщая, можно выделить следующие особенности деятельности Федеральной торговой комиссии в сфере регулирования персональных данных в потребительском секторе США. Во-первых, решение выносится органом в условиях соблюдения квазисудебной процедуры, предполагающей введение некоторых элементов состязательности в процедуру рассмотрения административного дела. Во-вторых, формирование императивных предписаний в данном случае возникает зачастую в силу соглашения между органом и организацией (consent order agreements). В-третьих, орган осуществляет дополнительный контроль за соблюдением выданного предписания путем возложения обязанности на организацию в определенный срок предоставить отчет о выполнении решения административного органа.

Франция, в отличие от США и России, сформировала более сбалансированный подход. Хотя принятие решения о применении мер административного принуждения за нарушения в сфере персональных данных осуществляется в административном порядке, Государственный совет Франции играет не меньшую роль в толковании применимого законодательства. Это объясняется изначальным подходом французских юристов к необходимости

²³³ FTC. In the Matter of Everalbum, Inc. 06.05.2021. URL: <https://www.ftc.gov/enforcement/cases-proceedings/1923172/everalbum-inc-matter> (дата обращения: 06.03.2023).

самостоятельного контроля администрацией принимаемых органами исполнительной власти актов, а также сосуществования мер административного принуждения и мер уголовной ответственности за совершение одного и того же нарушения в сфере персональных данных.

Французская модель вынесения органом по защите персональных данных актов индивидуального правоприменения также характеризуется рядом особенностей. Во-первых, правовой статус Национальной комиссии по информатике и свободам Франции определяется как национальным, так и наднациональным регулированием Европейского союза. В отличие от США, во Франции правовой режим персональных данных сформирован на уровне Закона об информатике и свободах²³⁴ и Регламента ЕС о защите персональных данных²³⁵. Во-вторых, во Франции существует судебный порядок обжалования решений органа по защите персональных данных. Наконец, во Франции помимо административных мер ответственности, налагаемых Национальной комиссией по информатике и свободам, действует также система уголовных наказаний за нарушения в сфере персональных данных.

Возможность вынесения Национальной комиссией по информатике и свободам Франции административных решений с привлечением к ответственности возникла во Франции достаточно поздно. Впервые указанные полномочия были внесены в Закон об информатике и свободах в 2004 году²³⁶ и ограничивались преимущественно возможностью наложения штрафа на нарушителя, предписания о запрете обработки персональных данных. Однако со временем перечень мер

²³⁴ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article20> (дата обращения: 06.03.2023).

²³⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE). URL: <http://data.europa.eu/eli/reg/2016/679/oj> (дата обращения: 06.03.2023).

²³⁶ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000006529399/2004-08-07/> (дата обращения: 06.03.2023).

административного принуждения, применяемых Национальной комиссией по информатике и свободам, расширился. Наделение Комиссии отдельными полномочиями по применению мер административного принуждения было обусловлено²³⁷ имплементацией Директивы ЕС о защите персональных данных²³⁸.

Особенности и перечень мер административного принуждения, которые может применять Национальная комиссия по информатике и свободам, перечислены в секции 3 Закона об информатике и свободах Франции²³⁹. В частности, предписания об устранении нарушений направляются председателем Национальной комиссии по информатике и свободам оператору персональных данных. Срок для устранения правонарушений определяется органом по защите персональных данных самостоятельно и в критичных ситуациях может составлять 24 часа. Возможность опубликования требования органа по защите персональных данных об устранении нарушений оставлена на усмотрение председателя.

Во Франции, помимо возможностей высоких административных штрафов и применения иных мер административного принуждения Национальной комиссией по информатике и свободам, сохраняется высокая степень криминализации правонарушений в сфере обработки персональных данных. Указанным уголовным правонарушениям²⁴⁰ посвящена секция V главы VI заголовка II книги II Уголовного кодекса Франции (статьи 226-16 – 226-24)²⁴¹. Например, уголовно наказуемы продолжение обработки после получения предписания Национальной комиссии по информатике и свободам о ее прекращении, неведение о

²³⁷ Communiqué de presse du Conseil des ministres du 18 juillet 2001. URL: <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000017759386/> (дата обращения: 06.03.2023).

²³⁸ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. URL: <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046> (дата обращения: 06.03.2023).

²³⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article20> (дата обращения: 06.03.2023).

²⁴⁰ Здесь и далее используется термин «уголовное правонарушение», поскольку французское уголовное прав различает три вида уголовных правонарушений, лишь одним из которых являются преступления (crimes).

²⁴¹ Code pénal. URL: <https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006165313/> (дата обращения: 06.03.2023).

нарушении законодательства о персональных данных, сбор персональных данных незаконным или обманным способом, обработка персональных данных для целей исследований в сфере здравоохранения без согласия таких лиц. В большинстве случаев уголовная ответственность физических лиц за совершение указанных правонарушений установлена в виде лишения свободы сроком на пять лет и штрафа в размере 300 тысяч евро. Исключение составляют уголовные правонарушения, направленные на препятствование деятельности Национальной комиссии по информатике и свободам, включая непредоставление информации по ее запросу. Ответственность за их совершение составляет один год лишения свободы и штраф в размере 15 тысяч евро (статья 226-22-2 Уголовного кодекса Франции). При вынесении приговора суд может также постановить о необходимости уничтожения всех персональных данных или их части, обрабатываемых нарушителем неправомерно.

Субъектами уголовной ответственности за нарушения в области персональных данных могут быть и юридические лица. При этом сумма штрафа для них увеличивается в пятикратном размере по отношению к размеру штрафа физических лиц (статьи 226-24, 131-38 Уголовного кодекса Франции), а также возможно применение иных мер, включая запрет на осуществление деятельности, запрет на продажу акций на фондовых рынках, конфискацию, обязанность опубликовать решение суда.

Таким образом, правоприменительная деятельность органов исполнительной власти в информационной сфере за счет усиления роли административного толкования может приобретать нормотворческий характер. На примере формирования компетенции Федеральной торговой комиссии США по регулированию персональных данных в потребительском секторе показано, что орган исполнительной власти может определять регулирование без издания отдельного нормативного акта в случаях, когда его полномочия намеренно широко определены законодателем. С другой стороны, российский подход с судебным порядком применения мер административного наказания также не препятствует усилению роли органа по защите персональных данных в толковании норм

действующего законодательства. Препятствием к усилению централизации регулирования информационной сферы является не возможность судебного обжалования актов органов по защите персональных данных, а фактическое участие судебных органов в формировании толкования принятого регулирования.

Другим фактором усиления роли административного толкования в информационной сфере является распространенность принятия органами исполнительной власти рекомендательных и разъяснительных актов.

Во всех рассматриваемых странах (США, Франция, Россия) признаны нормативные свойства рекомендательных и разъяснительных актов органа по защите персональных данных и выработаны определенные подходы к возможности обжалования их содержания.

В Российской Федерации рекомендательные акты в сфере персональных данных издаются Минцифры, и Роскомнадзор. Так, Роскомнадзором размещены разъяснения по обработке персональных данных в трудовых отношениях²⁴². Минцифры публиковало подробные разъяснения о локализации²⁴³. Разъяснения законодательства осуществляются органами не только путем размещения соответствующих рекомендаций, но и путем направления ответов на обращения граждан и организаций²⁴⁴.

Главенствующий в российской правовой практике подход исключает акты административного толкования из ряда нормативных, опираясь на формальные критерии: несоблюдение процедуры принятия нормативного акта, несоответствие полномочий. С одной стороны, такой подход освобождает суды от обязанности следовать разъяснениям органов исполнительной власти при принятии решений. С другой стороны, такой подход не снимает риски следования контролируруемыми

²⁴² Роскомнадзор. Разъяснения: Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве. URL: <https://pd.rkn.gov.ru/library/p195/> (дата обращения: 06.03.2023).

²⁴³ Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года. URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 06.03.2023).

²⁴⁴ Напр.: Письмо Роскомнадзора от 19.10.2021 № 08-71063 «О разъяснении законодательства» // СПС «КонсультантПлюс»; Письмо Роскомнадзора от 07.12.2021 N 08-82967 «О государственном контроле (надзоре) за обработкой персональных данных» // СПС «КонсультантПлюс».

субъектами подходу органа исполнительной власти, который может не соответствовать законодательству. Ключевое значение для формирования порядка судебного обжалования актов административного толкования имеет Постановление Конституционного Суда РФ от 31.03.2015 № 6-П, в котором суд отметил, что письма налогового органа могут обладать отдельными нормативными свойствами несмотря на то, что непосредственно не издаются как нормативно-правовой акт²⁴⁵. По результатам указанного рассмотрения законодатель предусмотрел отдельную процедуру обжалования актов, содержащих разъяснения законодательства и обладающих нормативными свойствами²⁴⁶.

Наличие формальной процедуры обжалования зачастую не приводит к полноценному пересмотру судами правовых позиций органов исполнительной власти. Верховным Судом РФ установлены критерии акта толкования, обладающего нормативными свойствами: «издание их органами государственной власти, органами местного самоуправления, иными органами, уполномоченными организациями или должностными лицами, наличие в них результатов толкования норм права, которые используются в качестве общеобязательных в правоприменительной деятельности в отношении неопределенного круга лиц»²⁴⁷.

Несмотря на подходящее определение актов административного толкования, судебная практика придерживается формализованного подхода. Например,

²⁴⁵ Постановление Конституционного Суда РФ от 31.03.2015 № 6-П «По делу о проверке конституционности пункта 1 части 4 статьи 2 Федерального конституционного закона «О Верховном Суде Российской Федерации» и абзаца третьего подпункта 1 пункта 1 статьи 342 Налогового кодекса Российской Федерации в связи с жалобой открытого акционерного общества «Газпром нефть»» // Российская газета, № 77, 13.04.2015.

²⁴⁶ Статья 217.1 Кодекса административного судопроизводства, статья 195.1 Арбитражного процессуального кодекса Российской Федерации, введенные в действие Федеральным законом от 15.02.2016 № 18-ФЗ «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации и Кодекс административного судопроизводства Российской Федерации в части установления порядка судебного рассмотрения дел об оспаривании отдельных актов» // Российская газета, № 33, 17.02.2016.

²⁴⁷ Пункт 3 Постановления Пленума Верховного Суда РФ от 25.12.2018 № 50 «О практике рассмотрения судами дел об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства и обладающих нормативными свойствами» // Российская газета, № 6, 15.01.2019.

Верховный Суд Российской Федерации отказался признавать письмо органа с ответом на обращение, содержащее толкование законодательства, нормативным по причине того, что письмо было ответом на обращение, в территориальные подразделения органа не направлялось. Факт размещения письма в справочно-правовых системах суд также не признал в качестве признака нормативности письма²⁴⁸. Традиционно практика по указанным делам не порождает отмены или признания недействительным соответствующего письма или разъяснительного документа органа. Суд ограничивается указанием на отсутствие нормативности письма, а затем отмечает, что по содержанию в письме не были выявлены отклонения от законодательства²⁴⁹.

В США менее распространено издание разъяснительных актов Федеральной торговой комиссией в рамках регулирования персональных данных в потребительском секторе. Более широкое значение имеет правоприменительная практика.

Наиболее известным рекомендательным документом Федеральной торговой комиссии, предопределившим формирование саморегулирования по защите персональных данных в потребительском секторе в США, является отчет 1998 года, где агентство изложило пять основополагающих принципов приватности²⁵⁰. В отсутствие законодательного и подзаконного регулирования указанные принципы фактически обеспечили единство подхода компаний к развитию политик конфиденциальности и систем защиты персональных данных в потребительском секторе США.

²⁴⁸ Решение Верховного Суда РФ от 16.06.2016 № АКПИ16-427 «Об отказе в удовлетворении заявления о признании недействующим письма ФНС России от 24.02.2016 № ГД-3-14/743@» // СПС «Консультант Плюс».

²⁴⁹ Напр.: Апелляционное определение Апелляционной коллегии Верховного Суда РФ от 02.03.2021 № АПЛ21-21 // СПС «КонсультантПлюс»; Апелляционное определение Апелляционной коллегии Верховного Суда РФ от 03.06.2021 № АПЛ21-171 // СПС «КонсультантПлюс».

²⁵⁰ FTC. Privacy Online: A Report to Congress. June, 1998. URL: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> (дата обращения: 06.03.2023).

Во Франции, наоборот, ввиду отсутствия полномочий по принятию нормативных правовых актов, регулирующих персональные данные, разъяснительные и рекомендательные акты органа по защите персональных данных более распространены. Французская модель предполагает не столько наделение независимого ведомства полномочиями подзаконного нормотворчества, сколько развитие у такого ведомства возможности путем предоставления мнений и разъяснений оказывать регулирующее воздействие на сферу компетенции.

В 2013 году Государственный совет Франции в ежегодном обзоре, посвященном «мягкому праву», выделил рекомендательные акты независимых административных ведомств в качестве административных актов «мягкого права», которые могут быть обжалованы наравне с обычными административными актами органов²⁵¹. Рекомендательные и разъяснительные акты Национальной комиссии по информатике и свободам обжалуются непосредственно в Государственный совет Франции.

Возможность обжалования разъяснительных документов позволяет Государственному совету осуществлять контроль за деятельностью Национальной комиссии по информатике и свободам и предотвращать возможную подмену актов административного толкования новыми положениями, не предусмотренными законодателем. Например, в 2020 году Государственный совет признал недействительными разъяснения Национальной комиссии по информатике и свободам о применении куки-файлов²⁵². В частности, Комиссия указала на запрет обуславливать использование сервиса согласием на обработку куки-файлов. Государственный совет посчитал, что Комиссия, устанавливая такой запрет, превысила свои полномочия, не установив надлежащего критерия для квалификации именно тех ситуаций, когда невозможность использования сервиса

²⁵¹ L'étude annuelle 2013 du Conseil d'État. Le droit souple. URL: <https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000280.pdf> (дата обращения: 06.03.2023).

²⁵² Conseil d'État 434684, lecture du 19 juin 2020. URL: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684> (дата обращения: 06.03.2023).

осуществляется в ущерб принципу свободы согласия на обработку персональных данных.

Таким образом, несмотря на активное участие законодателя в регулировании информационной сферы, в странах со смешанной формой правления (Россия, Франция) присутствует большая доля подзаконного регулирования, определяемого правительством. На нижестоящих уровнях не меньшую роль играет правоприменительная практика органа исполнительной власти. На примере сферы персональных данных показано, что правоприменительная деятельность также может приобретать нормотворческие черты. В таком случае усиливается централизация регулирования за счет совмещения органом исполнительной власти функций по контролю исполнения требований законодательства и принятию решений о наличии нарушений. Решением данной проблемы является развитие судебного контроля, способного установить более сбалансированный подход к толкованию законодательства и уменьшающего роль разъяснительных актов органов исполнительной власти.

2.2. Оказание государственных услуг

Оказание государственных услуг в электронной форме и электронных государственных услуг – ключевой аспект развития электронного правительства в России и за рубежом.

В первую очередь в электронную форму государствами переводятся услуги, связанные с взаимодействием с бизнесом и населением. В Европе среднее количество услуг, оказываемых в электронной форме, самое высокое и составляет в среднем 19, в Азии – 17, в Америке – 16, в Океании и Африке – 12²⁵³. Во всех

²⁵³ UN E-Government Survey 2022. P. 57. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%202.pdf> (дата обращения: 06.03.2023).

регионах в электронной форме доступны подача заявления о выдаче свидетельства о рождении и подача декларации о налогах.

Вопрос о целесообразности сохранения возможности для гражданина получить государственную услугу или ее результат в бумажной форме является дискуссионным. В зависимости от вида государственной или муниципальной услуги ее предоставление в настоящий момент может как не требовать, так и требовать личного посещения и предоставления либо получения документов на бумажном носителе.

Например, в Российской Федерации заявление на выдачу свидетельства о регистрации лица, совершающего операции по переработке средних дистиллятов, может быть подано и получено только в бумажной форме²⁵⁴. Свидетельство о регистрации по месту пребывания, напротив, может быть получено как в электронной, так и в бумажной форме²⁵⁵.

Во Франции также предусматривается возможность получения ряда государственных услуг в электронном формате. В частности, Министерство внутренних дел Франции позволяет получить сертификаты, связанные с регистрацией транспортных средств, посредством заполнения форм в сети Интернет²⁵⁶.

²⁵⁴ Приказ Федеральной налоговой службы от 3 ноября 2020 г. № ЕД-7-15/790@ «Об утверждении Административного регламента по предоставлению Федеральной налоговой службой государственной услуги по выдаче свидетельства о регистрации лица, совершающего операции по переработке средних дистиллятов, и формы решения о приостановлении (возобновлении) действия, о неполном устранении нарушений, повлекших за собой приостановление действия, об аннулировании свидетельства о регистрации лица, совершающего операции по переработке средних дистиллятов». URL: <http://publication.pravo.gov.ru/Document/View/0001202012240003> (дата обращения: 15.05.2023).

²⁵⁵ Пункт 126 Приказа МВД России от 31.12.2017 № 984 «Об утверждении Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по регистрационному учету граждан Российской Федерации по месту пребывания и по месту жительства в пределах Российской Федерации» (Зарегистрировано в Минюсте России 05.04.2018 № 50635). URL: <http://publication.pravo.gov.ru/Document/View/0001201804060020> (дата обращения: 15.05.2023).

²⁵⁶ Arrêté du 23 mai 2017 portant création d'un système de téléservices destiné à l'accomplissement de démarches administratives relatives aux certificats d'immatriculation des véhicules. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034832438> (дата обращения: 06.03.2023).

Однако, в отличие от российского законодательства, которое регламентирует процессуальные аспекты получения государственной услуги, французский подход основан на исчерпывающем определении собираемых в порядке оказания государственной услуги данных и особенностей их обработки органом исполнительной власти. Достоинством французского подхода является четкая регламентация деятельности органа исполнительной власти по обработке данных, предотвращающая их избыточное хранение. Достоинством российского подхода является однозначное установление условий получения государственной услуги и способа получения ее результата.

Перевод результатов получения государственной услуги в электронную форму характеризуется термином «реестровая модель». Особенностью реестровой модели оказания государственных и муниципальных услуг является закрепление юридического факта исключительно в электронном виде. Однако в условиях участившихся кибератак и направленности таких атак на причинение вреда информационной системе органа исполнительной власти, реестровая модель не исключает инцидентов в сфере компьютерной информации, которые могут привести к искажению реестровых записей либо исчезновению ряда внесенных данных.

В этой связи право на выбор бумажной формы предоставления государственной или муниципальной услуги или ее результата гарантирует гражданину²⁵⁷ возможность сохранить доказательства наличия юридического факта, определяющего его правовой статус, в случае инцидента в государственном реестре.

В условиях развития электронного правительства и государственных цифровых платформ возможность сохранения бумажной формы результата государственной или муниципальной услуги в меньшей степени отвечает

²⁵⁷ Термин «граждане» здесь и далее используется в более широком контексте для обозначения любого физического лица без привязки к принадлежности соответствующего лица определенному государству. См.: Бахрах Д.Н. Субъекты российского права // Экономика региона. 2006. № 2. С. 121–131.

требованиям эффективности и оперативности получения услуги. Однако эффективность не может являться определяющим критерием для правового регулирования деятельности органа исполнительной власти в ущерб предотвращению возможных рисков государственных информационных систем.

В Российской Федерации права гражданина на выбор формы предоставления государственной услуги по его усмотрению предусмотрено пунктом 3 статьи 5 Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ²⁵⁸. Такое право, согласно указанной статье, может быть ограничено только федеральным законом. Однако возможность отказа от электронной формы предоставления результата государственной услуги в соответствии с частью 2 статьи 7.4 Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ может быть предоставлена и нормативно правовым актом, регламентирующим порядок предоставления государственной услуги.

Из совокупности приведенных норм следует, что возможность отказа от электронной формы предоставления государственной услуги определяется в административном регламенте соответствующей услуги. Расширяя сферу ограничения органом исполнительной власти права гражданина на определение способа получения государственной услуги по своему усмотрению, законодатель не определяет порядок принятия органом исполнительной власти решения о целесообразности ограничения предоставления государственной услуги только электронной формой.

Баланс эффективности предоставления государственной услуги и интересов граждан может быть достигнут путем введения процедуры оценки рисков органом исполнительной власти при проектировании соответствующей государственной информационной системы. В соответствии с проведенной оценкой должен разрешаться вопрос о сохранении за гражданином права на получения результата

²⁵⁸ Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета, № 168, 30.07.2010.

государственной услуги в бумажной форме или отсутствия необходимости в предоставлении такого права.

Несмотря на сохранение возможности получить результат государственной услуги в бумажной форме, доля государственных услуг, оказываемых с предоставлением результата услуги в электронной форме, увеличивается.

Зарубежный опыт показывает, что при информировании граждан о получении государственных услуг иными способами органы исполнительной власти могут отсылать граждан к информации на официальном сайте в сети Интернет. В соответствии с исследованием Защитника прав²⁵⁹ Франции при использовании четырех публичных сервисов 40% из 15000 поступивших телефонных звонков не приводили к надлежащему информированию граждан о сервисах, предлагая гражданам посмотреть необходимую информацию в сети Интернет²⁶⁰. Электронное взаимодействие органов исполнительной власти с гражданами становится основным.

С одной стороны, наметившаяся в России и зарубежных странах тенденция к переходу органов исполнительной власти полностью на электронный документооборот ускоряет дальнейшее увеличение количества государственных услуг, оказываемых в электронной форме.

В Российской Федерации в соответствии с частью 2 статьи 7.4 Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ²⁶¹, вступившей в силу с 01.01.2022²⁶², результаты

²⁵⁹ Защитник прав – *Defenseur des droits* – административный орган Франции, который был создан в результате слияния нескольких предшествующих органов, действующих в сфере защиты прав человека и гражданина. См.: Chevallier J. *Le Défenseur des droits: unité ou diversité?* // *Revue française d'administration publique*. 2011/3. № 139. P. 433-445.

²⁶⁰ Etude sur les plateformes téléphoniques de quatre services publics : 40% des appels n'aboutissent pas. 26 Janvier 2023. URL: <https://www.defenseurdesdroits.fr/fr/a-la-une/2023/01/etude-sur-les-plateformes-telephoniques-de-quatre-services-publics-40-des-appels> (дата обращения: 06.03.2023).

²⁶¹ Российская газета, № 168, 30.07.2010.

²⁶² Федеральный закон от 30.12.2020 № 509-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета, № 2, 12.01.2021.

предоставления государственных и муниципальных услуг по общему правилу не оформляются на бумажном носителе.

В США в соответствии с Меморандумом Административно-бюджетного управления от 28 июня 2019 все федеральные агентства к 2022 году также обязаны были перейти к хранению всех документов, как временных, так и документов постоянного хранения, в электронной форме²⁶³. Однако уже в 2022 году срок полного перехода к электронной форме документов был перенесен на 2024 год²⁶⁴.

В связи с изложенным законодательство в условиях перехода к электронной форме взаимодействия также может возлагать на органы исполнительной власти обязанность по надлежащему технологическому обеспечению граждан для получения ими государственных и муниципальных услуг в электронной форме.

В Российской Федерации часть 2 статьи 10 Федерального закона от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»²⁶⁵ предусматривает необходимость создания пунктов подключения к сети Интернет в доступных для посещения местах. На основании ч. 6 указанной статьи утвержден и Порядок обеспечения условий доступности для инвалидов по зрению официальных сайтов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления в сети Интернет²⁶⁶.

²⁶³ OMB. Memorandum for heads of executive departments and agencies. Transition to Electronic Records. June 28, 2019. URL: <https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf> (дата обращения: 06.03.2023).

²⁶⁴ OMB. Memorandum for heads of executive departments and agencies. Update to Transition to Electronic Records. December 23, 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/12/M_23_07-M-Memo-Electronic-Records_final.pdf (дата обращения: 06.03.2023).

²⁶⁵ Российская газета, № 25, 13.02.2009.

²⁶⁶ Приказ Минкомсвязи России от 30.11.2015 № 48 «Об установлении Порядка обеспечения условий доступности для инвалидов по зрению официальных сайтов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления в сети «Интернет»» (Зарегистрировано в Минюсте России 01.02.2016 N 40905) // Российская газета, № 27, 10.02.2016.

Проблема технологического обеспечения граждан не была оставлена без внимания и в условиях усиленной цифровизации при проведении мер по предотвращению распространения коронавирусной инфекции. Например, в ч. 2.3.2. Порядка применения технологии электронного мониторинга местоположения гражданина в определенной геолокации с использованием мобильного приложения «Социальный мониторинг» в г. Москве²⁶⁷ была предусмотрена возможность предоставления гражданину технического устройства для установки приложения при отсутствии своего или невозможности установить приложение.

Во Франции доступность цифровых государственных услуг для граждан обеспечивается в рамках проекта «France Services», который был реализован Министерством объединения территорий и отношений с территориальными общностями (Ministère de la Cohésion des territoires et des Relations avec les collectivités territoriales). В территориальной доступности не более 30 минут пешком от каждого гражданина располагаются помещения «единого окна», в которых можно получить ряд электронных услуг, а также получить консультацию по переходу к цифровому взаимодействию (создание электронной почты, регистрация в интернет-сервисах). В 2022 году на территории Франции действовало 2 379 «единых окон»²⁶⁸.

Право гражданина на надлежащее технологическое обеспечение при взаимодействии с органами исполнительной власти в электронной форме, однако, не может толковаться расширительно. Гражданин вправе требовать от органа исполнительной власти предоставления ему необходимых технологий только в пределах, устанавливаемых законодательством. Однако вне зависимости от

²⁶⁷ Распоряжение руководителя департамента информационных технологий города Москвы № 64-16-186/20 от 29.04.2020 «Об утверждении порядка применения технологии электронного мониторинга местоположения гражданина в определенной геолокации с использованием мобильного приложения «Социальный мониторинг»». URL: <https://www.mos.ru/dit/documents/view/238534220/> (дата обращения: 06.03.2023).

²⁶⁸ France services : les services publics près de chez vous ! URL: <https://www.economie.gouv.fr/particuliers/france-services#> (дата обращения: 06.03.2023). Дата опубликования: 06.09.2022.

формальных способов реализации такого права нельзя исключить значение корреспондирующей к нему обязанности органа исполнительной власти обеспечить гражданину доступность электронных государственных и муниципальных услуг различными способами.

Право гражданина на надлежащее технологическое обеспечение при взаимодействии с органами исполнительной власти в электронной форме следует отличать от права на доступ к сети Интернет, получившего широкое обсуждения в российской и зарубежной правовой литературе в качестве разновидности «цифровых прав» человека²⁶⁹. Право на доступ к сети Интернет тесно связано с реализацией гражданином свободы слова и свободы информации²⁷⁰.

Право гражданина на надлежащее технологическое обеспечение при взаимодействии с органами исполнительной власти, во-первых, характеризует взаимодействие гражданина с администрацией в удобном и эффективном для него формате. По своему содержанию это право вытекает из «права на хорошее управление», содержание которого можно рассматривать как с точки зрения отношений гражданина и администрации²⁷¹, так и в более широком контексте – как принцип формирования государственной политики, основанный на уважении фундаментальных прав и свобод человека государством²⁷². Во-вторых, если право на доступ к сети Интернет обсуждается в контексте его отнесения к фундаментальным правам человека в цифровую эпоху, право на надлежащее технологическое обеспечение при взаимодействии с органами исполнительной власти не относится к таковым. Оно носит лишь вспомогательный характер,

²⁶⁹ Напр.: Варламова Н.В. Цифровые права – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Том 14. № 4. С. 9–46; Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. 2019. Том 14. № 3. С. 122–145; Щербович А.А. Конституционное право на доступ к Интернету: мировой опыт и выводы для России // Копирайт. 2015. № 3. С. 57–70.

²⁷⁰ Напр.: Щербович А.А. Конституционные гарантии свободы слова и права доступа к информации в сети Интернет: автореф. дис. ... к.ю.н. Москва, 2013.

²⁷¹ Петров А.Ю. «Право на хорошее управление» (right to good administration): традиции и современность // Вестник ЮУрГУ. Серия «Право». 2013. Т. 13. № 3. С. 88–92.

²⁷² Bach-Golecka D. The Emerging Right to Good Governance // American Journal of International Law. 2018. 112. P. 89-93.

указывая на необходимость учета цифровой грамотности и доверия населения к электронному взаимодействию при переходе органов исполнительной власти к использованию информационно-коммуникационных технологий в своей деятельности.

Надлежащее технологическое обеспечение оказания государственных услуг в электронной форме приводит к развитию органами исполнительной власти новых технологий и новых способов сбора данных о гражданах. Переход органов исполнительной власти к использованию различных приложений и сервисов для взаимодействия с гражданами создает возможности для сбора органом исполнительной власти дополнительных пользовательских данных, включая данные о перемещении, предпочтениях гражданина-пользователя²⁷³.

Американский юрист Б. Фридман, анализируя право органа исполнительной власти на доступ к таким дополнительным данным²⁷⁴, справедливо отмечает, что в отношении способов доступа органов исполнительной власти к данным граждан в американском конституционном праве уже сформировались правовые механизмы, предполагающие прохождение специальной процедуры для доступа к сведениям о гражданине (напр., для обыска, для прослушивания телефонных разговоров). Однако получение органами исполнительной власти доступа к таким данным в электронной форме не урегулировано²⁷⁵.

В российском праве обработка пользовательских данных о гражданах органами исполнительной власти регулируется законодательством о персональных данных. Однако правовой режим персональных данных основан на определении соответствующего законного условия обработки данных. При этом российские сервисы органов исполнительной власти не указывают конкретные

²⁷³ Oakley K. The Limit Does Not Exist: How Smartphone Technology Expands Electronic Monitoring and a Proposed Limitation // Harvard Journal of Law & Technology. 2022. Volume 36. № 1. P. 263–289.

²⁷⁴ Friedman B. Lawless Surveillance // New York University Law Review. 2022. Vol. 97. P. 1143–1214.

²⁷⁵ Friedman B. Op. cit. P. 1213: «Consider, for example, if the government required us to keep a diary of our movements. That would surely be a violation of the Fifth Amendment. But how different is it really if the government monitors us to get the same information?».

цели обработки пользовательских данных органом исполнительной власти. Более обширное согласие на использование cookies пользователь может предоставить при посещении официального портала Франции, включая возможность выбора интеграции со сторонними сервисами (напр., YouTube).

Получение согласия на использование органами исполнительной власти пользовательских данных граждан не охватывает вопрос о возможности использования органом исполнительной власти соответствующих данных. Необходимо дополнительное регулирование особенностей обработки пользовательских данных граждан.

Не менее дискуссионным остается вопрос и о правах граждан при использовании органами исполнительной власти технологий искусственного интеллекта для принятия решений в отношении граждан и анализа информации о них²⁷⁶.

Гражданин праве отказаться от принятия в отношении него решения на основании исключительно автоматизированной обработки данных о нем (human alternative). В США, в частности, такое право предложено в Билле о правах в сфере искусственного интеллекта, принятом Президентом США в 2022 году²⁷⁷. В российском и европейском праве такое право предусматривается законодательством о персональных данных.

Необходимость предоставления гражданину права отказаться от принятия решения в отношении него с использованием исключительно автоматизированной обработки обусловлена, с одной стороны, возможностью ошибок в рамках функционирования технологий искусственного интеллекта²⁷⁸, с другой стороны –

²⁷⁶ Архипов В.В., Наумов В.Б., Смирнова К.М. Пределы принятия юридически значимых решений с использованием искусственного интеллекта // Вестник Санкт-Петербургского университета. Право. 2021. № 4. С. 882-906.

²⁷⁷ Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public. October 04, 2022. URL: <https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/> (дата обращения: 06.03.2023).

²⁷⁸ Lowens E. Accuracy Is Not Enough: The Task Mismatch Explanation of Algorithm Aversion and Its Policy Implications // Harvard Journal of Law & Technology. 2020. Vol. 34. № 1. P. 259–278.

этическими аспектами использования искусственного интеллекта в государственном управлении.

Технологии искусственного интеллекта некоторые исследователи рассматривают, наоборот, как более нейтральные способы вынесения решений в отношении граждан²⁷⁹. В случаях, когда принятие решения в отношении гражданина может быть обусловлено более широкой степенью усмотрения органа исполнительной власти, гражданин должен иметь право требовать принятия в отношении него решения на основании исключительно автоматизированной обработки данных.

Наконец, в случае согласия гражданина на использование искусственного интеллекта для принятия решения в отношении него недостаточно информирования гражданина о способах работы соответствующей технологии. Во-первых, проблема заключается в самой скрытной природе алгоритмов²⁸⁰. Раскрытие алгоритма той или иной технологии не позволит большинству граждан проанализировать особенности его работы без дополнительных специальных познаний. Технологии искусственного интеллекта могут формировать новые алгоритмы для той или иной обработки информации в соответствии с поставленной целью, поэтому даже раскрытый алгоритм остается непонятным для получившего к нему доступ гражданина.

Поскольку непосредственное раскрытие алгоритма новых технологий не приведет к обеспечению надлежащего информирования гражданина об использовании технологий искусственного интеллекта органами исполнительной власти, необходимо установить целевое ограничение использования новых технологий органами исполнительной власти. Государственный орган исполнительной власти вправе использовать технологии больших данных и искусственного интеллекта в пределах его компетенции только в соответствии с

²⁷⁹ Youssef M. Here's Your Number, Now Please Wait in Line: The Asylum Backlog, Federal Court Litigation, and Artificial Intelligence in Agency Adjudication // The University of Chicago Law Review. 2022. Vol. 89. Is. 8. P. 2013–2066.

²⁸⁰ Kalpokas I. Algorithmic Governance. Politics and Law in the Post-Human Era. Cham: Palgrave Pivot, 2019. P. 38.

публично оглашенными им целями использования таких технологий. Орган исполнительной власти должен быть обязан также отчитываться о результатах использования им цифровых технологий, достижении поставленных целей и выявленных недостатков их использования²⁸¹.

Исследователи справедливо отмечают необходимость проведения оценки рисков внедрения искусственного интеллекта органом исполнительной власти на стадии проектирования²⁸², что позволит заранее оценить необходимость сохранения возможности для гражданина отказаться от использования только искусственного интеллекта при принятии в отношении него решения, а также заранее спроектировать надлежащие правовые процедуры обжалования решений, вынесенных с технической ошибкой искусственного интеллекта. Указанный подход применен и в проекте Регламента ЕС, посвященного регулированию искусственного интеллекта, предлагающего в том числе ограничения использования органами исполнительной власти технологий искусственного интеллекта для распознавания лиц в общественных местах или для оценки доверия к гражданину²⁸³.

Оказание государственных услуг в электронной форме характеризует не только эффективность государственного управления. Во-первых, реализация многих гражданских и политических прав становится в зависимость от технических возможностей и навыков гражданина²⁸⁴: появляется возможность электронного голосования, электронной подачи документов в суды с помощью платформы государственных услуг. Доступность получения государственных

²⁸¹ Подробнее особенности и значение обеспечения прозрачности исполнительной власти в цифровую эпоху рассмотрены в статье соискателя: Силкин В.В. Прозрачность исполнительной власти в цифровую эпоху // Российский юридический журнал. 2021. № 4 (139). С. 20–31.

²⁸² Selbst A.D. An Institutional View of Algorithmic Impact Assessments // Harvard Journal of Law & Technology. 2021. Volume 35. № 1. P. 117–191.

²⁸³ Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Document 52021PC0206. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> (дата обращения: 14.05.2023).

²⁸⁴ Alvares C. et al. Media in Europe: New questions for research and policy // Strasbourg: European Science Foundation ESF, 2014.

услуг в электронной форме влияет и на реализацию иных прав граждан²⁸⁵. Во-вторых, обработка пространственных данных в сервисах и приложениях органов исполнительной власти в режиме реального времени может затрагивать права и интересы граждан. Наконец, в связи с возможностями использования технологий искусственного интеллекта и анализа больших данных органами исполнительной власти необходимы дополнительные средства контроля за соблюдением прав граждан.

Выявление возникающих в связи с оказанием государственных услуг в электронной форме проблем и угроз фундаментальным правам человека может осуществлять уполномоченный по правам человека. В странах сложились разные подходы к формированию такого органа применительно к системе разделения властей. Он может действовать в пределах полномочий законодательной власти (Россия, Швеция) либо исполнительной (Франция). Однако анализ деятельности таких органов показывает, что они выявляют и учитывают те особенности взаимоотношений гражданина и администрации, которые могут и не быть выявлены в судебном или административном порядке.

В отчетах о деятельности российского федерального Уполномоченного по правам человека особенности защиты прав и свобод в условиях цифровизации впервые стали обособляться в 2020 году²⁸⁶ в разделе гражданских и политических прав и свобод. Среди поступивших обращений наиболее частыми по тематике были обращения в связи с организацией удаленного труда (37%), электронным голосованием (21%) и дистанционным образованием (17%). В 2021 году тематика обращений поменялась: основной темой обращений были персональные данные (32%), доступ к государственным услугам (16%) и блокировка контента

²⁸⁵ Шулакова А.А. Значение государственных услуг в реализации основных прав человека // Вопросы управления. № 3 (9). 2014. С. 38–45.

²⁸⁶ Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2020 год. URL: <https://ombudsmanrf.org/storage/74a0484f-7d5a-4fe4-883d-a1b5ba1dd5f8/documents/ezhegodnye-doklady/docs/doklad2020.pdf> (дата обращения: 06.03.2023).

пользователей в социальных сетях (15%)²⁸⁷. Однако в 2022 году права граждан в сфере цифровизации в целом не были выделены в отдельную группу.

Отдельными вопросами защиты прав в информационной сфере занимаются также Интернет-омбудсмен²⁸⁸, должность которого учреждена в аппарате Уполномоченного при Президенте Российской Федерации по правам предпринимателей²⁸⁹, Молодежный цифровой омбудсмен, деятельность которого законодательно не урегулирована и направлена на просветительскую деятельность среди молодежи по вопросам цифровизации²⁹⁰. Хотя деятельность указанных омбудсменов затрагивает отдельные аспекты информационной сферы, в части оказания государственных услуг в электронной форме и электронных государственных услуг не выявлено каких-либо инициатив с их стороны.

В отчетах Шведских парламентских омбудсменов отдельно выделен раздел, посвященный праву граждан на доступ к информации о деятельности органов исполнительной власти²⁹¹, однако не обособляются именно вопросы защиты прав и свобод в информационной сфере в целом²⁹². Это не исключает рассмотрение

²⁸⁷ Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2021 год. URL: <https://ombudsmanrf.org/storage/74a0484f-7d5a-4fe4-883d-a1b5ba1dd5f8/documents/14493f2b-4975-49d0-86dd-c9ac917436fe/0447a931-4bc9-4ce6-ae92-b32f8d741412.pdf> (дата обращения: 06.03.2023).

²⁸⁸ Интернет-омбудсмен. URL: <https://www.iombudsman.ru/about/> (дата обращения: 06.03.2023).

²⁸⁹ Федеральный закон от 07.05.2013 № 78-ФЗ «Об уполномоченных по защите прав предпринимателей в Российской Федерации» // Собрание законодательства Российской Федерации от 2013 г., № 19, ст. 2305.

²⁹⁰ Молодежный цифровой омбудсмен. Первый ЦифроЗащитник российской молодежи. URL: <https://www.youthombudsman.ru/team> (дата обращения: 06.03.2023).

²⁹¹ В Швеции право на доступ к административным документам является одним из основных конституционных прав человека.

²⁹² The Parliamentary Ombudsmen (JO). Annual reports. Summary in English of the annual reports. URL: <https://www.jo.se/en/About-JO/Annual-reports/> (дата обращения: 06.03.2023).

омбудсменами отдельных вопросов использования органами исполнительной власти технологий²⁹³ и взаимодействия с гражданами в электронной форме²⁹⁴.

Защитник прав Франции, наоборот, уделяет особое внимание вопросам цифровизации деятельности органов исполнительной власти. Впервые обратив внимание на защиту прав граждан в связи с цифровизацией государственного управления в 2019 году, в 2022 году Защитник прав Франции выпустил отдельное исследование по этому вопросу²⁹⁵, а также включил его в отчет за 2021 год²⁹⁶.

На возможность контроля уполномоченного по правам человека за деятельностью органов исполнительной власти справедливо обращал внимание В.А. Туманов²⁹⁷. Выступая с лекцией в Страсбурге, ученый рассматривал уполномоченного по правам человека в качестве одного из органов исполнительной власти, следуя привычному для слушателей французскому подходу. При отсутствии властных полномочий в целом контроль омбудсмена за деятельностью администрации позволяет в качестве дополнительного средства содействовать разрешению возникающих административно-правовых споров²⁹⁸.

Таким образом, внедрение новых технологий в процесс оказания государственных услуг органами исполнительной власти приводит к

²⁹³ The Parliamentary Ombudsmen (JO). Decision № 961-2020. 28.06.2022. The Swedish Police Authority forcibly photographed a person's motorcycle vest and driving licence with no legal grounds for doing so, thereby violating his right to privacy under Article 8 of the European Convention. URL: <https://www.jo.se/en/> (дата обращения: 06.03.2023).

²⁹⁴ The Parliamentary Ombudsmen (JO). Decision № 568-2021, 19.06.2022. Swedish Pensions Agency criticised for lack of accessibility and service. URL: <https://www.jo.se/en/> (дата обращения: 06.03.2023).

²⁹⁵ Le rapport du Défenseur des droits dématérialisation et inégalités d'accès aux services publics. 2022. URL: <https://www.defenseurdesdroits.fr/fr/rapports/2022/02/rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-on> (дата обращения: 06.03.2023).

²⁹⁶ Défenseur des droits. Le rapport d'activité de l'année 2021. URL: <https://www.defenseurdesdroits.fr/fr/dossier-de-presse/2022/07/rapport-annuel-dactivite-2021> (дата обращения: 06.03.2023).

²⁹⁷ Туманов В.А. Права человека и исполнительная власть // Советское государство и право. 1990. № 2. С. 49.

²⁹⁸ Зеленцов А.Б., Лафитский В.И., Тимошенко И.Г. и др. Тенденции развития контроля за деятельностью публичной администрации в зарубежных государствах: монография / отв. ред. В.И. Лафитский, И.Г. Тимошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2015. С. 257–339.

возникновению и развитию новых прав граждан в отношении применения органами исполнительной власти новых технологий и технологического обеспечения процесса оказания государственных услуг. Особенностью правового регулирования новых технологий в рамках оказания государственных услуг является необходимость обеспечения открытости информации об использовании таких технологий, их целях и результатах, а также применение риск-ориентированного подхода на стадии проектирования соответствующей технологии.

2.3. Информационная безопасность органа исполнительной власти

Переход к цифровому формату деятельности органа исполнительной власти формирует новую среду, основным активом в которой выступают данные, находящиеся в распоряжении субъектов информационных отношений. Кибератака на информационные ресурсы государственного органа может нанести вред как государству, так и отдельным невластным субъектам (например, в случае подмены сведений в государственном реестре).

Информационная безопасность – одно из направлений усиленной централизации регулирования информационной сферы в целом. Определение политики в сфере информационной безопасности в исследуемых странах (США, Франция, Россия) относится к компетенции главы государства.

Для содействия главе государства в реализации его полномочий по обеспечению информационной безопасности в исследуемых странах формируются отдельные государственные органы или должности. Такие органы могут формироваться и при правительстве (Франция) с целью содействия главе государства в реализации его полномочий по определению политики в сфере национальной безопасности.

Если система информационной безопасности в целом охватывает как внешнее воздействие уполномоченных органов исполнительной власти на информационную сферу, так и внутреннее взаимодействие между ними,

обязанности органов исполнительной власти в сфере информационной безопасности относятся преимущественно к более узкой сфере обеспечения кибербезопасности.

В отличие от координации и контроля в сфере информационной безопасности, стандартизация осуществляется профессиональным сообществом, а органы исполнительной власти утверждают необходимость применения того или иного технического стандарта. В исследуемых странах (Франция, США) наблюдается тенденция к принятию единых обобщающих различные практики справочников в сфере информационной безопасности.

Во Франции применимые стандарты утверждены Общим руководством по безопасности²⁹⁹, принятым на основании статьи 9 Ордонанса Президента Французской Республики № 2005-1516 от 08.12.2005³⁰⁰.

В США разработкой стандартов информационной безопасности для агентств занимается Национальный институт стандартов и технологий, образованный в составе Министерства торговли³⁰¹. В частности, Институтом разработан Фреймворк усовершенствования безопасности критической информационной инфраструктуры³⁰², который может использоваться для построения системы информационной безопасности.

В Российской Федерации такие обобщающие документы отсутствуют. Сводный перечень применимых к информационной сфере стандартов размещен на

²⁹⁹ Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029122964> (дата обращения: 06.03.2023).

³⁰⁰ Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/> (дата обращения: 06.03.2023).

³⁰¹ Sec. 20, National Institute of Standards and Technology Act. As Amended Through P.L. 117–263, Enacted December 23, 2022. URL: <https://www.govinfo.gov/content/pkg/COMPS-5388/pdf/COMPS-5388.pdf> (дата обращения: 06.03.2023).

³⁰² National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 April 16, 2018. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (дата обращения: 06.03.2023).

сайте ФСТЭК России³⁰³. ФСБ России отдельно утвержден стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения»³⁰⁴.

Система информационной безопасности выстраивается динамично и требует реагирования на различные вызовы новых технологий, усовершенствования кибератак. Разрозненное стандартизированное регулирование не позволяет выстроить единый последовательный план внедрения отдельных элементов системы информационной безопасности и усложняет особенности их применения. В этой связи представляется целесообразным закрепить за Федеральной службой безопасности Российской Федерации полномочия по обобщению требований различных стандартов информационной безопасности как в общем, так и для отдельных отраслей, и опубликованию единых справочников стандартов в сфере информационной безопасности органов исполнительной власти. По верному замечанию В.Б. Исакова именно практика определяет формирование технологических норм и стандартов³⁰⁵. В связи с этим важным направлением регулирования в сфере информационной безопасности органов исполнительной власти является учреждение совещательных органов, объединяющих специалистов различных органов исполнительной власти в сфере обеспечения информационной безопасности.

Необходимость формирования системы информационной безопасности органа исполнительной власти предполагает также формирование отдельных структурных подразделений и штатных единиц, непрерывно со стадии проектирования обеспечивающих соблюдение условий информационной безопасности и оценку возможных рисков и угроз. Грамотный учет данных в

³⁰³ ФСТЭК России. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Национальные стандарты. Обновлено: 19 февраля 2015 г. URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty> (дата обращения: 06.03.2023).

³⁰⁴ Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения». 12.11.2018. URL: <http://www.fsb.ru/fsb/npd/more.htm%21id%3D10437602%40fsbNpa.html> (дата обращения: 06.03.2023).

³⁰⁵ Исаков В. Б. Преемственность правовых норм в сфере технического регулирования // Юридическая техника. 2011. № 5. С. 184-191.

распоряжении органа исполнительной власти позволяет более точно определять возможные риски и последствия их утечки³⁰⁶ и анализировать степень общественной опасности кибератаки³⁰⁷.

В Российской Федерации образование отдельных структурных подразделений, ответственных за информационную безопасность, в органах исполнительной власти осуществляется на основании Указа Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»³⁰⁸ и утвержденных Правительством Российской Федерации в соответствии с ним типовых положений³⁰⁹.

В США в каждом агентстве в соответствии с Законом о модернизации федеральной информационной безопасности от 2014 года утверждена должность старшего управляющего по безопасности агентства в подчинении Главного управляющего в сфере информации³¹⁰. К полномочиям старшего управляющего по безопасности агентства относится как разработка внутренних документов по информационной безопасности, так и обучение иных служащих агентства правилам информационной безопасности.

Во Франции применяется иной подход, основанный на разделении технических специалистов и управленцев в сфере информационной безопасности в структуре органа исполнительной власти. В соответствии с Декретом Премьер-министра № 2022-513 от 08.04.2022 каждое министерство обязано назначить

³⁰⁶ Nugraha Y., Martin A. Cybersecurity service level agreements: understanding government data confidentiality requirements // Journal of Cybersecurity. Volume 8. Issue 1. 2022. URL: <https://academic.oup.com/cybersecurity/article/8/1/tyac004/6588067> (дата обращения: 06.03.2023).

³⁰⁷ Dykstra J., Gordon L.A., Loeb M.P., Zhou L. Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments // Journal of Cybersecurity. Volume 9. Issue 1. 2023. URL: <https://academic.oup.com/cybersecurity/article/9/1/tyad003/7100879> (дата обращения: 06.03.2023).

³⁰⁸ Российская газета, № 95, 04.05.2022

³⁰⁹ Постановление Правительства РФ от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» // Собрание законодательства РФ, 25.07.2022, № 30, ст. 5610.

³¹⁰ Federal Information Security Modernization Act of 2014. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text> (дата обращения: 06.03.2023).

государственного служащего, ответственного за безопасность информационных систем (*un fonctionnaire de sécurité des systèmes d'information*)³¹¹. Такой служащий отвечает за выработку общей политики информационной безопасности министерства и подведомственных ему организаций и контроль ее исполнения³¹². Дополнительно каждый министр обязан назначить одно или несколько квалифицированных лиц, непосредственно обеспечивающих безопасность информационных систем министерства. Квалифицированные лица координируются государственным служащим, ответственным за безопасность информационных систем.

Российское законодательство уделяет меньше внимания формам кооперации и обмена лучшими практиками между различными должностными лицами в органах исполнительной власти. В этой связи примечателен опыт США, основанный на образовании таких советов. В частности, для координации деятельности старших управляющих по безопасности агентств и обмена практиками при Административно-бюджетном управлении образован Совет главных управляющих информационной безопасностью, которым руководит Федеральный главный управляющий информационной безопасностью³¹³. Представляется положительной возможность заимствования различных совещательных органов между должностными лицами органов исполнительной власти, ответственными за информационную безопасность, что позволит обобщать возникающие проблемы и обмениваться лучшими практиками.

Развитие штатных единиц, специализированных на обеспечении информационной безопасности, в структуре органа исполнительной власти,

³¹¹ Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/> (дата обращения: 06.03.2023).

³¹² Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000046503138#JORFARTI000046503138> (дата обращения: 06.03.2023).

³¹³ CIO Council - CISO Committee. URL: <https://www.cio.gov/about/members-and-leadership/ciso-council/> (дата обращения: 06.03.2023).

позволяет организовать систему обмена информацией и уведомлениями об инцидентах или уязвимостях информационных систем различных органов исполнительной власти³¹⁴.

Как правило, такой обмен осуществляется централизованно. В частности, в Российской Федерации уведомления об инцидентах направляются в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации³¹⁵, оператором которой является Национальный координационный центр по компьютерным инцидентам в составе ФСБ России³¹⁶.

Во Франции учреждаемая в обязательном порядке в министерствах должность государственного служащего, ответственного за безопасность информационных систем, предполагает его обязанность уведомлять Национальное агентство безопасности информационных систем о любых инцидентах, связанных с информационными системами органа исполнительной власти³¹⁷.

В США в подчинении Министерства внутренней безопасности образован Федеральный центр инцидентов информационной безопасности (Federal information security incident center), с которым все агентства обязаны делиться информацией об инцидентах в соответствии с секцией 3556 (b) Закона о

³¹⁴ Brilingaitė A., Bukauskas L., Juozapavičius A., Kutka E. Overcoming information-sharing challenges in cyber defence exercises // Journal of Cybersecurity. Volume 8. Issue 1. 2022. URL: <https://academic.oup.com/cybersecurity/article/8/1/tyac001/6516499> (дата обращения: 15.05.2023).

³¹⁵ Статья 5 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4736.

³¹⁶ Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам») (Зарегистрировано в Минюсте России 06.09.2018 N 52109). URL: <http://publication.pravo.gov.ru/Document/View/0001201809100001> (дата обращения: 06.03.2023).

³¹⁷ Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/> (дата обращения: 06.03.2023).

модернизации федеральной информационной безопасности от 2014 года³¹⁸. Уведомлять об инцидентах могут также штаты и их органы местного самоуправления³¹⁹. Система взаимодействия Министерства внутренней безопасности США с органами штатов была укреплена в 2021 году в Законе о кибербезопасности штатов и местного самоуправления³²⁰. Дополнительно в 2022 году была введена обязанность агентств уведомлять частные организации об утечках, которые могут существенно повлиять на соблюдение конфиденциальности предоставленных такими организациями данных³²¹.

Вопрос о необходимости информирования государством граждан и организаций о произошедших утечках данных, имеющих значительные последствия для их деятельности, остается дискуссионным. Социологические исследования показывают, что граждане, подвергшиеся утечке данных, повлекшей значительный ущерб, склонны считать, что государство должно обеспечить систему надлежащего уведомления граждан об утечках, повлекших значительный ущерб, в то время как граждане, получившие меньший вред из-за утечек, занимают более умеренную позицию³²². Однако раскрытие информации об утечках может вызвать дополнительные общественные волнения, что только усилит неблагоприятные последствия кибератаки.

Выстраивание единых механизмов обмена информацией об инцидентах и развитие структурных подразделений, отвечающих за обеспечение информационной безопасности, наблюдаемые в исследуемых странах (Россия, Франция, США), свидетельствуют о тенденции к централизации регулирования

³¹⁸ Federal Information Security Modernization Act of 2014. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text> (дата обращения: 06.03.2023).

³¹⁹ Federal Incident Notification Guidelines. April 1, 2017. URL: <https://www.cisa.gov/federal-incident-notification-guidelines> (дата обращения: 06.03.2023).

³²⁰ State and Local Government Cybersecurity Act of 2021. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/2520/text> (дата обращения: 06.03.2023).

³²¹ Sec. 107, (b), Strengthening American Cybersecurity Act of 2022. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/3600/text#toc-id87c2d95a-b307-45ec-81dd-09e23e4addc4> (дата обращения: 06.03.2023).

³²² Snider K.L.G., Shandler R., Zandani S., Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies // Journal of Cybersecurity. Volume 7. Issue 1. 2021. URL: <https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745> (дата обращения: 06.03.2023).

информационных систем органов исполнительной власти в целом. Если Франция склонна вносить меньше изменений в подход к регулированию информационной безопасности органов исполнительной власти, Россия и США активно изменяют и усиливают законодательство в данной сфере. Наибольшая динамика регулирования отмечается в США.

Отмеченная тенденция может измениться с внедрением новых технологий и средств обеспечения информационной безопасности. В частности, потенциалом обладает использование технологий искусственного интеллекта для предотвращения инцидентов информационной безопасности³²³. Кроме того, набирающие популярность квантовые технологии исключают любую возможность несанкционированного доступа к компьютерной информации³²⁴. Как следствие, в случае применения квантовых технологий для передачи и обработки данных органами исполнительной власти может увеличиться доля автономии органа исполнительной власти в отношении находящихся в его распоряжении информационных систем. Однако внедрение квантовых коммуникаций требует на начальных этапах как финансирования, так и воспитания специалистов, способных работать с квантовыми коммуникациями³²⁵.

Развитие правового регулирования квантовых коммуникаций в целом³²⁶ нуждается в дополнительном уточнении в действующем законодательстве. Лидирующим в развитии квантовых технологий является Китай, принявший в 2020 г. в том числе и Закон о шифровании, урегулировавший вопросы развития

³²³ Dapel M.E., Asante M., Uba C.D., Agyeman M.O. Artificial Intelligence Techniques in Cybersecurity Management. In: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 2023.

³²⁴ Лескина Э.И. Квантовые технологии и перспективы правового регулирования защиты данных // Юрист. 2022. № 11. С. 2-6.

³²⁵ Albataineh, H., Nijim, M. Enhancing the Cybersecurity Education Curricula Through Quantum Computation. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.S., Tinetti, F.G. (eds) Advances in Security, Networks, and Internet of Things. Transactions on Computational Science and Computational Intelligence. Springer, Cham. 2021.

³²⁶ По справедливому замечанию Е.В. Холодной, квантовая коммуникация – более широкое понятие по отношению к квантовой криптографии. См.: Холодная Е.В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина. № 4 (92). 2022. С. 38-45.

квантовой криптографии³²⁷. В России в целом вопросы регулирования квантовых коммуникаций в настоящий момент носят дискуссионный характер³²⁸, однако их дальнейшее развитие представляется неизбежным.

2.4. Применение мер административного информационного воздействия

Стремление государства ограничить и регулировать деятельность субъектов информационных отношений приводит к возникновению и развитию различных мер административного принуждения в информационной сфере. В первую очередь указанные меры связаны с необходимостью обеспечения информационно-психологической безопасности граждан и устранения негативного воздействия на них³²⁹.

Дискуссионным остается вопрос об отнесении таких мер административного принуждения к той или иной группе мер административного принуждения, уже выделенных правовой наукой.

В административном праве советского периода сложилась дискуссия о разновидностях мер административного принуждения, подробно проанализированная Ю.С. Рябовым³³⁰. Часть исследователей, включая таких именитых деятелей административного права как Ц.А. Ямпольскую, А.Е. Лунева, Г.И. Петрова, придерживались двойного деления мер административного принуждения на меры административного взыскания и иные меры, которые относились во вторую группу, название которой предлагалось разными исследователями по-разному. Этот подход был свойственен литературе 50-60-х годов прошлого века.

³²⁷ Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О. Е. Кутафина. № 4 (92). 2022. С. 46-58.

³²⁸ Добробаба М.Б., Чаннов С.Е., Минбалеев А.В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина. № 4 (92). 2022. С. 25-37.

³²⁹ Лопатин В.Н. Информационная безопасность России: дис. ... д.ю.н. СПб., 2000. С. 15.

³³⁰ Рябов Ю.С. Административно-предупредительные меры. Теоретические вопросы. Пермь: Книжное издательство, 1974. С. 10-14.

Одной из наиболее полных работ, посвященных исследованию административного принуждения в указанный период, можно назвать работу Т.И. Козыревой, предлагавшей классификацию мер административного принуждения на меры административного взыскания и меры административного воздействия³³¹. Нельзя не согласиться с критикой такого подхода Ю.С. Рябовым, поскольку в таком случае все меры административного принуждения объединяются без надлежащего учета их различий.

Другая группа исследователей придерживалась более детальной классификации мер административного принуждения. Например, М.И. Еропкин выделял три вида мер административного принуждения на основе целей обеспечения защиты правопорядка: административно-предупредительные меры, меры административного пресечения и меры административного взыскания³³². Аналогичного подхода придерживался и Ю.С. Рябов³³³. Указанный подход к делению мер административного принуждения соответствовал усовершенствованию терминологического аппарата по сравнению с подходом 50-60-х годов прошлого века в условиях изменяющихся социальных отношений и в дальнейшем закрепился и в советской, и в российской правовой литературе³³⁴.

Отдельно стоит отметить исследования Д.Н. Бахраха, предлагавшего иную классификацию мер административного принуждения³³⁵. Отвергая двойное деление мер принуждения по причине разнородности иных мер, не отнесенных к взысканиям, автор также критиковал выделение мер административного предупреждения другими исследователями. Исследователь полагал, что меры предупреждения не относятся к административно-принудительным мерам, а

³³¹ Козырева Т.И. Административное принуждение и его виды. Москва, 1957. С. 21.

³³² Еропкин М.И., Попов Л.Л. Административно-правовая охрана общественного порядка. Ленинград: Лениздат, 1973. С. 167; Еропкин М.И., Ключниченко А.П. Советское административное право. Учебник для средних юридических учебных заведений. М.: Юрид. лит., 1979. С. 103.

³³³ Рябов Ю.С. Указ. соч. С. 15.

³³⁴ Напр.: Якуба О.М. Административная ответственность. Москва. Юридическая литература, 1972. С. 21; Семененко И.И. Административное принуждение. Ростов-на-Дону, 1999. С. 9; Козлов Ю.М. Административное право: Учебник. М.: Юристъ, 1999. С. 88.

³³⁵ Бахрах Д.Н. Советское законодательство об административной ответственности. Пермь, 1969. С. 35–37.

предложенное тройственное деление позволяет относить к предупредительным мерам и профилактические, по своей природе не связанные с принуждением. Вместо предупредительных мер автор предлагал выделить меры административного восстановления, направленные на возмещение причиненного вреда, возвращение к положению, существовавшему до нарушения.

Предложенная позиция критикуется некоторыми исследователями. Например, А.И. Каплунов предложил выделить четыре их вида: меры административного предупреждения, меры административного пресечения, меры административно-процессуального обеспечения и меры административной ответственности. Восстановительные меры исследователь относил к мерам государственного, но не административного принуждения³³⁶.

А.В. Коркин, стремясь согласовать сложившиеся в правовой литературе противоречия, выделил четыре вида мер административного принуждения, включая административное взыскание, административное предупреждение, административное пресечение и административное восстановление. К мерам административного восстановления исследователь отнес достаточно неоднородный состав: привод, аннулирование лицензий на оружие, снос самовольной постройки и возмещение убытков, причиненных административным правонарушением³³⁷.

Отдельный интерес представляют классификации мер административного принуждения исследователей саратовской школы административного права. В.М. Манохин разделяет меры обеспечительного предназначения на две группы: меры обеспечения и охраны порядка и безопасности (меры, применяемые в силу государственной необходимости, а также контрольно-предупредительные) и меры, обеспечивающие привлечение к административной ответственности³³⁸.

³³⁶ Каплунов А.И. Административное принуждение, применяемое органами внутренних дел (системно-правовой анализ): автореф. дис. ... д.ю.н. Москва, 2005. С. 27.

³³⁷ Коркин А.В. Институт административно-правового принуждения: меры, применяемые сотрудниками милиции: автореф. дис. ... к.ю.н. Челябинск, 2004. С. 24.

³³⁸ Манохин В.М. Административное право России: учебник. Саратов: Ай Пи Эр Медиа, 2011. С. 99–100.

Предложенная классификация уточнена Н.М. Кониным, выделившим пять групп мер административного принуждения: меры предупреждения для общественных нужд в силу сложившихся обстоятельств; контрольно-предупредительные меры; меры пресечения; меры обеспечения производства по делам об административных правонарушениях; меры административной ответственности³³⁹.

Административное принуждение в информационной сфере целесообразно рассматривать отдельно от иных мер принуждения. Процедуры применения мер административного принуждения в информационной сфере схожи, поскольку их реализация осуществляется путем определяемого законодательством взаимодействия уполномоченного органа с операторами связи, провайдерами хостинга или поисковыми сервисами. Их регулирование также осуществляется в рамках информационного законодательства отдельно от иных мер административного принуждения. В законодательстве закрепляются новые виды мер административного принуждения в информационной сфере (если изначально законодательство регулировало только ограничение доступа к информационным ресурсам, за последние несколько лет появились и иные меры), что свидетельствует о необходимости формирования общих положений их применения. Кроме того, сложившаяся в административном праве классификация мер административного принуждения основана на критерии цели их применения, в то время как административное принуждение в информационной сфере может быть направлено на достижение различных целей.

Меры принуждения в информационной сфере – меры административного информационного воздействия - могут быть определены как отдельный вид мер административного принуждения, состоящий во властном управленческом воздействии органа исполнительной власти на информационный ресурс с целью ограничения доступа к противоправной информации на территории государства либо понуждения владельца информационного ресурса к соблюдению законодательства. Меры административного информационного воздействия

³³⁹ Конин Н.М. Административное право России в вопросах и ответах: учебное пособие. М.: Проспект, 2013. С. 84–85.

обладают следующими особенностями: возможность реализации мер безотносительно установления личности субъекта; реализация мер воздействия в случаях, когда информация или деятельность владельца информационного ресурса являются противоправными; временный характер применяемых мер.

Практическая значимость обособления мер административного информационного воздействия обосновывается необходимостью развития общих положений о применении указанных мер, схожих с точки зрения процедур их применения, в информационном законодательстве, а также утверждения их единой законодательной классификации.

Меры административного информационного воздействия следует отличать от мер, направленных на исполнение судебного решения. Степень судебного усмотрения о необходимых мерах для устранения нарушения также гораздо шире, чем территориальное ограничение доступа к информационным ресурсам. Например, суд может предписать прекращение делегирования домена определенному лицу в случае выявления сходства доменного имени с соответствующим товарным знаком³⁴⁰.

Во Франции примером таких мер является решение суда в порядке срочного рассмотрения (*de référé*) об ограничении доступа к противоправному террористическому контенту в соответствии со статьей 706-23 Кодекса уголовной процедуры Франции³⁴¹. В порядке срочного рассмотрения суды также могут принимать решения и по иным делам, например, по блокировке сайтов с контрафактом³⁴².

³⁴⁰ Пункт 158 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда РФ, № 7, июль, 2019; Постановление Суда по интеллектуальным правам от 03.02.2020 № С01-1508/2019 по делу № А40-311941/2018 // СПС «КонсультантПлюс».

³⁴¹ Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029759791/ (дата обращения: 06.03.2023).

³⁴² Tribunal judiciaire de Paris, ordonnance de référé du 8 janvier 2020. URL: <https://www.legalis.net/jurisprudences/tribunal-judiciaire-de-paris-ordonnance-de-refere-du-8-janvier-2020/> (дата обращения: 06.03.2023); Tribunal de grande instance de Paris, 3ème chambre, 1ère section, jugement du 4 décembre 2014. URL: <https://www.legalis.net/jurisprudences/tribunal-de->

Меры исполнения судебного решения, в отличие от мер административного принуждения, не предоставляют органу исполнительной власти возможности принятия самостоятельного решения о применении ограничений к информационным ресурсам или исследования таким органом обстоятельств необходимости ограничения доступа к информационным ресурсам с целью последующей передачи решения для вынесения в суд (судебный порядок применения мер административного принуждения). Органы исполнительной власти, применяя меры в соответствии с вынесенным судебным решением, лишь исполняют решение суда, не обладая автономией, присущей им при реализации мер административного принуждения и не обладая особым статусом в судебных процедурах гражданского и арбитражного процесса, за исключением обычного процессуального статуса, если соответствующий орган исполнительной власти инициирует иск в пределах своей компетенции.

Не является мерами административного информационного воздействия также принятие решения о присвоении лицу определенного статуса, ограничивающего деятельность такого лица в информационной сфере. В частности, статус иностранного агента возникает с момента внесения Министерством юстиции Российской Федерации соответствующего лица в реестр³⁴³. Однако исполнение обязанностей и соблюдение запретов, связанных с деятельностью иностранных агентов, осуществляются не в соответствии с требованием отдельного органа исполнительной власти, а в соответствии с положениями закона.

Меры административного информационного воздействия могут реализовываться либо в судебном порядке, либо во внесудебном порядке. Судебный порядок назначения мер административного информационного воздействия позволяет, во-первых, обеспечить возможность подвластного субъекта приносить возражения, высказывать свою позицию в отношении

[grande-instance-de-paris-3eme-chambre-1ere-section-jugement-du-4-decembre-2014-2/](#) (дата обращения: 06.03.2023).

³⁴³ Федеральный закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием» от 14.07.2022 № 255-ФЗ // Российская газета, № 154-155, 19.07.2022.

предполагаемого факта – основания для применения мер принуждения. Во-вторых, судебный порядок применения мер административного информационного воздействия позволяет обеспечить судебный независимый контроль в отношении законности предлагаемых мер административного принуждения. Недостатком судебного порядка является длительность процедуры, не позволяющая органу исполнительной власти оперативно реагировать на вызовы информационной безопасности. Основанием для применения судебного порядка принятия решения о применении мер административного информационного воздействия является необходимость установления факта нарушения требований законодательства, оценка которого не может быть осуществлена органом исполнительной власти самостоятельно в рамках его компетенции.

В российском законодательстве ограничение доступа к информационному ресурсу путем административного принуждения, реализуемого в судебном порядке, осуществляется в отношении: ограничения доступа к информации, признанной запрещенной на территории Российской Федерации в силу судебного решения (пункт 2 части 5 статьи 15.1 Закона об информации), ограничения доступа к аудиовизуальному сервису (часть 14 статьи 10.5 Закона об информации), ограничения доступа к информационному ресурсу организатора распространения информации в сети Интернет в случае нарушения им возложенных на него обязанностей (статья 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ³⁴⁴ (далее – Закон об информации)), а также включения в реестр нарушителей прав субъектов персональных данных (статья 15.5 Закона об информации). Применение мер ограничения доступа к сайтам, нарушающим авторские права, является формой защиты гражданского права и предварительной обеспечительной мерой, принимаемой судом самостоятельно, без подготовки материалов или составления протокола органом исполнительной власти, в связи с чем к административно-принудительным мерам не относится.

³⁴⁴ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета, № 165, 29.07.2006.

К мерам административного информационного воздействия, реализуемым в судебном порядке, относится и ограничение доступа к информационному ресурсу иностранного средства массовой информации, выполняющего функции иностранного агента (статья 15.9 Закона об информации). Основанием для принятия органом по надзору в сфере коммуникаций и связи решения об ограничении доступа к информационному ресурсу в данном случае является решение о привлечении к ответственности за совершение административного правонарушения. Из формулировок закона следует, что орган исполнительной власти осуществляет процедуру блокировки безотносительно соответствующего предписания суда, но основываясь на судебном решении о применении мер административного взыскания за нарушение требований к деятельности иностранного агента.

Особо широко используется среди мер административного принуждения в судебном порядке ограничение доступа к информации, признанной запрещенной на территории Российской Федерации в силу судебного решения, выносимого в порядке административного судопроизводства³⁴⁵ (пункт 2 части 5 статьи 15.1 Закона об информации). Указанное положение позволяет Прокуратуре Российской Федерации обращаться с исками о признании информации запрещенной в тех случаях, которые напрямую не были отнесены законодателем к ведению административного органа. Например, по указанным основаниям осуществляется блокировка сайтов с информацией о способах хищения энергоносителей³⁴⁶, информации, побуждающей общество к незаконному уходу от уплаты налогов, суицидальному поведению, жестокому обращению с животными³⁴⁷. При этом признание информации запрещенной осуществляется исходя из нарушения публично-правового запрета, а не обстоятельств частного-правового спора.

³⁴⁵ Пункт 42 Обзора судебной практики Верховного Суда Российской Федерации № 2 (2018) (утв. Президиумом Верховного Суда РФ 04.07.2018) // Бюллетень Верховного Суда РФ, № 3, март, 2019 (начало), Бюллетень Верховного Суда РФ, № 4, апрель, 2019 (окончание).

³⁴⁶ Кассационное определение Первого кассационного суда общей юрисдикции от 21.12.2021 № 88а-32234/2021 // СПС «КонсультантПлюс».

³⁴⁷ Кассационное определение Девятого кассационного суда общей юрисдикции от 03.02.2021 N 88а-754/2021 по делу № 2а-9/2020 // СПС «КонсультантПлюс».

Например, суды отказали в признании информации о частной жизни лица, распространяемой без его согласия, запрещенной к распространению на территории Российской Федерации³⁴⁸. Запрет на распространение информации из частно-правовых отношений является мерой исполнения судебного решения, но не мерой административного принуждения, реализуемой в судебном порядке.

Внесудебный порядок применения мер административного информационного воздействия характеризуется более ускоренной процедурой, позволяющей в упрощенном порядке принять надлежащие меры реагирования на факты, несущие наиболее высокие риски информационной и общественной безопасности. В российском законодательстве присутствует множество оснований для применения мер административного информационного воздействия по ограничению доступа к информационным ресурсам во внесудебном порядке: ограничение доступа к информации, распространение которой в Российской Федерации запрещено (пункт 1 части 5 статьи 15.1 Закона об информации); ограничение доступа к информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории (статья 15.1-1 Закона об информации); ограничение доступа к недостоверной информации, которая порочит честь и достоинство гражданина (физического лица) или подрывает его репутацию и связана с обвинением гражданина (физического лица) в совершении преступления (статья 15.1-2 Закона об информации); ограничение доступа к информации, распространяемой с нарушением закона (статья 15.3 Закона об информации); ограничение доступа к информации, распространяемой с нарушением требований законодательства

³⁴⁸ Кассационное определение Девятого кассационного суда общей юрисдикции от 11.11.2020 № 88а-7747/2020 // СПС «КонсультантПлюс».

Российской Федерации о выборах и референдумах, и (или) агитационных материалов, изготовленных и (или) распространяемых с нарушением требований законодательства Российской Федерации о выборах и референдумах (статья 15.3-1 Закона об информации); ограничение доступа к копиям заблокированных сайтов (статья 15.6-1 Закона об информации); ограничении доступа к программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен (часть 10 статьи 15.8 Закона об информации).

Внесудебный порядок применения мер административного информационного воздействия предполагает привлечение дополнительных государственных органов при принятии решения об ограничении доступа к информационному ресурсу, если установление факта нарушения следует из компетенции такого органа. Например, Прокуратура Российской Федерации по этим основаниям рассматривает обращение с просьбой об ограничении доступа к информации, которая связана с обвинением гражданина в совершении преступления (статья 15.1-2 Закона об информации), поскольку прокуратура в рамках своих полномочий вправе направить поступившие материалы для проверки на предмет уголовного преследования в соответствующий орган предварительного расследования³⁴⁹. Аналогично распределяются полномочия о принятии решений об ограничении доступа к информационным ресурсам органами, определенными Правительством Российской Федерации в соответствии со статьей 15.1 Закона об информации, принимающими решение о выявлении информации, распространения которой в России запрещено³⁵⁰.

В качестве особого случая, когда решение об ограничении доступа осуществляется с возложением законодателем отдельных полномочий на орган исполнительной власти, является блокировка копий заблокированных сайтов посредством обращения в Минцифры (статья 15.6-1 Закона об информации). В

³⁴⁹ Пункт 4 части 1 статьи 140 Уголовного процессуального кодекса Российской Федерации от 18.12.2001 № 174-ФЗ // Российская газета, № 249, 22.12.2001.

³⁵⁰ Перечень приведен в Постановлении Правительства РФ от 26.10.2012 № 1101 // Российская газета, № 249, 29.10.2012.

данном случае орган исполнительной власти осуществляет сверку содержания сайтов.

Перечень мер административного информационного воздействия расширился с принятием Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации»³⁵¹ (далее - Закон о деятельности иностранных лиц). Статья 9 указанного закона устанавливает широкий перечень мер административного принуждения, принимаемых органом во внесудебном порядке, к иностранным лицам в сети Интернет, включая оповещение пользователей о нарушении законодательства информационным ресурсом, запрет рекламы, удаление из поиска, ограничение доступа к информационному ресурсу.

Во Франции термин мер административного принуждения отсутствует. Развитие мер административного взыскания вызвано во многом влиянием европейского права и остается слабо развитым с точки зрения единой теоретической системы и законодательства, сохраняется система трех видов уголовных правонарушений³⁵². В отношении административно-предупредительных и административно-пресекательных мер используется термин «меры полиции» (*mesures de police*)³⁵³. Практика Государственного совета Франции, с одной стороны, утверждает исполнительный характер акта органа исполнительной власти в качестве «фундаментального правила публичного права»³⁵⁴. С другой стороны, Государственным советом выработаны критерии оценки допустимости той или иной принятой меры. В частности, ограничение прав и свобод граждан путем административного принуждения возможно только в

³⁵¹ Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» // Собрание законодательства Российской Федерации от 2021 г., № 27, ст. 5064. (Часть первая).

³⁵² См., напр.: Мешков П.В. О проблемах понимания и реализации обеспечительных мер в производстве по делам об административных правонарушениях в России и за рубежом // Юрист. 2018. № 10. С. 64–69.

³⁵³ Napoli P. Qu'est-ce qu'une mesure de police? Considérations historiques après Gênes 2001 // *Multitudes*, 2003/1. № 11. P. 49 - 56.

³⁵⁴ Conseil d'Etat, Assemblée, 2 juillet 1982, Huglo, requête numéro 25288, publié au recueil. URL: <https://www.revuegeneraledudroit.eu/blog/decisions/conseil-detat-assemblee-2-juillet-1982-huglo-requete-numero-25288-publie-au-recueil/> (дата обращения: 06.03.2023).

случае рисков публичному порядку при условии пропорциональности такого ограничения. Эта правовая позиция была сформулирована Государственным советом в 1933 году по делу Benjamin, когда орган признал необоснованным запрет на проведение мероприятия³⁵⁵. Дополнительно в 2011 году Государственный совет Франции уточнил, что принимаемые органом исполнительной власти меры должны быть соответствующими, необходимыми и пропорциональными защите публичного порядка (*adaptées, nécessaires, proportionnées*)³⁵⁶.

За счет малого развития института административных правонарушений и верховенства теории исполнительности административных актов во французском праве отсутствуют аналоги административного принуждения в судебном порядке в информационной сфере. Орган исполнительной власти не лишен возможности при необходимости обратиться с требованием о принятии необходимых мер к суду в порядке срочного рассмотрения. Однако блокировка в таком случае будет мерой исполнения решения суда, поскольку у органа исполнительной власти отсутствует отдельная процессуальная роль в такой процедуре.

Законодательством, однако, устанавливаются отдельные меры внесудебного административного принуждения в информационной сфере. Например, должностные лица органа по защите прав потребителей вправе требовать в случае выявления нарушений владельцем информационного ресурса: размещения соответствующего информационного оповещения онлайн-платформами, ограничения доступа к противоправному контенту, в том числе путем блокировки доступа, а также блокировки доменного имени на срок до трех месяцев, продлеваемый единожды, с последующим принятием решения о прекращении прав в отношении домена или его передаче органу³⁵⁷.

³⁵⁵ Conseil d'État, 19 mai 1933, Benjamin. URL: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/1933-05-19/17413> (дата обращения: 06.03.2023).

³⁵⁶ Conseil d'État, Assemblée, 26/10/2011, 317827, Publié au recueil Lebon. URL: <https://www.legifrance.gouv.fr/ceta/id/CETATEXT000024736671> (дата обращения: 06.03.2023).

³⁵⁷ Art. L521-3-1, Code de la consommation. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069565/LEGISCTA000032223181/#LEGISCTA000032224975 (дата обращения: 06.03.2023).

Кроме того, статьей 6-1 Закона Франции о доверии в цифровой экономике³⁵⁸ предусмотрена возможность ограничения доступа к информационным ресурсам во внесудебном административном порядке в случаях, когда на таких ресурсах размещается детская порнография или сведения, призывающие к участию в террористических актах или одобряющие их. Уполномоченным административным органом для принятия решения об ограничении доступа является структурное подразделение Министерства внутренних дел Франции - Центральный офис борьбы с преступностью в сфере информационных технологий и коммуникаций (OCLCTIC) в составе Центральной дирекции судебной полиции³⁵⁹. Решения OCLCTIC направляются квалифицированному лицу из числа членов Национальной комиссии по информатике и свободам Франции, которое может опротестовать блокировку информационного ресурса. Таким образом в рамках внесудебной блокировки, осуществляемой органами внутренних дел, французским законодателем исключена необходимость судебного порядка, однако введен дополнительный контролирующий орган. Это позволяет оптимизировать сроки ограничения доступа к очевидно противоправной информации, уменьшая риск превышения полномочий.

С учетом проведенного сравнения мер административного информационного воздействия в России и Франции можно выделить следующие их виды, общие для рассматриваемых стран: 1) ограничение доступа к информационному ресурсу; 2) запрет на поисковую выдачу; 3) информирование пользователей оператором поисковой системы о нарушении законодательства на информационном ресурсе.

Таким образом, меры административного информационного воздействия представляют собой отдельную разновидность мер административного

³⁵⁸ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/> (дата обращения: 06.03.2023).

³⁵⁹ Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030195477/2021-02-22/> (дата обращения: 06.03.2023).

принуждения. Указанные меры могут осуществляться в судебном или во внесудебном порядке. Само по себе решение о применении мер административного информационного воздействия, вне зависимости от порядка его принятия, может быть обжаловано в судебном порядке, что создает необходимые гарантии защиты граждан и организаций от неправомерной блокировки информационного ресурса. Однако судебные процедуры применения мер административного информационного воздействия применяются в тех случаях, когда суд дополнительно должен принять решение о нарушении законодательства владельцем информационного ресурса и принятие такого решения не отнесено законодателем к самостоятельной компетенции органа исполнительной власти.

ГЛАВА 3. ПРАВОВЫЕ МОДЕЛИ РЕГУЛИРОВАНИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

3.1. Законодательство об электронном правительстве

Цифровизация деятельности всех государственных органов власти характеризуются в широком смысле термином «электронное государство»³⁶⁰. Для характеристики особенностей использования информационных технологий в деятельности органов исполнительной власти в узком смысле, а также в более широком смысле – для характеристики изменения государственного управления в связи с цифровизацией деятельности органов исполнительной власти, - используется термин «электронное правительство».

Дальнейшее развитие целей электронного правительства привело наряду с этим термином к возникновению таких смежных понятий как «открытое правительство» (open government, government 2.0), «цифровое правительство» (smart government, digital government). В современной литературе также используются термины «экосистема»³⁶¹, «платформа»³⁶². Однако указанные термины лишь конкретизируют отдельные направления развития электронного правительства в целом³⁶³. Указанное развитие не случайно – новые термины отражают поступательное движение от информационного обеспечения деятельности органов исполнительной власти к развитию интерактивных форм

³⁶⁰ Бачило И.Л. Правовая платформа построения электронного государства // Информационное право. М.: Юрист, 2008, № 4. С. 3–8; Богдановская И.Ю. Понятие «электронного государства»: правовые аспекты // Информационное общество и социальное государство: сборник научных работ. М.: ИГП РАН, 2009. С. 45–55; Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении: автореф. дис. ... д.ю.н. Саратов, 2014.

³⁶¹ Harrison T.M., Pardo T.A., Cook M. Creating open government ecosystems: a research and development agenda // Future Internet. 2012. № 4(4). P. 900–928; Dawes S.S., Vidiasova L., Parkhimovich O. Planning and designing open government data programs: An ecosystem approach // Government Information Quarterly. 2016. Volume 33. Issue 1. P. 15–27.

³⁶² O'Reilly T. Government as a Platform // innovations. 2010. Vol. 6. №. 1. P. 13–40.

³⁶³ Схожий подход характерен для работ, обобщающих различные элементы электронного государства. Напр.: Sun P.-L. et al. An implementation framework for E-Government 2.0. // Telematics and Informatics. 2015. Issue 32. P. 504–520; Abu-Shanab E., Harb Y. E-government research insights: Text mining analysis // Electronic Commerce Research and Applications. 2019.

взаимодействия органов исполнительной власти с гражданами и построению взаимного диалога.

Лидирующими странами по уровню развития электронного правительства по данным Организации Объединенных Наций³⁶⁴ являются страны северной Европы (Дания, Исландия, Финляндия, Швеция), а также США. Россия и Китай занимают соответственно 42 и 43 место в общем рейтинге стран. Наиболее высокое развитие электронное правительство получило в европейском регионе, где 81 % стран имеет самый высокий («very high») индекс развития электронного правительства. Азиатские и американские страны также сохраняют высокий уровень развития электронного правительства. Однако в азиатских странах более высокая доля государств с самым высоким («very high») индексом развития электронного правительства (32% против 24 % в американских странах), в то время как в американском регионе больше стран с высоким («high») индексом развития электронного правительства (69 % против 47% в азиатских странах). Наименее развито электронное правительство в странах Африки и Океании³⁶⁵.

Развитие электронного правительства приводит к изменениям в законодательстве, регулирующем деятельность органов исполнительной власти. Электронное правительство начало формироваться на определенном этапе развития конституционного государства, когда оно уже сформировалось и как правовое, и как социальное³⁶⁶. С учетом этого электронное правительство представляет собой новый этап развития конституционного государства в целом,

³⁶⁴ Организация Объединенных Наций использует Индекс развития электронного правительства. Одним из его компонентов является Индекс онлайн-услуг, в котором предоставление услуг и электронное взаимодействие (e-participation) в совокупности занимают 80%, в то время как инфраструктура (10%), технологии (5%) и доступность контента (5%) занимают меньшее значение. UN E-Government Survey 2022. P. 191. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%205.pdf> (дата обращения: 05.03.2023).

³⁶⁵ UN E-Government Survey 2022. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%202.pdf> (дата обращения: 05.03.2023).

³⁶⁶ Богдановская И.Ю. Понятие «электронного государства»: правовые аспекты // Информационное общество и социальное государство: сборник научных работ. М.: ИГП РАН, 2009. С. 45–55.

определяя особенности реализации прав и свобод человека и гражданина с учетом сформировавшихся конституционно-правовых ценностей.

В настоящее время эволюция электронного государства не оказала влияния на конституционные изменения, однако определяется возникающими в конституциях информационными правами человека и гражданина³⁶⁷.

Например, в части 2 статьи 5А Конституции Греции закреплена обязанность государства содействовать доступу к информации и электронному обмену для реализации прав граждан на участие в информационном обществе³⁶⁸. В Конституции Российской Федерации закреплена свобода информации. В конституциях других стран (Финляндия, Норвегия, Польша, Эстония) также содержатся положения, посвященные праву на информацию и праву на доступ к информации³⁶⁹.

На законодательном уровне регулирование электронного правительства развивается более активно. Сравнительно-правовое исследование показывает, что в одних странах принимаются законы об электронном правительстве (США, Италия, Германия, Австрия), в то время как других странах электронное правительство регулируется в рамках более общего законодательства о деятельности органов исполнительной власти (Франция, Швеция, Россия). В Канаде регулирование электронного правительства осуществляется на подзаконном уровне.

В случае, когда нормы об электронном правительстве включаются в более общие акты, использование информационных технологий в деятельности органов исполнительной власти рассматривается в качестве одного из направлений

³⁶⁷ «Доступ к электронным коммуникационным системам и службами приобретает правовой характер по мере того, как общество осознает, что такой доступ – это право личности, определяющее деятельность государственных органов». См.: Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М.: ЗАО «Юстицинформ», 2009. С. 235.

³⁶⁸ The Constitution of Greece. As revised by the parliamentary resolution of May 27th, 2008, of the VIIIth Revisionary Parliament. URL: <https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf> (дата обращения: 05.03.2023).

³⁶⁹ Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М.: ЗАО «Юстицинформ», 2009. С. 7–17.

развития деятельности органов исполнительной власти. Принимаемые нормы лишь уточняют особенности деятельности органов исполнительной власти с учетом развития электронного правительства.

В Российской Федерации принято несколько законов, посвященных отдельным аспектам государственного управления в цифровой сфере. В них содержатся положения об общем правовом режиме информации³⁷⁰, общие особенности предоставления государственных услуг, в том числе в цифровой среде, положения об электронной идентификации граждан при оказании государственных услуг³⁷¹. Устанавливаются дополнительные требования, направленные на обеспечение информационной безопасности наиболее значимых элементов информационной инфраструктуры государства³⁷². Однако единого акта, регулирующего электронное правительство, не принято. В целом российский законодатель ищет новую модель регулирования административных отношений и нормы об электронном правительстве также включаются в состав более общих положений. Об этом свидетельствуют и новые реформы в сфере контрольно-надзорной деятельности, развитие административной юстиции.

Для Франции также характерно усовершенствование административного законодательства в целом. Во Франции отдельные положения, регулирующие информационную сферу, были изложены в Законе о цифровой республике от 7 октября 2016г.³⁷³. Однако общее регулирование деятельности органов исполнительной власти определено Кодексом об отношениях между

³⁷⁰ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

³⁷¹ Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета, № 168, 30.07.2010.

³⁷² Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ", 31.07.2017, № 31 (Часть I), ст. 4736.

³⁷³ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL:https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=91758002E1CCA159BABD6D3F5D4B33F4.tplgfr34s_2?cidTexte=JORFTEXT000033202746&categorieLien=id (дата обращения: 05.03.2023).

администрацией и обществом³⁷⁴. Французский подход соответствует общей направленности государственной политики не столько в сторону развития электронного правительства, сколько к усовершенствованию системы государственного управления в целом.

Шведский законодатель, в отличие от Франции и России, медленнее реагирует на необходимость регулирования электронного правительства, дополняя законодательство с учетом сложившейся правовой традиции регулирования и организации системы подчинения органов исполнительной власти. В Швеции в 2010г. был принят Билль о публичной администрации, часть которого посвящена отдельным особенностям электронного правительства³⁷⁵. Если в части доступа к электронным документам органов исполнительной власти Швеция дополнила законодательство в 1970-е годы, иные направления деятельности органов исполнительной власти в сфере электронного правительства осуществляются без внесения дополнительных изменений в законодательство и рассматриваются в контексте общего регулирования деятельности органов исполнительной власти³⁷⁶.

В некоторых странах, наоборот, принимаются отдельные законы об электронном правительстве. Большинство стран, которые принимали законы об электронном правительстве, дополнительно принимали и другие законы, регулирующие отдельные аспекты деятельности органов исполнительной власти в электронной форме.

Закон об электронном государстве 2002 г.³⁷⁷ в США устанавливает обязанности агентств организовать официальные сайты в сети Интернет,

³⁷⁴ Code des relations entre le public et l'administration. URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=91C91B1A73A68E15149FA32687E64163.tplgfr34s_2?idSectionTA=LEGISCTA000031367685&cidTexte=LEGITEXT000031366350&dateTexte=20190210 (дата обращения: 05.03.2023).

³⁷⁵ Joinup. E-Government in Sweden, February 2016, Edition 18.0. URL: https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment%20in%20Sweden%20-%20February%202016%20-%2018_0_v1_00.pdf (дата обращения: 05.03.2023).

³⁷⁶ Reichel J. Regulating Automation of Swedish Public Administration // CERIDAP. Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche. 2023. № 1. P. 75–94.

³⁷⁷ USA. E-Government Act of 2002. URL: <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf> (дата обращения: 05.03.2023).

определяет правовой режим отдельных категорий информации в распоряжении агентств, вопросы информационной безопасности. Однако деятельность электронного правительства регулируют и другие законы – например, в части организации хранения электронных федеральных документов³⁷⁸, обеспечения доступа к информации о деятельности федеральных агентств³⁷⁹. Закон об электронном государстве установил условия для внедрения информационных технологий в деятельность агентств США. Однако дальше развитие электронного правительства получило новое направление, связанное с усилением взаимодействия органов исполнительной власти с невластными субъектами в информационной сфере. Закон об электронном государстве, таким образом, заложил основы перехода органов исполнительной власти к электронному правительству³⁸⁰.

В Италии, в отличие от США активно развивающей кодификацию, в 2005 году был принят Кодекс электронного правительства³⁸¹, который регулирует взаимодействие граждан в отношениях с государством в электронной сфере, организацию электронного документооборота, электронные подписи и электронный обмен данными. Кодекс регулирует отношения между публичными органами в информационной сфере и направлен на повышение эффективности государственного управления³⁸². Некоторые положения регулируются отдельно. Например, обработка персональных данных в публичном секторе регулируются Кодексом о защите персональных данных³⁸³.

³⁷⁸ Sec. 3301, (a), Presidential and Federal Records Act Amendments of 2014. URL: <https://www.congress.gov/bill/113th-congress/house-bill/1233/text> (дата обращения: 05.03.2023).

³⁷⁹ USA. Freedom of Information Act. PUBLIC LAW 89-487-JULY 4, 1966. URL: <https://www.govinfo.gov/content/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf> (дата обращения: 05.03.2023).

³⁸⁰ Минервин И.Г. Эволюция электронного правительства в США // Экономические и социальные проблемы России. 2015. № 2. С. 48–75.

³⁸¹ Codice dell'amministrazione digitale. Decreto Legislativo 7 marzo 2005, n. 82. URL: <https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/index.html> (дата обращения: 05.03.2023).

³⁸² Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М.: ЗАО «Юстицинформ», 2009. С. 233.

³⁸³ Italian Personal Data Protection Code. URL: <http://www.privacy.it/archivio/privacypcode-en.html> (дата обращения: 05.03.2023).

Положительно можно оценить Федеральный закон Германии об электронном правительстве 2013 г. (*Gesetz zur Förderung der elektronischen Verwaltung*)³⁸⁴. Закон предусматривает общие положения об электронном документообороте, стандартизации в информационной сфере, правовом режиме пространственных и персональных данных, использовании официальных сайтов в сети Интернет и официальной электронной почты (*De-Mail*). Несмотря на наличие дополнительных законов в сфере электронного правительства (например, в части усовершенствования государственных услуг онлайн³⁸⁵, цифровых подписей, последующего использования информации публичного сектора³⁸⁶), указанный закон в краткой и лаконичной форме затрагивает все основные аспекты правового регулирования электронного правительства.

Закон об электронном правительстве 2004 г.³⁸⁷ принят также в Австрии, однако он регулирует преимущественно электронные способы удостоверения личности и формирование системы электронной идентификации. В целом для регулирования электронного правительства в Австрии действует множество иных законов³⁸⁸.

Стоит отметить также принятие отдельных законов об электронном правительстве в ряде иных стран: Закон об электронном правительстве Танзании 2019 г., учредивший отдельное ведомство в сфере электронного правительства³⁸⁹,

³⁸⁴ German Act to promote electronic government. Translation provided by Gary Cox for the Federal Ministry of the Interior. The translation includes the amendment(s) to the Act by Article 1 of the Act of 25 July 2013 (Federal Law Gazette I p. 2749). URL: http://www.gesetze-im-internet.de/englisch_egovg/englisch_egovg.html#p0014 (дата обращения: 05.03.2023).

³⁸⁵ Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen. URL: <https://www.gesetze-im-internet.de/ozg/> (дата обращения: 05.03.2023).

³⁸⁶ European Commission. E-Government in Germany, February 2016, Edition 18.0. URL: https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment%20in%20Germany%20-%20February%202016%20-%202018_00%20-%20v2_00.pdf (дата обращения: 05.03.2023).

³⁸⁷ Österreich. Gesamte Rechtsvorschrift für E-Government-Gesetz, Fassung vom 20.06.2020. URL: [https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230#:~:text=\(1\)%20Dieses%20Bundesgesetz%20dient%20der,an%20diese%20Stellen%20erleichtert%20werden.](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230#:~:text=(1)%20Dieses%20Bundesgesetz%20dient%20der,an%20diese%20Stellen%20erleichtert%20werden.) (дата обращения: 05.03.2023).

³⁸⁸ European Commission. E-Government in Austria, January 2015, Edition 18.0. URL: https://joinup.ec.europa.eu/sites/default/files/document/2015-03/egov_in_austria_-_january_2015_-_v_18_0_final.pdf (дата обращения: 05.03.2023).

³⁸⁹ Tanzania. E-Government Act, 2019. URL: <https://gisp.gov.go.tz/assets/docs/e-Government%20Act,%202019.pdf> (дата обращения: 05.03.2023).

Законы о цифровом правительстве государства Белиз³⁹⁰ и Независимого государства Папуа Новая Гвинея от 2022 года³⁹¹.

В Канаде, в отличие от указанных ранее стран, регулирование электронного правительства осуществляется на подзаконном уровне и ориентировано в первую очередь на развитие цифровых сервисов. Для регулирования электронного правительства принимаются акты органов исполнительной власти: политики, устанавливающие общие цели развития электронного правительства, и директивы, конкретизирующие необходимые меры по достижению установленных политиками целей. С 1 апреля 2020 г. в Канаде вступили в силу Политика об услугах и цифровых технологиях³⁹², устанавливающая общие принципы развития информационных систем органов исполнительной власти центрального аппарата, и Директива об услугах и цифровых технологиях³⁹³. Политика, утвержденная Казначейством Канады, является обязательным для исполнения органами центральной администрации нормативным актом, а директива, принятая Председателем Казначейства Канады в исполнение требований политики, конкретизирует требования к органам исполнительной власти по развитию информационных систем. Основной целью принятой политики является усовершенствование государственной деятельности с помощью цифровой трансформации, в то время как иные особенности правового регулирования электронного правительства не охватываются указанными актами.

Сравнение опыта законодательного регулирования электронного правительства показывает, что страны со сложившейся традицией

³⁹⁰ Beliz. An Act to establish the E-Governance and Digitalization Department and provide for its powers, duties and functions; to promote and regulate the provision of electronic government (e-government) services; to enhance service delivery, citizen's access, and the efficiency and effectiveness of government administrative procedures; and to provide for matters connected therewith or incidental thereto. 2022. URL: <https://www.nationalassembly.gov.bz/wp-content/uploads/2022/10/Act-No-24-of-2022-Digital-Government-Act-2022.pdf> (дата обращения: 05.03.2023).

³⁹¹ Papua New Guinea. Digital Government Act. 2022. URL: https://www.parliament.gov.pg/uploads/acts/22A_41.pdf (дата обращения: 05.03.2023).

³⁹² Canada, Policy on Service and Digital. URL: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603> (дата обращения: 05.03.2023).

³⁹³ Canada. Directive on Service and Digital. URL: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601> (дата обращения: 05.03.2023).

административного права (Франция, Швеция), не принимают отдельные законы об электронном правительстве и рассматривают электронное правительство в контексте общей характеристики деятельности органов исполнительной власти.

В Российской Федерации также развивается регулирование электронного правительства в составе общих норм о деятельности органов исполнительной власти. Однако российское законодательство отражает поиск нового подхода к регулированию деятельности органов исполнительной власти в целом: оптимизации государственных и муниципальных услуг, организации предоставления доступа к информации о деятельности государственных органов.

Страны, для которых характерно в большей степени разрешение вопроса о повышении эффективности деятельности органов исполнительной власти, чем развитии отдельных административно-правовых институтов, принимают специальное законодательство, посвященное электронному правительству. В первую очередь к таким странам относятся США и Канада.

Следуют указанному подходу также Италия и Германия. Примечательно, что Италия и Германия занимают 37 и 22 места в общем рейтинге развития электронного правительства³⁹⁴.

В этой связи принятие отдельного закона, посвященного электронному правительству в Российской Федерации, представляется нецелесообразным, поскольку не позволяет развивать отдельные положения об электронном правительстве в рамках более крупных правовых институтов, регулирующих деятельность органов исполнительной власти.

Современный этап развития электронного правительства характеризуется усилением роли частных и государственных цифровых платформ в государственном управлении (3.2). В рамках развития платформенного подхода существенное значение получают регулирование электронного обмена данными

³⁹⁴

органами исполнительной власти (3.3) и государственной электронной идентификации (3.4)³⁹⁵.

3.2. Электронное правительство в эпоху цифровых платформ

С развитием электронного взаимодействия сетевые формы получают все большее распространение в деятельности органов исполнительной власти³⁹⁶.

Именно цифровые платформы являются основной формой организации сетевых связей между различными участниками информационного взаимодействия, которыми являются и органы исполнительной власти.

С одной стороны, частные цифровые платформы используются для сетевого взаимодействия различных участников информационных отношений, включая властных субъектов.

Использование различными участниками сетевого взаимодействия, включая органы исполнительной власти, цифровых платформ приводит к постепенному формированию их публично-правового статуса.

На начальных этапах информатизации широкую роль в определении правового статуса цифровых платформ играло саморегулирование. Большинство из таких платформ, являясь транснациональными корпорациями, стремились

³⁹⁵ Отдельные особенности реализации электронного правительства рассмотрены также в других главах диссертации. В частности, особенности оказания государственных услуг в электронной форме, традиционно характеризующие электронное правительство, а также обязанности органов исполнительной власти по обеспечению их информационной безопасности, рассмотрены во второй главе. В рамках характеристики моделей регулирования электронного правительства выделенные в настоящей главе аспекты представляются наиболее показательными, поскольку они отражают подход государства к развитию информационных систем для целей реализации электронного правительства.

³⁹⁶ «В целях развития цифровой экономики, основанной на использовании данных, необходимо посредством внедрения цифровых технологий и цифровых платформ обеспечить сокращение временных и административных затрат при предоставлении государственных и муниципальных услуг, осуществлении контрольно-надзорных функций, функционировании государственных и муниципальных органов». См.: Основные направления деятельности Правительства Российской Федерации на период до 2024 года (утверждены Председателем Правительства Российской Федерации 29.09.2018). С. 19. URL: <http://static.government.ru/media/files/ne0vGNJUK9SQjIGNNsXIX2d2CpCho9qS.pdf> (дата обращения: 14.05.2023).

сохранить единое регулирование на территории различных стран. Отсюда возникает феномен «права Макдональдса» или «Гугл-права»³⁹⁷, которое на ранних этапах развития цифровизации обеспечивает формирование единой регулятивной среды.

Постепенно, однако, саморегулирование цифровых платформ конкретизируется и уточняется в позитивном праве. Современный этап характеризуется усилением патернализма государственного управления³⁹⁸. Это связано с усилением внимания государств к деятельности транснациональных корпораций и развитием различных мер, направленных на поддержание государственного суверенитета в сети Интернет, как с точки зрения определения границ национальной юрисдикции, так и с точки зрения необходимости усиления системы мер информационной безопасности³⁹⁹.

По характеру функционала цифровые платформы неоднородны: социальные сети, стриминговые сервисы, новостные агрегаторы, агрегаторы для продажи товаров и т.д. Стремление законодателя учесть особенности различных видов платформ приводит к возникновению многообразных технических терминов в законодательстве⁴⁰⁰.

В России онлайн-платформы не определяются в законодательстве. Вместо этого используются другие термины для регулирования деятельности отдельных Интернет-сервисов в зависимости от предоставляемого ими функционала (новостные агрегаторы, аудиовизуальные сервисы, организаторы распространения информации в сети Интернет, социальные сети). Российский подход основан на функциональной дифференциации Интернет-сервисов, к которым относятся и цифровые платформы. Это позволяет регулировать деятельность не только

³⁹⁷ См., напр.: Захарова М.В. Учение о юридических картах мира. М.: Аспект Пресс, 2022.

³⁹⁸ См.: Путило Н.В., Волкова Н.С. Феномен «Nannystate»: новый вид государства или модификация государственного патернализма в современных условиях? // Журнал российского права. 2020. № 12. С. 19–31; Терещенко Л.К. Государственное регулирование и дерегулирование в сфере связи // Журнал российского права. 2019. № 10. С. 98–108.

³⁹⁹ Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации : автореф. дис. ... д.ю.н. Москва, 2021.

⁴⁰⁰ Наумов В.Б. Негативные закономерности формирования понятийного аппарата в сфере регулирования Интернета и идентификации // Информационное право. 2018. № 1. С. 32–39.

цифровых платформ, но также иных субъектов информационных отношений. Цифровые платформы таким образом сочетают несколько информационных правовых статусов в рамках своей деятельности в зависимости от функционала.

Европейский подход непосредственно оперирует термином «онлайн платформа». Статья L111-7 Кодекса потребления Франции выделяет два вида онлайн-платформ: платформы для обмена и поисковые сервисы⁴⁰¹. Более однородное регулирование позволяет уточнять требования к деятельности цифровых платформ в публичном секторе. Например, на онлайн-платформы во Франции возлагаются дополнительные обязанности по раскрытию правил индексации контента, соблюдения отдельных процедур прозрачности в электоральный период⁴⁰². Дополнительно на онлайн-платформы возложена обязанность по обеспечению мер реагирования на незаконный контент при получении сообщений пользователями⁴⁰³.

Органы исполнительной власти также становятся участниками сетевого обмена с невластными субъектами в рамках деятельности цифровых платформ⁴⁰⁴.

⁴⁰¹ «L.-Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur :

1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;

2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service». Code de la consommation. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033219601/ (дата обращения: 05.03.2023).

⁴⁰² Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559> (дата обращения: 05.03.2023).

⁴⁰³ Art. 6-4, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/> (дата обращения: 05.03.2023).

⁴⁰⁴ В частности, органы исполнительной власти как в России, так и за рубежом активно используют цифровые платформы для информирования граждан о своей деятельности. Например, в отчете Национальной комиссии по информатике и свободам Франции за 2021 год учитывается количество зарегистрированных аккаунтов для прохождения массового онлайн-курса по персональным данным и количество пользователей в социальных сетях с указанием процента. CNIL, Rapport annuel, 2021. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf (дата обращения: 05.03.2023).

Федеральная торговая комиссия США также в отчете за 2021 год для конгресса США по контролю в сфере приватности отмечает проведенные мероприятия и созданные для информирования граждан блоги. FTC Report to Congress on Privacy and Security. A Report to

Отношения по использованию социальных сетей предполагают возникновение юридической связи между органом исполнительной власти и цифровой платформой, на которой создается его аккаунт. Создание аккаунта в социальных сетях требует безоговорочное принятие условий пользовательского соглашения, которое не содержит дополнительных положений, регулирующих отношения в сфере обработки пользовательской активности должностных лиц органа исполнительной власти.

Данная проблема находит свое отражение в разрешении вопроса о возможности использования федеральными агентствами США платформы TikTok. Распоряжением Административно-бюджетного управления США от 27.02.2023⁴⁰⁵ на основании Закона об отсутствии ТикТок на государственных устройствах⁴⁰⁶ федеральным агентствам запрещено использовать приложение TikTok, а также любые его аналоги, создаваемые компанией ByteDance Limited.

Частные цифровые платформы могут также использоваться органами исполнительной власти в качестве средств направления официальных уведомлений. В частности, уведомления портала Госуслуги могут направляться пользователям социальной сети «ВКонтакте» с января 2023 года⁴⁰⁷.

Таким образом, правовое регулирование использования органами исполнительной власти частных цифровых платформ нуждается в дополнительном уточнении в законодательстве. Такое использование не может осуществляться на основании безоговорочного принятия органом исполнительной власти условий пользовательского соглашения, в связи с чем в законодательстве необходимо уточнить публично-правовую юридическую связь, которая возникает

Congress. September 13, 2021. URL: https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (дата обращения: 05.03.2023).

⁴⁰⁵ OMB. «No TikTok on Government Devices» Implementation Guidance. February 27, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf (дата обращения: 05.03.2023).

⁴⁰⁶ No TikTok on Government Devices Act. Passed the Senate December 14, 2022. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/1143/text> (дата обращения: 05.03.2023).

⁴⁰⁷ Минцифры России. Уведомления Госуслуг и оплата штрафов ГИБДД теперь доступны ВКонтакте. URL: <https://digital.gov.ru/ru/events/42384/> (дата обращения: 05.03.2023). Дата опубликования: 18.01.2023.

между органом исполнительной власти и цифровой платформой в рамках его присоединения к условиям пользовательского соглашения как гражданско-правовой сделки.

Гражданско-правовая природа отношений между органом исполнительной власти и частной платформой характеризуется возникновением договора между Российской Федерацией или ее субъектом и частной цифровой платформой, поскольку субъектом гражданских правоотношений является публично-правовое образование в соответствии со статьей 124 Гражданского кодекса Российской Федерации⁴⁰⁸. Однако частноправовые средства защиты не позволяют регулировать возникающие в отношении использования официального аккаунта отношения, направлены преимущественно на восстановление имущественного положения потерпевшей стороны.

Нарушение частной цифровой платформой условий использования аккаунта органа исполнительной власти может иметь публично-правовые последствия, которые не могут быть оценены в денежном эквиваленте. Например, утрата доступа к данным для входа в официальный аккаунт органа исполнительной власти, ложное опубликование неправомерной информации с аккаунта органа исполнительной власти или утрата пользовательской истории аккаунта могут негативно отразиться на общественном порядке и безопасности в целом.

В рамках формирования правового режима официальных аккаунтов органов исполнительной власти на частных цифровых платформах необходимо законодательное закрепление особенностей хранения пользовательской информации аккаунта органа исполнительной власти частной цифровой платформой, включая обязанность содействовать в документировании и хранении пользовательской активности аккаунта органа исполнительной власти в социальных сетях. Указанные обязанности могут быть уточнены в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ путем предоставления Правительству Российской

⁴⁰⁸ Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Российская газета, № 238-239, 08.12.1994.

Федерации полномочий по определению условий использования органами исполнительной власти частных цифровых платформ. Такой подход позволит более оперативно реагировать на изменения в функционале частных цифровых платформ и своевременно вводить необходимые уточнения.

С другой стороны, в рамках организации деятельности государственных органов в сети Интернет государство само создает цифровые платформы, необходимые как для межведомственного сетевого взаимодействия, так и для взаимодействия государственных органов с невластными субъектами⁴⁰⁹.

Цифровые платформы как форма организации сетевых связей между различными органами публичной власти особенно актуальны в связи с переходом к обработке данных органами исполнительной власти в информационных системах, их накоплению⁴¹⁰. Отдельное развитие в законодательстве получают государственные реестры – информационные системы, включение в которые является правоустанавливающим фактом⁴¹¹.

Российская Федерация за счет более оперативного и централизованного регулирования информатизации деятельности органов исполнительной власти раньше, чем США и Франция, осуществила переход на реестровую модель государственных и муниципальных услуг, отказавшись от выдачи многих бумажных носителей⁴¹².

Обмен данными, находящимися в информационных системах различных органов исполнительной власти, необходимый для предотвращения дублирования сбора информации разными органами публичной власти в рамках оказания

⁴⁰⁹ Например, в Индии для взаимодействия с гражданами по различным вопросам формирования государственной политики действует платформа MyGov, в которой насчитывается более 28 миллионов пользователей. MyGov: An Overview. URL: <https://www.mygov.in/overview/> (дата обращения: 05.03.2023).

⁴¹⁰ Чаннов С.Е. Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. 2018. № 9. С. 48–54.

⁴¹¹ См.: Терещенко Л.К. Реестровая модель оказания государственных и муниципальных услуг // Журнал российского права. 2021. № 7. С. 110–120.

⁴¹² Статья 7.4 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ, 02.08.2010, № 31, ст. 4179.

государственных и муниципальных услуг, осуществляется с помощью цифровых платформ.

Государственные цифровые платформы упрощают сетевой обмен между различными органами публичной власти. Сетевое горизонтальное взаимодействие между различными участниками информационных отношений осуществляется централизованно с участием органа исполнительной власти, определяющего особенности информационного обмена, а также органа исполнительной власти — оператора цифровой платформы, координирующих информационный межведомственный обмен данными.

Для характеристики сетевого межведомственного взаимодействия, позволяющего сократить издержки по разработке отдельных технологий и информационных систем, Т. О’Райли предложил термин «государство как платформа», предполагающий функционирование механизмов электронного правительства аналогично функционированию различных Интернет-платформ⁴¹³. Использование цифровых платформ в государственном управлении предполагает не только внедрение новых технологий, но и новую модель общественных отношений⁴¹⁴, основанную на организации инфраструктуры для сетевого взаимодействия органов различных уровней публичной власти между собой, а также с невластными субъектами.

В отличие от модели электронного правительства, сфокусированной на развитии государственных информационных систем, «государство как платформа» позволяет объединять различных владельцев информации и обеспечивать обмен данными с использованием инфраструктуры цифровой платформы. Функционально государственная цифровая платформа может быть использована одновременно для реализации государственных функций в

⁴¹³ O’Reilly T. *Government as a Platform // innovations*. 2010. Vol. 6. №. 1. P. 13–40.

⁴¹⁴ Janssen M., Estevez E. *Lean government and platform-based governance—Doing more with less // Government Information Quarterly*. 2013. Issue 30. P. S1–S8; Brown A. et al. *Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: Towards a Platform Assessment Framework (PAF) // Government Information Quarterly*. 2017. Issue 34. P. 167–182.

различных отраслях⁴¹⁵, а также для организации отношений в частноправовой сфере (заключение договоров с использованием платформы, отправка юридически значимых сообщений другим пользователям). Кроме того, цифровая платформа позволяет органам исполнительной власти объединять и анализировать различные виды данных в режиме реального времени для принятия эффективных управленческих решений (cognitive government)⁴¹⁶.

Платформенный подход предполагает большую свободу обмена данными между различными участниками информационного взаимодействия и позволяет реализовывать обмен данными между различными органами публичной власти как в силу требований законодательства, так и в силу отдельных соглашений между ними, обеспечивая безопасность передачи данных.

В настоящий момент в Российской Федерации активно развиваются государственные цифровые платформы. В частности, платформа «ГосТех» позволяет обеспечить централизованное развитие и сопровождение жизненных циклов различных государственных информационных систем⁴¹⁷, Единая информационная платформа национальной системы управления данными

⁴¹⁵ Стырин Е.М., Дмитриева Н.Е., Синятуллина Л.Х. Государственные цифровые платформы: от концепта к реализации // Вопросы государственного и муниципального управления. 2019. № 4. С. 31 -60.

⁴¹⁶ UN E-Government Survey 2022. The Future of Digital Government: Trends, Insights and Conclusions. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%205.pdf> (дата обращения: 05.03.2023).

⁴¹⁷ Распоряжение Правительства РФ от 21.10.2022 № 3102-р «Об утверждении Концепции создания и функционирования единой цифровой платформы Российской Федерации «ГосТех», плана мероприятий («дорожной карты») по созданию единой цифровой платформы Российской Федерации «ГосТех»» // Собрание законодательства РФ, 31.10.2022, № 44, ст. 7594; Постановление Правительства РФ от 16.12.2022 № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555» // Собрание законодательства РФ, 26.12.2022, № 52, ст. 9610.

обеспечивает инфраструктуру обмена данными между информационными системами различных государственных органов⁴¹⁸.

Направление «Государство как цифровая платформа» было закреплено также в пункте 6.1 Общенационального плана действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике (одобрен Правительством РФ 23.09.2020, протокол № 36, раздел VII) (№ П13-60855 от 02.10.2020)⁴¹⁹. В рамках достижения результатов указанного направления указаны сервисы, предоставляющие невластным субъектам инфраструктуру для взаимодействия: создание на Едином портале государственных и муниципальных услуг (функций) сервисов для взаимодействия с банками в рамках получения льготных кредитов; создание единой цифровой платформы ведения и акцептования оферт с использованием инфраструктуры электронного правительства; запуск сервиса «Госпочта», позволяющего полностью цифровизовать документооборот.

Указанные примеры наглядно демонстрируют ключевую особенность подхода «государство как платформа»: государственная платформа может использоваться не только для взаимодействия с органами исполнительной власти, но может также предоставляться для взаимодействия невластных субъектов между собой (например, отправка письменных извещений через Госуслуги). Таким образом в рамках использования цифровой платформы государство создает условия для массового информационного обслуживания за счет взаимодействия государственных и негосударственных информационных ресурсов⁴²⁰. Государство, предоставляя функционал платформы, выступает гарантом

⁴¹⁸ Постановление Правительства РФ от 14.05.2021 № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства РФ, 24.05.2021, № 21, ст. 3585.

⁴¹⁹ СПС «КонсультантПлюс».

⁴²⁰ Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении: автореф. дис. ... д.ю.н. Саратов, 2014. С. 14.

достоверности полученной информации, содержания юридически значимого действия и личности пользователя, совершившего такое действие.

Использование государственной платформы для организации взаимодействия субъектов в невластных информационных отношениях ставит вопрос об ответственности органов исполнительной власти за технические сбои и ошибки государственной платформы. В Российской Федерации предусмотрена гражданско-правовая ответственность публично-правовых образований за совершение незаконного действия или бездействия⁴²¹. Однако техническая ошибка может не быть вызвана незаконными действиями органа исполнительной власти, являющегося оператором государственной платформы. При рассмотрении данного вопроса важно также обратить внимание, что непосредственно техническое обслуживание платформы может осуществляться не органами исполнительной власти, а подведомственными им учреждениями или иными организациями на основании соответствующего государственного контракта.

В этой связи целесообразно внести уточнения в гражданское законодательство, уточняющие гражданско-правовую ответственность публично-правовых образований за технические ошибки государственной платформы при реализации невластных отношений, а также организации, осуществляющей техническое обслуживание государственной платформы.

Исследователи в сфере государственного и муниципального управления отмечают еще одну особенность государственной цифровой платформы: возможность рассмотрения жалоб пользователей внутри платформы с помощью ее функционала («первичный арбитраж»)⁴²², что позволяет также собирать больше информации об удовлетворенности пользователя теми или иными сервисами обмена данными в рамках функционала цифровой платформы.

⁴²¹ Белясов С.Н. Возмещение вреда государством и должностными лицами в решениях Конституционного Суда Российской Федерации // Право и государство: теория и практика. 2017. № 6. С. 21-24.

⁴²² Стырин Е.М., Родионова Ю.Д. единая информационная система в сфере закупок как государственная цифровая платформа: современное состояние и перспективы // Вопросы государственного и муниципального управления. 2019. № 3. С. 49–70.

Американский исследователь А. Аниш в начале XXI в. ввел понятие «алгократии» как нового способа управления⁴²³. Автор выделил ряд особенностей, которые отличают алгократию от привычной бюрократической системы управления, указывая на усиление горизонтальных и послабление вертикальных управленческих связей. Во-первых, особенности функционирования управленцев определены тем программным обеспечением, которое они используют, и его возможностями. Во-вторых, утрачивается роль властно-подчинительных отношений, поскольку акцент смещается в сторону информационных систем как сетей взаимодействия, где каждый управленец выступает отдельным «узлом» соединения.

Подход А. Аниша во многом схож с идеями сетевого государства и общества, предполагавшими ослабление и упразднение вертикальных структур власти, что справедливо подвергается критике в юридической литературе⁴²⁴. Однако отдельные элементы сетевого взаимодействия наиболее заметны в рамках использования органами исполнительной власти государственных и частных цифровых платформ.

Немецкие исследователи Б. Бендер и М. Гейне сформулировали три ключевых признака цифровых платформ, используемых в государственном управлении⁴²⁵. Во-первых, цифровая платформа представляет собой отдельную экосистему, в которой на равных ролях участвуют различные субъекты информационных отношений. В отличие от обычных информационных систем, в платформе нет руководителя, однако есть координатор, обеспечивающий взаимодействие равных субъектов (*orchestration*). Во-вторых, технологическая архитектура платформы предоставляет любым участникам взаимодействия

⁴²³ Aneesh A. Technologically Coded Authority: The Post-Industrial Decline in Bureaucratic Hierarchies, 2002.

⁴²⁴ См.: Липень С. В. Сетевая парадигма и современное государство в юридических исследованиях начала XXI в. // Актуальные проблемы российского права. 2020. Т. 15. № 10. С. 11—19.

⁴²⁵ Bender B., Heine M. Government as a Platform? Constitutive Elements of Public Service Platforms. In: Kö A., Francesconi E., Kotsis G., Tjoa A.M., Khalil I. (eds) Electronic Government and the Information Systems Perspective. Springer. 2021. Vol. 12926. P. 3–20.

возможность самостоятельно ее дорабатывать для собственных нужд, используя ключевые характеристики платформы. Наконец, цифровая платформа отличается особым порядком управления. Оператор платформы использует различные формальные и неформальные механизмы для управления поведением пользователей платформы.

Целесообразно рассмотреть каждую из обозначенных особенностей с правовой точки зрения. Во-первых, в рамках деятельности государственных цифровых платформ органы исполнительной власти осуществляют полномочия по идентификации пользователя и подтверждению целостности и неизменности содержания юридически значимых действий, совершаемых с использованием функционала платформы. Такие юридически значимые действия могут быть как связанными с получением государственных и муниципальных услуг, так и не связанными с оказанием соответствующих услуг органами публичной власти.

Таким образом государственная цифровая платформа становится способом обеспечить надлежащий уровень доверия для осуществления отношений между невластными субъектами в сети Интернет.

Во-вторых, особенностью государственных цифровых платформ является их реализация для выполнения публичных функций государства. Сервисы платформы, используемые различными невластными субъектами, не могут формироваться только на основании отдельного гражданско-правового соглашения между оператором платформы и соответствующим субъектом. Правовым основанием функционирования сервиса и заключения соответствующего соглашения должно быть уполномоченное решение соответствующего органа исполнительной власти.

Наконец, необходимо дополнительное правовое регулирование деятельности оператора платформы, осуществляющего первичное разрешение споров по поступившим от пользователя обращениям (техническая поддержка). Отношения по использованию государственной цифровой платформы не могут быть основаны на принятии пользовательского соглашения. Правила использования платформы определяются соответствующими нормативными

правовыми актами и являются обязательными для пользователя не в силу его согласия с условиями пользовательского соглашения, а в силу непосредственной императивной силы властного предписания органа исполнительной власти о правилах использования соответствующей платформы.

Внедрение государственных цифровых платформ позволяет органам исполнительной власти получать доступ к данным других участников информационного взаимодействия, а также определять правила реализации правовых отношений между пользователями платформы. Сетевая форма взаимодействия, организуемая в рамках государственной цифровой платформы, приводит к установлению иерархического контроля органа исполнительной власти – оператора цифровой платформы – за деятельностью участников информационных отношений. Что усиливает централизацию регулирования информационной сферы и требует дополнительных правовых гарантий, препятствующих злоупотреблению оператором государственной цифровой платформы полномочиями по ее техническому и организационному обеспечению.

Российский подход по своему содержанию наиболее близок технократической модели «государства как платформы»⁴²⁶. Реализация «государства как платформы» изначально предполагает дата-центрированный подход, снижающий издержки по обмену данными между различными информационными системами. Технологическое развитие цифровых платформ, однако, не исключает необходимости уточнения правового статуса органов исполнительной власти, осуществляющих полномочия по развитию цифровой платформы и управлению ей.

Таким образом, с развитием электронного взаимодействия увеличивается значение сетевых связей между органами различных уровней публичной власти и невластными субъектами. Важной формой развития сетевых связей являются цифровые платформы. Платформенный подход усиливает сочетание частно-

⁴²⁶ Smorgunov L. Government as a Platform: Critics of a Technocratic Culture of Public Governance in Digital Era. In: Alexandrov D., Boukhanovsky A., Chugunov A., Kabanov Y., Koltsova O., Musabirov I. (eds) Digital Transformation and Global Society. DTGS 2019. Communications in Computer and Information Science. Springer. 2019. Vol. 1038. P. 41–54.

правовых и публично-правовых методов регулирования деятельности органов исполнительной власти в информационной сфере.

На основе анализа государственных и частных цифровых платформ представляется целесообразным определить цифровые платформы как информационную инфраструктуру взаимодействия различных информационных систем для целей организации информационных отношений между пользователями цифровой платформы. Такое определение, безусловно, не отражает все технологические аспекты цифровых платформ, однако подчеркивает их основную отличительную черту.

Использование органами исполнительной власти частных цифровых платформ (например, для направления юридически значимых сообщений, а также для информирования граждан о своей деятельности) требует дополнительного регулирования в законодательстве, определяющего особенности отношений органа исполнительной власти как пользователя и платформы с учетом его публично-правового статуса.

Однако государство не только становится «пользователем» частных цифровых платформ, но также развивает свои цифровые платформы, что приводит к переходу к модели «государства как платформы», которая предполагает использование публично-правовой платформы для упрощения отношений между невластными субъектами. В этой связи возникает необходимость уточнения гражданского законодательства в части имущественной ответственности публично-правовых образований за технические ошибки государственной платформы (например, не было доставлено уведомление об отказе от договора электронным заказным письмом).

3.3. Правовой режим электронного обмена данными

В рамках цифровизации государственных и муниципальных услуг и перехода органов исполнительной власти на электронный документооборот повышается роль правового регулирования электронного обмена данными и

документами между различными органами исполнительной власти. Одним из преимуществ такого обмена является устранение необходимости дублированного сбора необходимой информации для предоставления соответствующей государственной услуги.

Электронный обмен данными осуществляется преимущественно на основании соглашений об информационном взаимодействии, заключаемых заинтересованным лицом с органом исполнительной власти – оператором соответствующей информационной системы. Однако заключение таких соглашений может быть либо обусловлено самостоятельным решением соответствующего органа исполнительной власти, либо обязательным для организации электронного взаимодействия в рамках единой информационной инфраструктуры.

В Российской Федерации для организации информационного обмена на основании статьи 7.1 Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ⁴²⁷ используется Единая система межведомственного электронного взаимодействия, оператором которой является Минцифры России⁴²⁸. Указанным органом также обслуживается инфраструктура, обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее - Инфраструктура взаимодействия)⁴²⁹, в рамках которой осуществляется обмен

⁴²⁷ Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета, № 168, 30.07.2010.

⁴²⁸ Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия») // Сборник законодательства РФ, 20.09.2010, № 38, ст. 4823.

⁴²⁹ Постановление Правительства РФ от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Положением об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и

между различными информационными системами участников предоставления государственных и муниципальных услуг, а также организаций, не участвующих в оказании таких услуг⁴³⁰. Несмотря на единое регулирование взаимодействия с инфраструктурой, для организаций, не участвующих в оказании государственных услуг, сохраняется обязанность заключать соглашения о взаимодействии с оператором инфраструктуры взаимодействия, определяющие правила использования доступа к подключенной информационной системе.

Соглашения о взаимодействии заключаются и для присоединения к иным государственным информационным системам. В частности, заключение соглашения о взаимодействии необходимо для технической поддержки витрин данных в Единой информационной платформе национальной системы управления данными⁴³¹.

Кроме того, соглашения о взаимодействии заключаются между органами исполнительной власти для межведомственного электронного взаимодействия при оказании государственных услуг. Заключение таких соглашений было предусмотрено в пункте 14 Положения о единой системе межведомственного электронного взаимодействия в редакции от 11.08.2016⁴³². В текущей редакции этот пункт исключен. Однако из документации, регламентирующей регистрацию

муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме») // Собрание законодательства РФ, 13.06.2011, № 24, ст. 3503.

⁴³⁰ Постановление Правительства РФ от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Правилами присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме») // Собрание законодательства РФ, 31.12.2012, № 53 (ч. 2), ст. 7938.

⁴³¹ Постановление Правительства РФ от 14.05.2021 № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства РФ", 24.05.2021, № 21, ст. 3585; Напр.: Соглашение о взаимодействии при обеспечении предоставления государственных услуг и исполнении государственных функций в электронном виде (Заключено в г. Москве 13.04.2011 № ИЩ-П13-8684) // СПС «КонсультантПлюс».

⁴³² СПС «КонсультантПлюс».

в Единой системе межведомственного взаимодействия, следует, что соглашения о взаимодействии заключаются после подачи заявления на присоединение к системе⁴³³.

Можно встретить и примеры условий взаимодействия в рамках оказания государственных услуг, сформулированных в виде договора присоединения⁴³⁴. Однако различное изменение форматов и способов заключения двусторонних актов для начала осуществления информационного взаимодействия и электронного обмена данными не изменяют необходимости заключения таких актов. В связи с этим можно полагать, что даже в случаях, когда орган исполнительной власти обязан осуществлять электронный обмен данными, присоединение к единой инфраструктуре осуществляется путем заключения двустороннего акта, который может быть обозначен как «соглашение об информационном взаимодействии».

Российский подход не исключает и возможности заключения между различными органами исполнительной власти отдельных соглашений об информационном обмене для реализации их полномочий в случаях, когда на органы не возложены обязанности по подключению к единой инфраструктуре взаимодействия⁴³⁵.

Обмен данными между агентствами США осуществляется только на основании отдельных соглашений между ними. Единая инфраструктура межведомственного обмена не формируется. В рекомендациях, подготовленных рабочей группой по обмену данными Главного совета по обмену данными США в 2022 году, одной из основных проблем организации информационного обмена обозначено отсутствие единых типовых форм соглашений об обмене данными.

⁴³³ Правила и процедуры работы в Единой системе межведомственного электронного взаимодействия по Методическим рекомендациям версии 3.XX. URL: https://info.gosuslugi.ru/docs/section/СМЭВ_3/ (дата обращения – 26.10.2023). С. 63.

⁴³⁴ Регламент обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде (версия 3.5) от 30.05.2013. URL: <https://smev.gosuslugi.ru/portal/> (дата обращения: либо -, либо :, унифицировать 28.05.2023).

⁴³⁵ Напр.: Соглашение об информационном обмене между Министерством промышленности и торговли Российской Федерации и Федеральной таможенной службой (Заключено в г. Москве, 26.08.2009 № 01–12/0026, № ХВ-9888/07) // СПС «КонсультантПлюс».

Подготовка и согласование соглашений между агентствами занимают месяцы и снижают возможности оперативного информационного обмена⁴³⁶.

Во Франции также распространен обмен данными между органами исполнительной власти на основании отдельных соглашений, однако присутствуют отдельные элементы централизованной инфраструктуры обмена данными. В большинстве случаев соглашения об информационном взаимодействии носят возмездный характер: в среднем в год от 900 до 1400 администраций приобретают данные у других органов исполнительной власти для реализации своих миссий⁴³⁷. Развитость системы возмездного обмена данными между различными органами исполнительной власти привела к централизованному развитию открытых данных, снижающих издержки по обмену данными между органами исполнительной власти различного уровня.

Общий правовой режим обмена данными между органами исполнительной власти во Франции установлен в статьях L114-8 – L114-10 Кодекса отношений между обществом и администрацией⁴³⁸ и нацелен на обмен необходимыми данными для оказания соответствующей государственной услуги. Положения Кодекса особо уделяют внимание обязанности органа информировать заявителя о документах, которые будут получены у других ведомств и необходимы для оказания соответствующей государственной услуги. Заявитель предоставляет самостоятельно необходимый документ только в случае, если он не может быть получен органом напрямую.

Однако аппарат Премьер-Министра Франции предоставляет должностным лицам органов исполнительной власти дополнительные централизованные сервисы коммуникации и обмена данными. В частности, для передачи данных

⁴³⁶ CDOC. Recommendations for improving the methods to access and share data within and between agencies. 2022. URL: https://resources.data.gov/resources/2021_DS WG%20Recommendations_and_Findings_508/ (дата обращения: 05.03.2023).

⁴³⁷ Pouillaude H.-B. L'échange des données publiques entre administrations // Le droit administratif au défi du numérique. AFDA. 2019. P. 31.

⁴³⁸ Code des relations entre le public et l'administration. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000031366350/LEGISCTA000031367410/ (дата обращения: 05.03.2023).

может использоваться сервис «France transfert»⁴³⁹, которые позволяет безопасно передавать данные в больших объемах. Кроме того, для взаимодействия по различным проектам может использоваться платформа «OSMOSE»⁴⁴⁰.

Стандартизация межведомственного электронного обмена осуществляется в соответствии с Общим руководством интероперабельности (RGI)⁴⁴¹, которое утверждается на основании статьи 11 Ордонанса Президента Французской республики № 2005-1516 от 08.12.2005 и устанавливает технические правила взаимодействия информационных систем, нормы и стандарты, используемые органами исполнительной власти⁴⁴².

Хотя в рассматриваемых странах (США, Россия, Франция) встречается упоминание соглашений об информационном взаимодействии, заключаемых органами исполнительной власти для передачи данных другим участникам информационных отношений, правовая природа таких соглашений не определена. Отсутствует и отдельное регулирование, конкретизирующее права и обязанности участников электронного обмена в таких соглашениях.

Одной из форм упрощения электронного обмена данными между различными органами исполнительной власти является развитие отдельных механизмов обеспечения открытости информации о деятельности органов исполнительной власти⁴⁴³. Открытость данных, принадлежащих органам исполнительной власти, позволяет также разрешить проблему повторного финансирования органами исполнительной власти технологий и организации сбора данных.

⁴³⁹ France transfert. URL: <https://www.numerique.gouv.fr/outils-agents/france-transfert/> (дата обращения: 05.03.2023).

⁴⁴⁰ Osmose, plateforme des communautés professionnelles de l'État. URL: <https://www.numerique.gouv.fr/outils-agents/osmose/> (дата обращения: 05.03.2023).

⁴⁴¹ Référentiel général d'interopérabilité (RGI). 12 janvier 2016 - mis à jour le 18 décembre 2020. URL: <https://www.numerique.gouv.fr/publications/interopabilite/> (дата обращения: 05.03.2023).

⁴⁴² Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/> (дата обращения: 05.03.2023).

⁴⁴³ Дамм И. А., Акунченко Е. А., Щедрин Н. В. Открытость публичной власти: вопросы понятийно-категориального аппарата // Вестник Санкт-Петербургского университета. Право. 2019. № 2. С. 226–242.

В Российской Федерации создание платформы открытого программного обеспечения, которое может использоваться в том числе разными органами исполнительной власти, началось с 2022 года⁴⁴⁴.

В США Административно-бюджетное управление, устанавливая общие принципы развития оборота данных в публичном секторе, отдельно уделило внимание необходимости развития обмена данными как внутри федеральных агентств, так и между федеральными агентствами и государственными органами нижестоящих уровней⁴⁴⁵. В части предотвращения повторного финансирования разработки программного обеспечения федеральные агентства США с 2016 года также обязаны размещать по открытым лицензиям не менее 20% разработанного исходного текста программного обеспечения⁴⁴⁶.

Хотя изначально правовой институт открытых данных сформировался в рамках «открытого правительства», открытые данные и в современный период цифровизации остаются значимым направлением развития электронного государства в разных странах⁴⁴⁷. Однако развиваются и иные способы обмена информацией. В частности, дискуссионным является вопрос о доступе государственных органов к обезличенным данным организаций в рамках Национальной системы управления данными⁴⁴⁸. Критика предложенного в

⁴⁴⁴ Постановление Правительства Российской Федерации от 10.10.2022 № 1804 «О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения». URL: <http://publication.pravo.gov.ru/Document/View/0001202210120022> (дата обращения: 05.03.2023).

⁴⁴⁵ OMB. Federal Data Strategy - A Framework for Consistency. June 4, 2019. URL: <https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf> (дата обращения: 05.03.2023).

⁴⁴⁶ OMB. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. August 8, 2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf (дата обращения: 05.03.2023).

⁴⁴⁷ UN E-Government Survey 2022. The Future of Digital Government: Trends, Insights and Conclusions. [Электронный ресурс]. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%205.pdf> (дата обращения: 05.03.2023).

⁴⁴⁸ Кинякина Е., Курашева А. Минцифры хочет разрешить бизнесу самостоятельно обезличивать данные. Ведомости. URL: <https://www.vedomosti.ru/technology/articles/2022/10/06/944301->

законопроекте решения свидетельствует о необходимости соблюдения баланса интересов органов исполнительной власти и организаций при организации электронного обмена данными, однако не исключает необходимость усовершенствования правового института предоставления информации о деятельности органов исполнительной власти.

Значимым барьером для развития оборота данных является сложившийся в России подход к регулированию предоставления информации о деятельности органов исполнительной власти, который исключает возможность взимания платы за дополнительную аналитическую работу органа исполнительной власти для передачи данных заинтересованному лицу.

Российский подход допускает предоставление данных органом исполнительной власти за плату для компенсации некоторых расходов на изготовление и пересылку экземпляров документов в большом объеме⁴⁴⁹. Правила определения такой платы установлены Правительством Российской Федерации на основании закона. Дополнительная аналитическая работа органа исполнительной власти исключается, что лишает заявителя возможности получить необходимый объем данных.

Закон об открытых данных США также возлагает на агентства обязанность публиковать наборы открытых данных на специальном портале и не регулирует особенности передачи открытых данных гражданам другими способами, хотя упоминает обязанность федеральных агентств принимать во внимание запросы граждан на размещение определенной информации в формате открытых данных в приоритетном порядке⁴⁵⁰. В соответствии с Законом о свободе информации в США от 1967 г. агентствам предоставлена возможность самостоятельно установить

[razreshit-biznesu-samostoyatelno-obezlichivat-dannie](#) (дата обращения: 05.03.2023). Дата публикации: 06.10.2022.

⁴⁴⁹ Постановление Правительства РФ от 24.10.2011 № 860 «Об утверждении Правил взимания платы за предоставление информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации от 2011 г., № 44, ст. 6273

⁴⁵⁰ Section 3506, (6), (B), Foundations for Evidence-Based Policymaking Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4174/text> (дата обращения: 05.03.2023).

правила взимания платы за предоставление запрашиваемых данных в отдельном нормативном акте⁴⁵¹ на основании общих правил, утверждаемых Административно-бюджетным управлением Исполнительного офиса Президента США.

Аналогичные положения можно найти и в европейском праве. Директива Европейского союза № 2019/1024 устанавливает приоритет предоставления открытых данных по запросу граждан безусловно и безвозмездно, однако не исключает возможность органа исполнительной власти передать открытые данные на определенных условиях (license), а равно на условиях исключительной лицензии. Кроме того, допускается взимание с граждан сборов за предоставление данных для покрытия маргинальных издержек по созданию органом исполнительной власти необходимого набора данных⁴⁵².

В Индии также созданы условия для надлежащего электронного обмена данными органов исполнительной власти. Национальная политика обмена и доступности данных, принятая Министерством науки и технологий Индии в 2012 году, предусматривает как размещение данных органов исполнительной власти общедоступным способом, так и обусловленные формы предоставления данных (регистрация, разрешение уполномоченного органа). В Индии не исключается также возможность платного предоставления данных органами исполнительной власти⁴⁵³.

Передача данных преимущественно на безвозмездной основе лишает орган исполнительной власти возможности выделить ресурсы для сбора необходимого набора данных и проведения дополнительной аналитической работы. Безусловно,

⁴⁵¹ The Freedom of Information Act, 5 U.S.C. § 552. URL: <https://www.justice.gov/oip/freedom-information-act-5-usc-552> (дата обращения: 05.03.2023).

⁴⁵² Article 6, paragraph 1: The re-use of documents shall be free of charge. However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024> (дата обращения: 05.03.2023).

⁴⁵³ India. National Data Sharing and Accessibility Policy. 2012. URL: <https://dst.gov.in/sites/default/files/gazetteNotificationNDSAP.pdf> (дата обращения: 05.03.2023).

возмездное предоставление данных органом исполнительной власти другим субъектам информационных отношений при этом должно быть ограничено публичными интересами и не может быть основной целью его деятельности. Однако сложившийся в российском праве подход исключает возможность взимания органом исполнительной власти платы для покрытия расходов на поиск и анализ запрашиваемой информации.

В связи с изложенным предлагается внести изменения в российское законодательство в части предоставления полномочий органам исполнительной власти по взиманию платы за дополнительную аналитическую работу для подготовки запрашиваемых документов, а также по ограничению условий использования предоставленных данных. Предлагаемые изменения изложены в приложении.

3.4. Государственная электронная идентификация

Организация электронного взаимодействия граждан и органов исполнительной власти осуществляется посредством осуществления органами исполнительной власти или уполномоченными организациями государственной электронной идентификации. Формирование системы государственной электронной идентификации тесно связано с развитием правового института удостоверения личности. Удостоверение личности осуществлялось органами исполнительной власти и ранее, однако было направлено на осуществление государственного контроля в сфере перемещений граждан⁴⁵⁴. Постепенно удостоверение личности приобретает также коммуникативную функцию, обеспечивающую подтверждение личности участников различных субъектов правоотношений⁴⁵⁵. В условиях цифровизации государственного управления значение коммуникативной функции возрастает.

⁴⁵⁴ Конькова А.Ю. Документирование удостоверения личности в дореволюционной России // Вестник РГГУ. 2016. № 2 (4). С. 18–26.

⁴⁵⁵ См.: Thomas Ph. A. Identity Cards // Modern Law Review. 1995. I. 58. № 5. P. 702–713.

Государство изначально формирует национальную систему идентификации для автоматизации процесса получения лицами государственных и муниципальных услуг. Затем по мере расширения государственной информационной инфраструктуры система национальной идентификации начинает использоваться также для удостоверения личности лица в отношениях с другими лицами, а государство выступает гарантом достоверности идентификации для определенных правоотношений.

Идентификация, осуществляемая в рамках электронного взаимодействия граждан с органами исполнительной власти, - более широкое понятие, чем удостоверение личности. В отличие от удостоверения личности идентификация может быть менее надежной в зависимости от отношений, в которых она используется. Даже оставаясь в определенной степени неопознанным, гражданин идентифицируется в сети Интернет по файлам cookie, электронной почте⁴⁵⁶. Также и сам факт использования лицом государственного электронного идентификатора позволит определить лицо в системе учета соответствующего органа исполнительной власти, однако непосредственное удостоверение его личности осуществляется путем сверки биологических и физиологических данных, как непосредственно, так и при помощи информационных технологий.

В Российской Федерации постановлением Правительства Российской Федерации от 28 ноября 2011 г. N 977 введена в действие Единая система идентификации и аутентификации (ЕСИА), которая позволяет обеспечить централизованное подтверждение личности пользователя при взаимодействии в различных государственных информационных системах⁴⁵⁷.

⁴⁵⁶ См.: Camp J.L. Economics of Identity Theft: Avoidance, Causes and Possible Cures // Springer Science+Business Media, LLC, 2007.

⁴⁵⁷ Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с Требованиями к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и

Основной особенностью использования ЕСИА является возможность обращаться за государственными и муниципальными услугами онлайн с помощью простой электронной подписи⁴⁵⁸. Однако в настоящий момент наблюдается тенденция к расширению функционала ЕСИА и для совершения иных юридически значимых действий при взаимодействии с юридическими лицами частного сектора. Например, для получения кредитной истории онлайн субъект кредитной истории вправе использовать ЕСИА для собственной идентификации⁴⁵⁹ и подписать заявление о получении кредитной истории простой электронной подписью.

Кроме того, в Российской Федерации получила реализацию система национальной биометрической идентификации, осуществляемой преимущественно кредитными организациями. В соответствии с частью 27 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ⁴⁶⁰, введенной в действие Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 № 479-ФЗ⁴⁶¹, осуществление биометрической идентификации официально приравнивалось к предъявлению документа, удостоверяющего личность гражданина. Позже эта норма была перенесена в отдельный закон о Единой биометрической системе идентификации⁴⁶².

муниципальных услуг в электронной форме) // Собрание законодательства РФ, 05.12.2011, № 49 (ч. 5), ст. 7284.

⁴⁵⁸ Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (вместе с Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг) // Собрание законодательства РФ, 04.02.2013, № 5, ст. 377.

⁴⁵⁹ Часть 7.2 статьи 6 Федерального закона «О кредитных историях» от 30.12.2004 № 218-ФЗ // Российская газета, № 2, 13.01.2005.

⁴⁶⁰ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

⁴⁶¹ Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 № 479-ФЗ // Российская газета, № 1, 11.01.2021.

⁴⁶² Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании

Таким образом, российский подход к системе электронной идентификации и удостоверения личности осуществляется централизованно в рамках создания государством единой инфраструктуры обмена необходимыми идентификационными данными, однако не привязан к документам, удостоверяющим личность.

Европейский подход к формированию системы электронной идентификации основан на переходе к новым форматам документов удостоверения личности: от бумажных документов к картам с цифровым чипом. При этом сохраняется один документ, который может быть использован для удостоверения личности гражданина в различных отношениях. Некоторые из европейских стран (например, Австрия) используют такие документы для идентификации гражданина при получении им государственных услуг⁴⁶³.

Другие страны столкнулись с правовыми проблемами при переходе к использованию пластиковых карт для идентификации граждан в цифровой среде, поэтому были вынуждены заимствовать более гибкий подход стран общего права к электронной идентификации гражданина. В частности, часть положений, позволяющих осуществлять электронную идентификацию гражданина с использованием его пластиковой карты, во Франции были на законодательном

утратившими силу отдельных положений законодательных актов Российской Федерации» // Российская газета, № 1, 09.01.2023.

⁴⁶³ Регламент ЕС 2019/1157 установил единые требования к картам идентичности, предусмотрев обязательное включение в них сведений об отпечатках пальцев и биометрических данных изображения лица. При этом Регламент не затрагивает возможности использования карт идентичности для целей использования гражданами услуг электронного правительства, что остается на усмотрение стран-участников ЕС. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. URL: <http://data.europa.eu/eli/reg/2019/1157/oj> (дата обращения: 05.03.2023).

уровне предложены еще в 2012 году⁴⁶⁴, однако были признаны неконституционными⁴⁶⁵.

Франция сформировала более гибкий подход к идентификации лица для целей получения государственных услуг, основанный на возможности использования сторонних сервисов. Однако введение нового формата пластиковых карт удостоверения личности⁴⁶⁶ позволило использовать карты нового формата для подключения к порталу государственных услуг⁴⁶⁷.

В странах общего права изначально используется децентрализованный подход, предполагающий возможность существования нескольких документов удостоверения личности. При переходе к более централизованному контролю за документами удостоверения личности страны сталкиваются с сопротивлением со стороны гражданского общества.

Например, в Великобритании создание единой системы документов удостоверения личности было встречено негативно⁴⁶⁸. Как в правовой литературе⁴⁶⁹, так и в социологических опросах отмечалось, что чем более граждане чувствуют принуждение к получению единых карт идентичности, тем

⁴⁶⁴ Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF n°0075 du 28 mars 2012 page 5604, texte n° 2. URL: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=20170503> (дата обращения: 05.03.2023).

⁴⁶⁵ Le Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012 // ORF n°0075 du 28 mars 2012 page 5607, texte n° 6. URL: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582452> (дата обращения: 05.03.2023).

⁴⁶⁶ Décret n° 2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés » (TES) URL: <https://www.legifrance.gouv.fr/eli/decret/2021/3/13/INTD2104790D/jo/texte> (дата обращения: 05.03.2023).

⁴⁶⁷ См. ответы на частые вопросы на официальной странице описания сервиса «service public d'identité numérique». URL: <https://france-identite.gouv.fr/questions-frequentes/> (дата обращения: 05.03.2023).

⁴⁶⁸ Thomas Ph. A. Identity Cards // *Modern Law Review*. 1995. I. 58. № 5. P. 702 – 713; Perri 6 Should We Be Compelled to Have Identity Cards? Justifications for the Legal Enforcement of Obligations // *Political Studies*. 2005. № 53. P. 243–261.

⁴⁶⁹ Sullivan C. The United Kingdom Identity Cards Act 2006 – Civil or Criminal? // *International Journal of Law and Information Technology*. 2006. № 3 (15). P. 320–361.

более они были обеспокоены неприкосновенностью частной жизни⁴⁷⁰. В настоящий момент в Великобритании предусмотрены разные виды документов, удостоверяющих личность гражданина⁴⁷¹. Однако предъявление таких документов не является обязательным в частных отношениях между гражданами. Например, карты для подтверждения совершеннолетия выдаются некоммерческой организацией⁴⁷².

В США также действует децентрализованный подход к документам удостоверения личности и сервисам электронных государственных услуг. Однако если в Великобритании предусматриваются различные способы идентификации и участие гражданского общества, децентрализованный подход США основан на разграничении компетенции штатов и федерации.

Каждый из штатов самостоятельно определял форматы выдачи документов, удостоверяющих личность граждан. Однако террористические акты 11 сентября 2001г. изменили этот подход: Конгрессом США был принят Закон «Real ID»⁴⁷³, установивший единые требования и стандарты к содержанию водительских лицензий. Требования вызвали критическую оценку во многих штатах, выпустивших законодательство против указанного акта⁴⁷⁴. Не остались в стороне

⁴⁷⁰ Joinson A.N., Paine C., Buchanan T., Reips U. Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom // Journal of Information Science. 2006. № 32 (4). P. 334–343.

⁴⁷¹ Identity Documents Act 2010. URL: http://www.legislation.gov.uk/ukpga/2010/40/pdfs/ukpga_20100040_en.pdf (дата обращения: 05.03.2023).

⁴⁷² Citizencard. URL: <https://www.citizencard.com/about-us> (дата обращения: 05.03.2023).

⁴⁷³ USA, REAL ID Act of 2005. URL: <https://www.congress.gov/bill/109th-congress/house-bill/418/text> (дата обращения: 05.03.2023).

⁴⁷⁴ Electronic Privacy Information Center. Real ID Implementation Review: Few Benefits, Staggering Costs. Analysis Of The Department Of Homeland Security's National ID Program. May, 2008. URL: https://epic.org/privacy/id_cards/epic_realid_0508.pdf (дата обращения: 05.03.2023); Testimony of Legislative Counsel Katie Corrigan on the Establishment of a National ID Card System Before The House Government Reform Subcommittee on Government Efficiency, Financial Management And Intergovernmental Relations. November 16, 2001. URL: <https://www.aclu.org/other/testimony-legislative-counsel-katie-corrigan-establishment-national-id-card-system-house?redirect=technology-and-liberty/testimony-legislative-counsel-katie-corrigan-establishment-national-id-card-s> (дата обращения: 05.03.2023); Speech by Barry Steinhardt concerning the use of uniform driver's licenses as a national ID, February 10, 2002. URL: <https://www.aclu.org/other/speech-barry-steinhardt-concerning-use-uniform-drivers-licenses-national-id?redirect=technology-and-liberty/speech-barry-steinhardt-concerning-use-uniform-drivers-licenses-national-id> (дата обращения: 05.03.2023);

и некоторые исследователи, отмечающие потенциальную опасность социальной дискриминации на основе реализации системы национальной идентификации⁴⁷⁵. Принятый в 2005 г., Закон «Real ID» так и не был реализован⁴⁷⁶.

Таким образом, развитие системы государственной электронной идентификации обусловлено сложившимся в стране подходом к удостоверению личности. Удостоверение личности предшествует формированию государственных электронных идентификаторов.

В.Б. Наумов определяет идентификацию как «информационный процесс, направленный на установление субъектного и (или) объектного состава общественных отношений на основе идентификатора или их совокупности в соответствии с содержанием отношений и их правовой природой, определяемых социально-экономическими, правовыми и технологическими условиями их развития в информационном обществе в ходе его цифровой трансформации»⁴⁷⁷.

Идентификация, осуществляемая органами исполнительной власти, обладает рядом дополнительных характеристик.

Во-первых, идентификация органом исполнительной власти всегда представляет собой правовой режим, в рамках которого законодательством установлены обязанности должностных лиц по достоверному определению или созданию идентификатора, относимого к отдельному лицу. При этом не всякая идентификация в целом может считаться правовым режимом, поскольку при

Coalition letter to President Bush urging him to reject National ID Card, February 11, 2002. URL: <https://www.aclu.org/legal-document/coalition-letter-president-bush-urging-him-reject-national-id-card?redirect=technology-and-liberty/coalition-letter-president-bush-urging-him-reject-national-id-card> (дата обращения: 05.03.2023).

⁴⁷⁵ Lyon D. National ID Cards: Crime-Control, Citizenship and Social Sorting // Policing. January 2007. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.605.4170&rep=rep1&type=pdf> (дата обращения: 05.03.2023).

⁴⁷⁶ USA, Department of Homeland Security. 6 CFR Part 37, RIN 1601-AA97. Effective on April 27, 2020. URL: <https://www.govinfo.gov/content/pkg/FR-2020-04-27/pdf/2020-08481.pdf> (дата обращения: 05.03.2023); DHS Announces Extension of REAL ID Full Enforcement Deadline. Release Date: April 27, 2021. URL: <https://www.dhs.gov/real-id/news/2021/04/27/dhs-announces-extension-real-id-full-enforcement-deadline> (дата обращения: 05.03.2023).

⁴⁷⁷ Наумов В.Б. Институт идентификации в информационном праве: автореф. дис. ... д.ю.н. Москва. 2020. С. 11.

регистрации в Интернет-сервисах соответствующей обязанности по подтверждению достоверности личности пользователя может не быть.

Отсюда следует вторая особенность идентификации, осуществляемой органами исполнительной власти – орган исполнительной власти не вправе самостоятельно создавать дополнительные идентификаторы, имеющие юридическое значение, если такое полномочие не предоставлено им законодательством. Действующее законодательство предусматривает разные виды идентификаторов, создаваемых органами исполнительной власти в рамках различной компетенции. Например, Федеральная налоговая служба Российской Федерации на основании части 7 статьи 84 Налогового кодекса Российской Федерации⁴⁷⁸ присваивает каждому налогоплательщику индивидуальный номер налогоплательщика (ИНН), который налогоплательщик обязан использовать при взаимодействии с налоговым органом. Особенности выдачи ИНН определены приказом ФНС России от 29.06.2012 № ММВ-7-6/435@⁴⁷⁹. Аналогично, территориальный орган Пенсионного фонда Российской Федерации при постановке физического лица на учет присваивает ему страховой номер индивидуального лицевого счета (СНИЛС)⁴⁸⁰. В качестве идентификаторов могут выступать и реквизиты документов удостоверения личности, а также ФИО, дата рождения.

В-третьих, идентификация, осуществляемая органом исполнительной власти многофакторна, включает в себя не только определение лица по его

⁴⁷⁸ Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // Российская газета, № 148-149, 06.08.1998.

⁴⁷⁹ Приказ ФНС России от 29.06.2012 № ММВ-7-6/435@ «Об утверждении Порядка и условий присвоения, применения, а также изменения идентификационного номера налогоплательщика» (Зарегистрировано в Минюсте России 14.08.2012 № 25183) // Российская газета, № 192, 22.08.2012.

⁴⁸⁰ Пункт 13 Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах, утвержденной Приказом Минтруда России от 22.04.2020 № 211н «Об утверждении Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах» (Зарегистрировано в Минюсте России 15.07.2020 № 58956). URL: <http://publication.pravo.gov.ru/Document/View/0001202007160003> (дата обращения: 05.03.2023).

идентификатору, но также сопоставление идентификатора с иными сведениями о лице с привлечением доверенной третьей стороны.

В частности, дополнительное подтверждение личности для присвоения идентификатора в Российской Федерации требуется при регистрации на портале Госуслуг. Удостоверение личности гражданина при регистрации осуществляется либо посредством использования усиленной квалифицированной электронной подписи, либо посредством введения кода активации, полученного при посещении уполномоченных центров регистрации⁴⁸¹. В указанных случаях подтверждение соответствия идентификатора гражданину осуществляет либо аккредитованный удостоверяющий центр, выдавший ему усиленную квалифицированную электронную подпись, либо иная организация, имеющая статус центра регистрации.

Схожий подход к идентификации используется и в других странах. Во Франции введенный в 2018 г. сервис FranceConnect⁴⁸², используемый как единая платформа для получения государственных услуг, позволяет пользователю идентифицироваться с помощью нескольких разных сторонних сервисов⁴⁸³ – например, идентификационного сервиса почты или налоговой. В Великобритании для использования платформы получения государственных услуг в электронном виде сервис GOV.UK VERIFY указывает, что у гражданина должен быть паспорт или водительское удостоверение, однако подтверждение его личности осуществляется отдельными организациями онлайн, которые вправе также

⁴⁸¹ Подпункт з) пункта 6.1 Положения о федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме (утв. Приказом Минкомсвязи России от 13.04.2012 № 107) (Зарегистрировано в Минюсте России 26.04.2012 № 23952) // Российская газета, № 112, 18.05.2012.

⁴⁸² Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'Etat. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037611479/> (дата обращения: 05.03.2023).

⁴⁸³ Assemblée nationale. Rapport d'information sur l'identité numérique. 08.07.2020. URL: https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/115b3190_rapport-information#_Toc256000062 (дата обращения: 05.03.2023).

запрашивать сведения о гражданине в банках и других организациях, чтобы подтвердить сведения о нем⁴⁸⁴.

Однако переход к электронной идентификации в рамках платформенного подхода ставит вопрос не только об особенностях осуществления электронной идентификации органами исполнительной власти, но также и о правах граждан в отношении сведений, в совокупности составляющих их цифровой профиль.

Результатом идентификации является создание учетной единицы в государственной информационной системе, в которой помимо идентификаторов хранится и иная информация, относящаяся к гражданину. В правовой литературе предлагались разные термины для обозначения такой учетной единицы: «информационный портрет личности»⁴⁸⁵, «цифровой профиль»⁴⁸⁶, «виртуальное лицо»⁴⁸⁷, «цифровая идентичность»⁴⁸⁸.

В подзаконных актах и стратегических документах в настоящий момент более распространен термин «цифровой профиль»⁴⁸⁹. Цифровой профиль, согласно Концепции и архитектуры цифрового профиля – ЕСИА 2.0, понимается как «совокупность цифровых записей о гражданине, содержащихся в

⁴⁸⁴ Описание сервиса GOV.UK VERIFY на официальном сайте. URL: <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify> (дата обращения: 05.03.2023).

⁴⁸⁵ Бондарь Н.С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25–42.

⁴⁸⁶ См.: Виноградова Е.В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е.В. Виноградова, Т.А. Полякова, А.В. Минбалеев // Правоприменение. 2021. Т. 5. № 4. С. 5–19; Жарова А. К. Правовое обеспечение цифрового профилирования деятельности человека // Вестник ЮУрГУ. Серия «Право». 2020. Т. 20. № 2. С. 80–87; Мочалов А.Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica (Русский закон). 2021. № 9. С. 88–101.

⁴⁸⁷ Андрущенко Е.С. Проблема идентификации субъектов Интернет-отношений. Виртуальное лицо // Информационное общество: проблемы развития законодательства. Сборник научных работ. М.: ИГП РАН, ЮРКОМПАНИ, 2012. С. 79–86.

⁴⁸⁸ Туликов А.В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): дис. ... к.ю.н. Москва. 2017. 180 с.

⁴⁸⁹ Постановление Правительства РФ от 3 июня 2019 г. № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (вместе с Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах) // Собрание законодательства РФ, 10.06.2019, № 23, ст. 2963.

информационных системах государственных органов и организаций»⁴⁹⁰. Цифровой профиль представляет собой простую совокупность всех сведений и подвластном субъекте в государственных информационных системах, включая сведения о согласиях такого лица на обработку его данных.

Цифровой профиль играет ключевую роль во взаимодействии органов исполнительной власти и граждан в рамках развития государственных цифровых платформ. В рамках использования государственной цифровой платформы гражданин получает право подтверждать достоверность своих данных на информационных ресурсах третьих лиц с использованием функционала своего цифрового профиля. Например, гражданин вправе для получения кредитной истории онлайн использовать ЕСИА для собственной идентификации⁴⁹¹ в информационной системе бюро кредитных историй.

Право гражданина использовать учетную запись в государственных информационных системах⁴⁹² для подтверждения информации о себе на сторонних ресурсах можно обозначить как право на цифровую идентичность. Если цифровой профиль как термин характеризует совокупность сведений о гражданине в его учетной записи, то цифровая идентичность обозначает идентификаторы учетной записи гражданина, подтверждающие его личность в информационных отношениях как с органами исполнительной власти, так и с другими их участниками⁴⁹³.

⁴⁹⁰ Разработаны в рамках Плана мероприятий по направлению «Информационная инфраструктура» Программы «Цифровая экономика Российской Федерации».

⁴⁹¹ Часть 7.2 статьи 6 Федерального закона «О кредитных историях» от 30.12.2004 № 218-ФЗ // Российская газета, № 2, 13.01.2005.

⁴⁹² Право на цифровую идентичность тесно связано с правовым институтом удостоверения личности и может реализовываться преимущественно в рамках использования учетной записи государственной информационной системы, позволяющей достоверно подтвердить идентификационные данные пользователя. Вместе с тем, не исключен и более широкий подход к пониманию рассматриваемого права, включающий возможность подтверждения данных пользователя с использованием учетной записи негосударственной информационной системы. Однако данный подход не относится к предмету диссертационного исследования, поскольку не характеризует правовой статус органа исполнительной власти в информационной сфере.

⁴⁹³ Правовая идентичность подробно исследована Н.В. Исаевой, определяющей правовую идентичность как «качество субъекта права, характеризующее его актуальное состояние посредством юридического самоопределения в категориях прав, свобод, обязанностей и ответственности, воспринимаемых как правовые ценности, обеспечивающие положительные

Хотя право на цифровую идентичность напрямую не закреплено в законе, на основе действующих положений законодательства можно утверждать, что указанное право в Российской Федерации сформировалось. Оно следует, в частности, из статьи 19 Гражданского кодекса Российской Федерации⁴⁹⁴, согласно которой гражданин приобретает свои гражданские права и обязанности под своим именем. В публично-правовых отношениях право лица на его цифровую идентичность следует из возможности использования государственных цифровых платформ для целей получения государственных и муниципальных услуг либо взаимодействия с иными пользователями платформы⁴⁹⁵. Использование чужой цифровой идентичности может быть также квалифицировано в качестве преступления на основании статьи 272 Уголовного кодекса Российской Федерации⁴⁹⁶, криминализующей неправомерный доступ к компьютерной информации, а также на основании иных статей уголовного законодательства в зависимости от обстоятельств совершенного преступного деяния.

Право на цифровую идентичность – информационное право, которое непосредственно следует из развития государственных и частных цифровых платформ и является основой реализации конституционных прав граждан с помощью цифровых технологий, получившей название «цифрового гражданства» в российской литературе⁴⁹⁷. Аналогичный подход можно встретить во Франции. В докладе Национального совета по цифровизации от июня 2020 года, посвященном цифровым идентичностям и цифровому гражданству, справедливо отмечается о

правовое сознание и правовую активность». Цифровая идентичность, следуя предложенному автором определению, является одним из средств юридического самоопределения личности для вступления в правовые отношения. См.: Исаева Н.В. Правовая идентичность (теоретико-правовое исследование): дис. ... докт. юрид. наук. М., 2014. С. 22.

⁴⁹⁴ Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Российская газета, № 238-239, 08.12.1994.

⁴⁹⁵ Часть 11 статьи 7 Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета, № 168, 30.07.2010.

⁴⁹⁶ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

⁴⁹⁷ Дмитрик Н.А. Корпорации в своем праве // Закон. 2021. № 12. С. 103 – 114; Кравец И.А. Цифровое гражданство и конституционные вызовы в информационном и алгоритмическом обществе // Сравнительное конституционное обозрение. 2023. N 2. С. 93 - 123.

способности цифровых идентичностей обеспечить гражданину необходимые инструменты для взаимодействия с государством и обществом в информационной сфере⁴⁹⁸. Представляется, на начальных этапах институционализации права на цифровую идентичность оно может быть закреплено в Федеральном законе «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ, поскольку предоставление возможности передачи данных из государственных информационных систем можно рассматривать как отдельный вид электронной государственной услуги.

Одновременно, результаты проведенного в настоящем параграфе сравнения подходов к удостоверению личности показывают, что понятие «цифрового гражданства» и право на цифровую идентичность, предполагающее увеличение сбора данных органами исполнительной власти о гражданах, могут восприниматься и как противоречащие конституционным правам и свободам. В связи с чем в США под «цифровым гражданством» в большей степени понимается формирование навыков обучающихся по безопасному использованию цифровых технологий⁴⁹⁹, а право на цифровую идентичность в понимании, предложенном в настоящем исследовании, не получает развития в связи с децентрализованным подходом США к регулированию системы удостоверения личности.

⁴⁹⁸ Rapport du Conseil national du numérique. Identités numériques. Clés de voûte de la citoyenneté numérique. Juin 2020. URL: <https://cnnumerique.fr/files/uploads/2020/2020.06.19.ra-cnum-idnum-web3.pdf> (дата обращения: 25.10.2023).

⁴⁹⁹ What is digital citizenship? URL: <https://www.cyberwise.org/digital-citizenship#:~:text=Digital%20Citizenship%2C%20which%20is%20%22the,favor%20of%20positive%20online%20interactions.&text=Our%20mission%20is%20to%20help,and%20wise%20users%20of%20technology> (дата обращения: 25.10.2023).

ЗАКЛЮЧЕНИЕ

Правовой статус – широкое понятие в юридической литературе, которое можно раскрывать различными способами. Составляющими правового статуса являются и компетенция, и ответственность органа, и задачи, которые стоят перед ним в рамках участия в регулировании информационной сферы. Правовой статус органа исполнительной власти в информационной сфере – характеристика юридических особенностей его деятельности, порядка и целей формирования, взаимоотношений с другими органами государства.

Система органов публичной власти перестраивается для регулирования информационной сферы. Для целей обеспечения эффективности государственного управления информационной сферой усиливается централизация системы.

В аппарате правительства и главы государства возникают новые структурные единицы, призванные координировать развитие электронного правительства. В странах со смешанной формой правления (Россия, Франция) полномочия главы государства и правительства нуждаются в дополнительном разграничении. Если глава государства определяет общие направления развития политики государства в целом, правительство реализует установленные направления, осуществляя оперативную координацию электронного правительства. В некоторых парламентских республиках (Индия) координационные полномочия передаются профильному министерству.

Изменения происходят и на уровне министерств. Ряд стран следует по пути укрепления полномочий существующих министерств, деятельность которых связана с информационной сферой (Франция, США). В азиатских странах (Сингапур, Индия, Китай) и России, наоборот, учреждаются специальные профильные министерства для регулирования информационной сферы, что усиливает централизацию системы органов исполнительной власти.

Франция и США – страны с более длительной историей развития административного аппарата, столкнувшиеся с проблемой его излишней бюрократизации. В результате в указанных странах были учреждены независимые

коллегиальные органы, способные учитывать интересы бизнеса (США) либо, наоборот, более независимо защищать права граждан, воздействуя на другие органы исполнительной власти (Франция). Указанные независимые органы играют значительную роль в регулировании отдельных областей информационной сферы – в первую очередь, персональных данных.

Необходимость развития информационных технологий в отдельных регионах и на уровне местного самоуправления приводит к созданию центральными органами исполнительной власти различных мер поддержки цифровизации на нижестоящих уровнях (Россия, Франция). Некоторые страны предоставляют органам местного самоуправления возможность самостоятельного объединения для развития цифровизации (США), в то время как другие страны, устанавливая единое направление развития электронного правительства, сталкиваются с необходимостью выстроить систему взаимодействия различных органов нижестоящего уровня (Германия).

Хотя на отдельных уровнях исполнительной власти наблюдается территориальная или функциональная децентрализация, общая тенденция перестройки аппарата исполнительной власти характеризуется усилением централизации, что связано с необходимостью организации более оперативного и эффективного управления информационной сферой. Особенно заметна эта тенденция в сфере информационной безопасности.

Централизация системы органов исполнительной власти для регулирования информационной сферы сопровождается усилением государственного регулирования информационной сферы в целом, что отражается на полномочиях органов исполнительной власти в информационной сфере.

Подзаконное нормотворчество и правоприменительная деятельность органов исполнительной власти начинают играть ключевую роль в регулировании информационной сферы. В отдельных странах законодатель склонен делегировать органам исполнительной власти нормотворчество в части определения процедурных аспектов регулирования информационной сферы (Россия, Франция). Преимущественно такое регулирование осуществляется правительством. Глава

государства в рассматриваемых странах может либо принимать «замещающее» законодательство в информационной сфере на период до принятия соответствующего закона парламентом (Франция), либо определять направления развития политики государства, конкретизируемые в законах и подзаконных актах на нижестоящем уровне (Россия). На примере сферы защиты персональных данных видно, что правоприменительная практика органов исполнительной власти зачастую определяет регулирование в указанном направлении, опережая суды (Россия, Франция, США). В связи с этим усиливается роль актов административного толкования – рекомендаций, разъяснений органов исполнительной власти.

Возрастание значения государственного суверенитета в информационной сфере приводит и к развитию главами государств системы информационной безопасности органов исполнительной власти в следующих направлениях: стандартизация в сфере информационной безопасности; обособление отдельных штатных единиц в структуре органа исполнительной власти для обеспечения информационной безопасности; формирование единой системы обмена сведениями об инцидентах кибербезопасности. Дополнительно в некоторых сравниваемых странах развиваются новые меры административного принуждения в информационной сфере (Франция, Россия).

Изменяется компетенция органов исполнительной власти в связи с переходом оказания государственных услуг в электронный формат, что приводит к появлению новых возможностей анализа пользовательских данных граждан – получателей государственных услуг. Сам электронный формат оказания государственных услуг влияет на реализацию других прав граждан. Судебные издержки рассмотрения споров, однако, не позволяют гражданам оперативно воздействовать на исполнительную власть для устранения нарушений. В связи с этим стоит отметить роль омбудсменов в контроле за деятельностью органов исполнительной власти в электронной форме (Франция, Россия, Швеция), что позволяет преодолеть бюрократические сложности рассмотрения обращений и жалоб граждан в административном порядке и избежать судебной процедуры.

Внедрение информационных технологий в деятельность самих органов исполнительной власти, получившее обозначение «электронное правительство», также влияет на правовой статус органов исполнительной власти, уточняя полномочия органов исполнительной власти по использованию информационных технологий в своей деятельности.

Развитие электронного правительства предполагает поиск нового подхода к регулированию деятельности органов исполнительной власти. В зарубежных странах, развитые правовые институты которых заимствуются и в других юрисдикциях, сложились разные подходы к законодательному регулированию электронного правительства. В странах с развитой традицией административного права (Франция, Швеция) регулирование электронного правительства осуществляется в рамках общего регулирования деятельности органов исполнительной власти. Другие страны, наоборот, принимали специальное законодательство для оперативного разрешения вопросов развития электронного правительства (Германия, США, Италия). Российская Федерация развивает регулирование электронного правительства в рамках более общих законов, регулирующих деятельность органов исполнительной власти.

Правовое регулирование электронного правительства имеет ряд общих характеристик в сравниваемых странах. В частности, развитие электронного документооборота и электронного обмена данными органов исполнительной власти осуществляется на основании отдельных соглашений об информационном взаимодействии. Однако заключение таких соглашений может быть либо обусловлено необходимостью информационного обмена в рамках единой инфраструктуры, либо осуществляется для информационного обмена по усмотрению соответствующего органа исполнительной власти.

Развитие электронного обмена данными органов исполнительной власти тесно связано с правом на доступ к информации о деятельности органов исполнительной власти. Создание условий для свободного информационного обмена осуществляется в том числе путем предоставления органам исполнительной власти возможности обмениваться данными на возмездной

основе с целью компенсации части издержек по сбору данных (дополнительному анализу).

Общим для развития электронного правительства в России и зарубежных странах является и формирование системы государственной электронной идентификации. Электронная идентификация – существенное условие перехода к электронному взаимодействию органов исполнительной власти и подвластных субъектов. Развивающаяся система государственной электронной идентификации связана с подходом к организации системы удостоверения личности в стране и может предоставлять гражданам больше выбора в способах удостоверения личности (страны общего права) либо организовываться с учетом единого подхода к удостоверению личности.

Система государственной электронной идентификации может использоваться также и для подтверждения личности участников невластных информационных отношений. Право гражданина требовать от органов исполнительной власти предоставления достоверной информации о нем невластными субъектам в таком случае приобретает самостоятельный характер (право на цифровую идентичность), хотя ограничено пределами взаимодействия органа исполнительной власти и соответствующего частного субъекта.

Возможности электронного правительства получают усиление в связи с возрастанием роли частных и государственных цифровых платформ в организации общественных отношений. Выстраиваемые на основе цифровых платформ сетевые связи в системе государственного управления приводят к сочетанию частного и публичного методов правового регулирования деятельности органов исполнительной власти в информационной сфере.

Обозначенные характеристики деятельности органов исполнительной власти в информационной сфере свидетельствуют о развитии и укреплении правового статуса органов исполнительной власти в различных странах в трех направлениях: структурно-функциональном, учитывающем особенности формирования системы органов исполнительной власти; в части развития полномочий органов исполнительной власти в информационной сфере;

управленческом, связанном с характером деятельности органов исполнительной власти (электронное правительство). Однако постановка исследовательской проблемы позволяет только обще охарактеризовать происходящие изменения. В этой связи сохраняется перспективность более детальных исследований государственного управления в отдельных областях информационной сферы: в сфере связи, рекламы, защиты прав потребителя, информационной безопасности, государственных закупок и финансов (цифровые национальные валюты).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Конституции

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: <http://publication.pravo.gov.ru/Document/View/0001202007040001> (дата обращения: 05.03.2023).
2. The Constitution of Greece. As revised by the parliamentary resolution of May 27th, 2008, of the VIIIth Revisionary Parliament. URL: <https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dceба27c8/001-156%20aggliko.pdf> (дата обращения: 05.03.2023).
3. Constitution du 4 octobre 1958. URL: <https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095822> (дата обращения: 05.03.2023).
4. USA Constitution. URL: <https://www.archives.gov/founding-docs/constitution-transcript> (дата обращения: 05.03.2023).

Законы

5. Федеральный конституционный закон от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» // Собрание законодательства РФ, 09.11.2020, № 45, ст. 7061.
6. Федеральный конституционный закон от 26.02.1997 № 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации» // Российская газета, № 43-44, 04.03.1997.
7. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Российская газета, № 238-239, 08.12.1994.
8. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 1.
9. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // Российская газета, № 148-149, 06.08.1998.
10. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Российская газета, № 249, 22.12.2001.
11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954.
12. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 № 479-ФЗ // Российская газета, № 1, 11.01.2021.
13. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ. URL:

- <http://publication.pravo.gov.ru/Document/View/0001201407220042> (дата обращения: 16.05.2023).
14. Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» от 24.11.2014 № 364-ФЗ. URL: <http://publication.pravo.gov.ru/Document/View/0001201411250005?index=12&rangeSize=1> (дата обращения: 16.05.2023).
 15. Федеральный закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием» от 14.07.2022 № 255-ФЗ // Российская газета, № 154-155, 19.07.2022.
 16. Федеральный закон «О кредитных историях» от 30.12.2004 № 218-ФЗ // Российская газета, № 2, 13.01.2005.
 17. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
 18. Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета, № 168, 30.07.2010.
 19. Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» // Собрание законодательства Российской Федерации от 2021 г., № 27, ст. 5064. (Часть первая).
 20. Федеральный закон от 07.05.2013 № 78-ФЗ «Об уполномоченных по защите прав предпринимателей в Российской Федерации» // Собрание законодательства Российской Федерации от 2013 г., № 19, ст. 2305.
 21. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Российская газета, № 135, 10.07.2003.
 22. Федеральный закон от 15.02.2016 № 18-ФЗ «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации и Кодекс административного судопроизводства Российской Федерации в части установления порядка судебного рассмотрения дел об оспаривании отдельных актов» // Российская газета, № 33, 17.02.2016.
 23. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4736.
 24. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Российская газета, № 1, 09.01.2023.

25. Федеральный закон от 30.12.2020 № 509-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета, № 2, 12.01.2021.
26. Закон Москвы от 24.10.2001 № 52 «Об информационных ресурсах и информатизации города Москвы». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&vkart=card&nd=120029610&rdk=&backlink=1> (дата обращения: 05.03.2023);
27. Закон Республики Татарстан от 13 ноября 2007 г. № 58-ЗРТ «Об информационных системах и информатизации Республики Татарстан». URL: <https://digital.tatarstan.ru/zakon-rt-ob-informatsionnih-sistemah-i.htm> (дата обращения: 05.03.2023).
28. Code de la consommation. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033219601/ (дата обращения: 05.03.2023).
29. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029759791/ (дата обращения: 06.03.2023).
30. Code des relations entre le public et l'administration. URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=91C91B1A73A68E15149FA32687E64163.tplgfr34s_2?idSectionTA=LEGISCTA000031367685&cidTexte=LEGITEXT000031366350&dateTexte=20190210 (дата обращения: 05.03.2023).
31. Code pénal. URL: <https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006165313/> (дата обращения: 06.03.2023).
32. Codice dell'amministrazione digitale. Decreto Legislativo 7 marzo 2005, n. 82. URL: <https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/index.html> (дата обращения: 05.03.2023).
33. Italian Personal Data Protection Code. URL: <http://www.privacy.it/archivio/privacocode-en.html> (дата обращения: 05.03.2023).
34. Beliz. An Act to establish the E-Governance and Digitalization Department and provide for its powers, duties and functions; to promote and regulate the provision of electronic government (e-government) services; to enhance service delivery, citizen's access, and the efficiency and effectiveness of government administrative procedures; and to provide for matters connected therewith or incidental thereto. 2022. URL: <https://www.nationalassembly.gov.bz/wp-content/uploads/2022/10/Act-No-24-of-2022-Digital-Government-Act-2022.pdf> (дата обращения: 05.03.2023).
35. Federal Information Security Modernization Act of 2014. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text> (дата обращения: 06.03.2023).

36. Foundations for Evidence-Based Policymaking Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4174/text> (дата обращения: 05.03.2023).
37. German Act to promote electronic government. Translation provided by Gary Cox for the Federal Ministry of the Interior. The translation includes the amendment(s) to the Act by Article 1 of the Act of 25 July 2013 (Federal Law Gazette I p. 2749). URL: http://www.gesetze-im-internet.de/englisch_egovg/englisch_egovg.html#p0014 (дата обращения: 05.03.2023).
38. Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen. URL: <https://www.gesetze-im-internet.de/ozg/> (дата обращения: 05.03.2023).
39. Gramm-Leach-Bliley Act. Public law 106–102. 106th Congress. Nov. 12, 1999. URL: <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf> (дата обращения: 06.03.2023).
40. H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/3359/text> (дата обращения: 05.03.2023).
41. H.R.4174 - Foundations for Evidence-Based Policymaking Act of 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4174/text> (дата обращения: 05.03.2023).
42. Identity Documents Act 2010. URL: http://www.legislation.gov.uk/ukpga/2010/40/pdfs/ukpga_20100040_en.pdf (дата обращения: 05.03.2023).
43. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/> (дата обращения: 05.03.2023).
44. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000006529399/2004-08-07/> (дата обращения: 06.03.2023).
45. Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF n°0075 du 28 mars 2012 page 5604, texte n° 2. URL: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=20170503> (дата обращения: 05.03.2023).
46. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=91758002E1CCA159VABD6D3F5D4B33F4.tplgfr34s_2?cidTexte=JORFTEXT000033202746&categorieLien=id (дата обращения: 05.03.2023).
47. Loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendante. URL : <https://www.legifrance.gouv.fr/eli/loi/2017/1/20/PRMX1604064L/jo/texte> (дата обращения: 05.03.2023).

48. Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559> (дата обращения: 05.03.2023).
49. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: <https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article20> (дата обращения: 06.03.2023).
50. Loi organique n° 2017-54 du 20 janvier 2017 relative aux autorités administratives indépendantes et autorités publiques indépendantes. URL : <https://www.legifrance.gouv.fr/eli/loi/2017/1/20/PRMX1604073L/jo/texte> (дата обращения: 05.03.2023).
51. National Institute of Standards and Technology Act. As Amended Through P.L. 117–263, Enacted December 23, 2022. URL: <https://www.govinfo.gov/content/pkg/COMPS-5388/pdf/COMPS-5388.pdf> (дата обращения: 06.03.2023).
52. National Science and Technology Policy, Organization, and Priorities Act of 1976. URL: <https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg459.pdf> (дата обращения: 05.03.2023).
53. No TikTok on Government Devices Act. Passed the Senate December 14, 2022. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/1143/text> (дата обращения: 05.03.2023).
54. Österreich. Gesamte Rechtsvorschrift für E-Government-Gesetz, Fassung vom 20.06.2020. URL: [https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230#:~:text=\(1\)%20Dieses%20Bundesgesetz%20dient%20der,an%20diese%20Stellen%20erleichtert%20werden.](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230#:~:text=(1)%20Dieses%20Bundesgesetz%20dient%20der,an%20diese%20Stellen%20erleichtert%20werden.) (дата обращения: 05.03.2023).
55. Papua New Guinea. Digital Government Act. 2022. URL: https://www.parliament.gov.pg/uploads/acts/22A_41.pdf (дата обращения: 05.03.2023).
56. Presidential and Federal Records Act Amendments of 2014. URL: <https://www.congress.gov/bill/113th-congress/house-bill/1233/text> (дата обращения: 05.03.2023).
57. State and Local Government Cybersecurity Act of 2021. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/2520/text> (дата обращения: 06.03.2023).
58. Strengthening American Cybersecurity Act of 2022. URL: <https://www.congress.gov/bill/117th-congress/senate-bill/3600/text#toc-id87c2d95a-b307-45ec-81dd-09e23e4addc4> (дата обращения: 06.03.2023).
59. Tanzania. E-Government Act, 2019. URL: <https://gisp.gov.go.tz/assets/docs/e-Government%20Act,%202019.pdf> (дата обращения: 05.03.2023).
60. United States Chief Technology Officer Act. URL: <https://www.congress.gov/bill/114th-congress/house-bill/1764/text> (дата обращения: 05.03.2023).

61. USA, Department of Homeland Security. 6 CFR Part 37, RIN 1601-AA97. Effective on April 27, 2020. URL: <https://www.govinfo.gov/content/pkg/FR-2020-04-27/pdf/2020-08481.pdf> (дата обращения: 05.03.2023).
62. USA, REAL ID Act of 2005. URL: <https://www.congress.gov/bill/109th-congress/house-bill/418/text> (дата обращения: 05.03.2023).
63. USA. E-Government Act of 2002. URL: <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf> (дата обращения: 05.03.2023).
64. USA. Freedom of Information Act. 1966. URL: <https://www.govinfo.gov/content/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf> (дата обращения: 05.03.2023).
65. USA. The Paperwork Reduction Act of 1980 (Pub. L. No. 96-511, 94 Stat. 2812, codified at 44 U.S.C. §§ 3501–352144 U.S.C. §§ 3501–352144 U.S.C. §§ 3501–3521). URL: <https://www.govtrack.us/congress/bills/96/hr6410/text> (дата обращения: 05.03.2023).
66. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. URL: <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf> (дата обращения: 05.03.2023).

Акты Европейского союза

67. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE). URL: <http://data.europa.eu/eli/reg/2016/679/oj> (дата обращения: 06.03.2023).
68. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. URL: <http://data.europa.eu/eli/reg/2019/1157/oj> (дата обращения: 05.03.2023).
69. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024> (дата обращения: 05.03.2023).
70. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. URL: <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046> (дата обращения: 06.03.2023).
71. CJUE. Arrêt de la Cour (grande chambre) du 16 juillet 2020. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems. Affaire C-311/18. URL: <https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgreg=fr&jge=&td=%>

3BALL&jur=C%2CT%2CF&num=C-311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252C%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=fr&avg=&cid=13413760 (дата обращения: 06.03.2023).

Нормативно-правовые акты государственных органов

72. Указ Президента Российской Федерации от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». URL: <http://www.kremlin.ru/acts/news/69810> (дата обращения: 05.03.2023).
73. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 05.03.2023).
74. Указ Президента Российской Федерации от 21.12.2020 № 800 «Вопросы Государственного Совета Российской Федерации». URL: <http://publication.pravo.gov.ru/Document/View/0001202012210077?index=0&rangeSize=1> (дата обращения: 05.03.2023).
75. Указ Президента РФ от 07.03.2020 № 175 «О некоторых вопросах Совета Безопасности Российской Федерации» (вместе с Положением о Совете Безопасности Российской Федерации, Положением об аппарате Совета Безопасности Российской Федерации) // Собрание законодательства РФ, 09.03.2020, № 10, ст. 1323.
76. Указ Президента РФ от 21.01.2020 № 21 «О структуре федеральных органов исполнительной власти» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 346.
77. Указ Президента РФ от 19.07.2018 № 444 «Об упорядочении деятельности совещательных и консультативных органов при Президенте Российской Федерации» (вместе с Положением о Совете при Президенте Российской Федерации по стратегическому развитию и национальным проектам) // Собрание законодательства РФ, 23.07.2018, № 30, ст. 4717.
78. Указ Президента Российской Федерации от 14.06.2018 № 334 «О мерах по оптимизации структуры Администрации Президента Российской Федерации» (вместе с «Положением об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи») // Собрание законодательства РФ, 18.06.2018, № 25, ст. 3646.
79. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: <http://kremlin.ru/acts/bank/41460/page/1> (дата обращения: 05.03.2023).
80. Указ Президента Российской Федерации от 18.06.2012 № 876 «Об Управлении Президента Российской Федерации по общественным связям и

- коммуникациям» // Собрание законодательства Российской Федерации от 2012 г., № 26 , ст. 3498.
81. Указ Президента РФ от 18.06.2012 № 874 «Об утверждении Положения об Управлении пресс-службы и информации Президента Российской Федерации» // Собрание законодательства РФ, 25.06.2012, № 26, ст. 3497.
 82. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102046005> (дата обращения: 05.03.2023).
 83. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). URL: <http://government.ru/info/35568/> (дата обращения: 05.03.2023).
 84. Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (утверждено Указом Президента РФ от 06.05.2011 № 590) // Собрание законодательства РФ, 09.05.2011, № 19, ст. 2721.
 85. Основные направления деятельности Правительства Российской Федерации на период до 2024года (утверждены Председателем Правительства Российской Федерации 29.09.2018). С. 19. URL: <http://static.government.ru/media/files/ne0vGNJUk9SQjIGNNsXlX2d2CpCho9qS.pdf> (дата обращения: 14.05.2023).
 86. Постановление Правительства Российской Федерации от 15.04.2023 № 603 «Об утверждении приоритетных направлений проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации и Положения об условиях отнесения проектов к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации, о представлении сведений о проектах технологического суверенитета и проектах структурной адаптации экономики Российской Федерации и ведении реестра указанных проектов, а также о требованиях к организациям, уполномоченным представлять заключения о соответствии проектов требованиям к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации». URL: <http://static.government.ru/media/files/8JsiO5kSIItJA1g5IHhGd5qiQVACelECn.pdf> (дата обращения: 05.05.2023).
 87. Постановление Правительства РФ от 16.12.2022 № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего

- хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555» // Собрание законодательства РФ, 26.12.2022, № 52, ст. 9610.
88. Постановление Правительства Российской Федерации от 10.10.2022 № 1804 «О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения». URL: <http://publication.pravo.gov.ru/Document/View/0001202210120022> (дата обращения: 05.03.2023).
89. Постановление Правительства РФ от 21.01.2022 № 29 «Об утверждении Правил присоединения сетей электросвязи и их взаимодействия и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации» // Собрание законодательства РФ", 31.01.2022, № 5, ст. 763.
90. Постановление Правительства РФ от 14.05.2021 № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства РФ, 24.05.2021, № 21, ст. 3585.
91. Постановление Правительства РФ от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» // Собрание законодательства РФ, 17.06.2019, № 24, ст. 3099.
92. Постановление Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (вместе с Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах) // Собрание законодательства РФ, 10.06.2019, № 23, ст. 2963.
93. Постановление Правительства Российской Федерации от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями». URL: <http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102487569&backlink=1&&nd=102466887> (дата обращения: 05.03.2023).
94. Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное

- общество» // Собрание законодательства РФ, 05.05.2014, № 18 (часть II), ст. 2159.
95. Постановление Правительства Российской Федерации от 26.08.2013 № 735 «О Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности» // Собрание законодательства РФ, 02.09.2013, № 35, ст. 4521.
96. Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (вместе с Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг) // Собрание законодательства РФ, 04.02.2013, № 5, ст. 377.
97. Постановление Правительства РФ от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Правилами присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме») // Собрание законодательства РФ, 31.12.2012, № 53 (ч. 2), ст. 7938.
98. Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с Требованиями к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме») // Собрание законодательства РФ, 05.12.2011, № 49 (ч. 5), ст. 7284.
99. Постановление Правительства РФ от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Положением об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения

- государственных и муниципальных функций в электронной форме») // Собрание законодательства РФ, 13.06.2011, № 24, ст. 3503.
100. Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия») // Собрание законодательства РФ, 20.09.2010, № 38, ст. 4823.
101. Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций) // Российская газета, № 49, 24.03.2009.
102. Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // Собрание законодательства РФ, 09.06.2008, № 23, ст. 2708.
103. Постановление Правительства Российской Федерации от 28.03.2008 № 215 «О Правительственной комиссии по федеральной связи и информационным технологиям // Собрание законодательства РФ, 31.03.2008, № 13, ст. 1315.
104. Постановление Правительства РФ от 19.01.2005 № 30 «О Типовом регламенте взаимодействия федеральных органов исполнительной власти» // Российская газета, № 12, 25.01.2005.
105. Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)»» // Собрание законодательства РФ, 04.02.2002, № 5, ст. 531.
106. План законопроектной деятельности Правительства Российской Федерации на 2023 год (утв. Распоряжением Правительства Российской Федерации от 23 декабря 2022 г. № 4112-р). URL: <http://static.government.ru/media/files/ON30zFKdZXJwOeXlaJRB62ID4uu8trDE.pdf> (дата обращения: 05.03.2023).
107. Распоряжение Правительства РФ от 21.10.2022 № 3102-р «Об утверждении Концепции создания и функционирования единой цифровой платформы Российской Федерации «ГосТех», плана мероприятий («дорожной карты») по созданию единой цифровой платформы Российской Федерации «ГосТех»» // Собрание законодательства РФ, 31.10.2022, № 44, ст. 7594.
108. Распоряжение Правительства РФ от 22.01.2020 № 56-р «Об утверждении структуры Аппарата Правительства Российской Федерации и о признании утратившими силу некоторых актов Правительства Российской Федерации» // Собрание законодательства РФ, 27.01.2020, № 4, ст. 440.
109. Распоряжение Правительства Российской Федерации от 03.09.2013 № 1578-р. URL: <http://static.government.ru/media/files/41d489d9ad294a026279.pdf> (дата обращения: 05.03.2023).
110. Приказ Минтруда России от 22.04.2020 № 211н «Об утверждении Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах» (Зарегистрировано в Минюсте

- России 15.07.2020 № 58956). URL: <http://publication.pravo.gov.ru/Document/View/0001202007160003> (дата обращения: 05.03.2023).
111. Приказ МВД России от 31.12.2017 № 984 «Об утверждении Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по регистрационному учету граждан Российской Федерации по месту пребывания и по месту жительства в пределах Российской Федерации» (Зарегистрировано в Минюсте России 05.04.2018 № 50635). URL: <http://publication.pravo.gov.ru/Document/View/0001201804060020> (дата обращения: 15.05.2023).
112. Приказ Минкомсвязи России от 30.11.2015 № 48 «Об установлении Порядка обеспечения условий доступности для инвалидов по зрению официальных сайтов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления в сети "Интернет» (Зарегистрировано в Минюсте России 01.02.2016 N 40905) // Российская газета, № 27, 10.02.2016.
113. Приказ Минкомсвязи РФ от 01.11.2010 № 156 «Об организации плановых проверок деятельности подведомственных Министерству связи и массовых коммуникаций Российской Федерации федеральной службы и федеральных агентств» (вместе с Инструкцией по организации плановых проверок деятельности подведомственных Министерству связи и массовых коммуникаций Российской Федерации Федеральной службы и федеральных агентств) (Зарегистрировано в Минюсте РФ 08.12.2010 № 19141) // Российская газета, № 291, 24.12.2010.
114. Приказ Минкомсвязи России от 13.04.2012 № 107 «Об утверждении Положения о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (Зарегистрировано в Минюсте России 26.04.2012 № 23952) // Российская газета, № 112, 18.05.2012.
115. Приказ Федеральной налоговой службы от 03.11.2020 № ЕД-7-15/790@ «Об утверждении Административного регламента по предоставлению Федеральной налоговой службой государственной услуги по выдаче свидетельства о регистрации лица, совершающего операции по переработке средних дистиллятов, и формы решения о приостановлении (возобновлении) действия, о неполном устранении нарушений, повлекших за собой приостановление действия, об аннулировании свидетельства о регистрации лица, совершающего операции по переработке средних дистиллятов». URL: <http://publication.pravo.gov.ru/Document/View/0001202012240003> (дата обращения: 15.05.2023).

116. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». URL: <http://publication.pravo.gov.ru/Document/View/0001202104210039> (дата обращения: 05.03.2023).
117. Приказ ФНС России от 29.06.2012 № ММВ-7-6/435@ «Об утверждении Порядка и условий присвоения, применения, а также изменения идентификационного номера налогоплательщика» (Зарегистрировано в Минюсте России 14.08.2012 № 25183) // Российская газета, № 192, 22.08.2012.
118. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам») (Зарегистрировано в Минюсте России 06.09.2018 N 52109) //
119. Распоряжение Департамента информационных технологий города Москвы от 13.03.2023 № 64–16-120/23 «Об утверждении Правил использования информационных систем и ресурсов города Москвы при реализации проекта «Электронный дом». URL: <https://www.mos.ru/dit/documents/normativnye-pravovye-akty-departamenta/view/283481220/> (дата обращения: 05.03.2023).
120. Распоряжение Департамента информационных технологий города Москвы от 31.03.2023 № 64–16-168/23 «Об установлении порядка направления и рассмотрения заявок о предоставлении доступа к наборам городских данных». URL: <https://www.mos.ru/dit/documents/normativnye-pravovye-akty-departamenta/view/285419220/> (дата обращения: 05.03.2023).
121. Распоряжение руководителя Департамента информационных технологий города Москвы № 64-16-186/20 от 29.04.2020 «Об утверждении порядка применения технологии электронного мониторинга местоположения гражданина в определенной геолокации с использованием мобильного приложения «Социальный мониторинг»». URL: <https://www.mos.ru/dit/documents/view/238534220/> (дата обращения: 06.03.2023).
122. Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029122964> (дата обращения: 06.03.2023).
123. Arrêté du 23 mai 2017 portant création d'un système de téléservices destiné à l'accomplissement de démarches administratives relatives aux certificats d'immatriculation des véhicules. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034832438> (дата обращения: 06.03.2023).
124. Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité

- numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL : <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000046503138#JORFARTI000046503138> (дата обращения: 06.03.2023).
125. Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'Etat. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037611479/> (дата обращения: 05.03.2023).
126. Canada, Policy on Service and Digital. URL: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603> (дата обращения: 05.03.2023).
127. Canada. Directive on Service and Digital. URL: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601> (дата обращения: 05.03.2023).
128. Décret du 4 juillet 2022 relatif à la composition du Gouvernement. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046013941> (дата обращения: 05.03.2023).
129. Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000021542333/2010-01-13/> (дата обращения: 05.03.2023).
130. Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212/> (дата обращения: 05.03.2023).
131. Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030195477/2021-02-22/> (дата обращения: 06.03.2023).
132. Décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000030315053/#LEGIARTI000030315053> (дата обращения: 05.03.2023).
133. Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405903> (дата обращения: 05.03.2023).
134. Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense. URL:

- <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405967> (дата обращения: 05.03.2023).
135. Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039281619/2021-07-14/> (дата обращения: 05.03.2023).
136. Décret n° 2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés » (TES) URL: <https://www.legifrance.gouv.fr/eli/decret/2021/3/13/INTD2104790D/jo/texte> (дата обращения: 05.03.2023).
137. Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/> (дата обращения: 06.03.2023).
138. Executive Order № 13719 of February 9, 2016. Establishment of the Federal Privacy Council. URL: <https://www.govinfo.gov/content/pkg/FR-2016-02-12/pdf/2016-03141.pdf> (дата обращения: 05.03.2023).
139. Executive Order № 13859 of February 11, 2019. Maintaining American Leadership in Artificial Intelligence. URL: <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence> (дата обращения: 05.03.2023).;
140. Executive Order 13960 of December 3, 2020. Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. URL: <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government> (дата обращения: 05.03.2023).
141. Executive Order № 13526. Classified National Security Information. December 29, 2009. URL: <https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information> (дата обращения: 05.03.2023).
142. Executive Order № 13556. Controlled Unclassified Information. URL: <https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information> (дата обращения: 05.03.2023).
143. Executive Order on Ensuring Responsible Development of Digital Assets. March 9, 2022. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (дата обращения: 05.03.2023).
144. Executive Order on Improving the Nation's Cybersecurity. May 12, 2021. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> (дата обращения: 05.03.2023).;

145. Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries. June 9, 2021. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/> (дата обращения: 05.03.2023).
146. FTC. Telemarketing Sales Rule. US Code of Federal Regulations. Aug. 10, 2010. URL: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-310> (дата обращения: 05.03.2023).
147. India. National Data Sharing and Accessibility Policy. 2012. URL: <https://dst.gov.in/sites/default/files/gazetteNotificationNDSAP.pdf> (дата обращения: 05.03.2023).
148. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. URL: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> (дата обращения: 05.03.2023).
149. Federal Incident Notification Guidelines. April 1, 2017. URL: <https://www.cisa.gov/federal-incident-notification-guidelines> (дата обращения: 06.03.2023).
150. Livre blanc sur la défense et la sécurité nationale. Le 13 juillet 2012. URL: <http://www.livreblancdefenseetsecurite.gouv.fr/index.html> (дата обращения: 05.03.2023).
151. M-21-30 Protecting Critical Software Through Enhanced Security Measures. August 10, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf> (дата обращения: 05.03.2023).
152. M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident. August 27, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf> (дата обращения: 05.03.2023);
153. M-22-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response. October 8, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf> (дата обращения: 05.03.2023);
154. M-22-05 Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements. December 6, 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf> (дата обращения: 05.03.2023);
155. M-22-16 Administration Cybersecurity Priorities for the FY 2024 Budget. July 22, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf> (дата обращения: 05.03.2023).; M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. January 26, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf> (дата обращения: 05.03.2023);
156. M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices September 14, 2022. URL:

- <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf> (дата обращения: 05.03.2023);
157. Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. January 19, 2022. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/> (дата обращения: 05.03.2023).
158. Memorandum on Renewing the National Security Council System. February 4, 2021. URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system/> (дата обращения: 05.03.2023).;
159. National Cybersecurity Strategy. March 2023. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> (дата обращения: 05.03.2023).
160. OMB. «No TikTok on Government Devices» Implementation Guidance. February 27, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf (дата обращения: 05.03.2023).
161. OMB. Federal Data Strategy - A Framework for Consistency. June 4, 2019. URL: <https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf> (дата обращения: 05.03.2023).
162. OMB. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. August 8, 2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf (дата обращения: 05.03.2023).
163. OMB. Memorandum for heads of executive departments and agencies. Transition to Electronic Records. June 28, 2019. URL: <https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf> (дата обращения: 06.03.2023).
164. OMB. Memorandum for heads of executive departments and agencies. Update to Transition to Electronic Records. December 23, 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/12/M_23_07-M-Memo-Electronic-Records_final.pdf (дата обращения: 06.03.2023).
165. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/> (дата обращения: 05.03.2023).
166. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/> (дата обращения: 06.03.2023).

167. Référentiel général d'interopérabilité (RGI). 12 janvier 2016 - mis à jour le 18 décembre 2020. URL: <https://www.numerique.gouv.fr/publications/interopabilite/> (дата обращения: 05.03.2023).
168. Revue nationale stratégique 2022, présentée le mercredi 9 novembre par le Président de la République. URL: http://www.sgdsn.gouv.fr/communiqués_presse/revue-nationale-strategique-2022/ (дата обращения: 05.03.2023).
169. The New York State Office of Information Technology Services. Process for Establishing Information Technology Policies, Standards, and Guidelines. № NYS-P09-003. Updated: 05.04.2021. URL: https://its.ny.gov/system/files/documents/2022/10/nys-p09-003_process_for_establishing_information_technology_policies.pdf (дата обращения: 05.03.2023).

Судебная практика

170. Постановление Конституционного Суда РФ от 31.03.2015 № 6-П «По делу о проверке конституционности пункта 1 части 4 статьи 2 Федерального конституционного закона «О Верховном Суде Российской Федерации» и абзаца третьего подпункта 1 пункта 1 статьи 342 Налогового кодекса Российской Федерации в связи с жалобой открытого акционерного общества «Газпром нефть»» // Российская газета, № 77, 13.04.2015.
171. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда РФ, № 7, июль, 2019;
172. Постановление Пленума Верховного Суда РФ от 25.12.2018 № 50 «О практике рассмотрения судами дел об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства и обладающих нормативными свойствами» // Российская газета, № 6, 15.01.2019.
173. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2018) (утв. Президиумом Верховного Суда РФ 04.07.2018) // Бюллетень Верховного Суда РФ, № 3, март, 2019 (начало), Бюллетень Верховного Суда РФ, № 4, апрель, 2019 (окончание).
174. Решение Верховного Суда РФ от 16.06.2016 № АКПИ16-427 «Об отказе в удовлетворении заявления о признании недействующим письма ФНС России от 24.02.2016 № ГД-3-14/743@» // СПС «Консультант Плюс».
175. Апелляционное определение Апелляционной коллегии Верховного Суда РФ от 02.03.2021 № АПЛ21-21 // СПС «КонсультантПлюс»;
176. Апелляционное определение Апелляционной коллегии Верховного Суда РФ от 03.06.2021 № АПЛ21-171 // СПС «КонсультантПлюс».

177. Кассационное определение Девятого кассационного суда общей юрисдикции от 03.02.2021 N 88а-754/2021 по делу № 2а-9/2020 // СПС «КонсультантПлюс».
178. Кассационное определение Девятого кассационного суда общей юрисдикции от 11.11.2020 № 88а-7747/2020 // СПС «КонсультантПлюс».
179. Кассационное определение Первого кассационного суда общей юрисдикции от 21.12.2021 № 88а-32234/2021 // СПС «КонсультантПлюс».
180. Постановление Суда по интеллектуальным правам от 03.02.2020 № С01-1508/2019 по делу № А40-311941/2018 // СПС «КонсультантПлюс».
181. Conseil d'État 434684, lecture du 19 juin 2020. URL: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684> (дата обращения: 06.03.2023).
182. Conseil d'État, 19 mai 1933, Benjamin. URL: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/1933-05-19/17413> (дата обращения: 06.03.2023).
183. Conseil d'État, Assemblée, 26/10/2011, 317827, Publié au recueil Lebon. URL: <https://www.legifrance.gouv.fr/ceta/id/CETATEXT000024736671> (дата обращения: 06.03.2023).
184. Conseil d'Etat, Assemblée, 2 juillet 1982, Huglo, requête numéro 25288, publié au recueil. URL: <https://www.revuegeneraledudroit.eu/blog/decisions/conseil-detat-assemblee-2-juillet-1982-huglo-requete-numero-25288-publie-au-recueil/> (дата обращения: 06.03.2023).
185. L'étude annuelle 2013 du Conseil d'État. Le droit souple. URL: <https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000280.pdf> (дата обращения: 06.03.2023).
186. Le Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012 // ORF n°0075 du 28 mars 2012 page 5607, texte n° 6. URL: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582452> (дата обращения: 05.03.2023).
187. Tribunal de grande instance de Paris, 3ème chambre, 1ère section, jugement du 4 décembre 2014. URL: <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-1ere-section-jugement-du-4-decembre-2014-2/> (дата обращения: 06.03.2023).
188. Tribunal judiciaire de Paris, ordonnance de référé du 8 janvier 2020. URL: <https://www.legalis.net/jurisprudences/tribunal-judiciaire-de-paris-ordonnance-de-refere-du-8-janvier-2020/> (дата обращения: 06.03.2023).
189. Shibley v. Time, Inc., 45 Ohio App. 2d 69, 341 N.E.2d 337 (Ohio Ct. App. 1975). URL: https://casetext.com/case/shibley-v-time-inc/case-details?PHONE_NUMBER_GROUP=C (дата обращения: 05.03.2023).
190. Dwyer v. American Express Co., 273 Ill. App. 3d 742, 652 N.E.2d 1351 (Ill. App. Ct. 1995). URL: https://casetext.com/case/dwyer-v-american-express-co/case-details?PHONE_NUMBER_GROUP=C (дата обращения: 05.03.2023).

191. Dyer v. Northwest Airlines Corporations, 334 F. Supp. 2d 1196 (D.N.D. 2004).
URL: <https://law.justia.com/cases/federal/district-courts/FSupp2/334/1196/2520672/> (дата обращения: 05.03.2023).

Монографии, учебные пособия, книги

192. Атаманчук Г.В. Теория государственного управления: учебник. М.: Омега-Л, 2010. 525 с.
193. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации: новая редакция (постатейный). 3-е изд., перераб. и доп. М.: Проспект, 2020. 256 с.
194. Бахрах Д. Н., Российский Б. В., Старилов Ю. Н. Административное право: Учебник для вузов. 2-е изд., изм. и доп. М.: Норма, 2005. 799 с.
195. Бахрах Д.Н. Советское законодательство об административной ответственности. Пермь, 1969. 344 с.
196. Бачило И.Л. Функции органов управления. Москва, 1976. 198 с.
197. Государственное управление в СССР в условиях научно-технической революции / отв. ред. М. И. Пискотин. М.: Наука, 1978. 407 с.
198. Децентрализованные органы и учреждения в системе исполнительной власти зарубежных государств: научно-практическое пособие / Н. М. Касаткина, Ф. А. Лещенков, А. Н. Пилипенко и др.; отв. ред. А. Н. Пилипенко. М.: ИЗиСП: Норма: ИНФРА-М, 2018. 208 с.
199. Зеленцов А.Б., Лафитский В.И., Тимошенко И.Г. и др. Тенденции развития контроля за деятельностью публичной администрации в зарубежных государствах: монография / отв. ред. В.И. Лафитский, И.Г. Тимошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2015. 446 с.
200. Еропкин М.И. Советское административное право. Учебник для средних юридических учебных заведений. М.: Юрид. лит., 1979. 311 с.
201. Еропкин М.И., Попов Л.Л. Административно-правовая охрана общественного порядка. Ленинград: Лениздат, 1973. 328 с.
202. Захарова М.В. Учение о юридических картах мира. М.: Аспект Пресс, 2022. 264 с.
203. Информационное право: учебник / Бачило И.Л. 4-е изд., перераб. и доп. М.: Юрайт, 2016. 437 с.
204. Информационные ресурсы развития Российской Федерации: Правовые проблемы / Институт государства и права. М.: Наука, 2003. 403 с.
205. Исполнительная власть в Российской Федерации. Проблемы развития / отв. ред. И.Л. Бачило. М.: Юрист. 1998. 431 с.
206. История государства и права зарубежных стран: Учебник для вузов. В 2 ч. Ч. 2 / под общ. ред. д.ю.н. проф. О.А. Жидкова и д.ю.н. проф. Н.А. Крашенинниковой. 2-е изд. стер. М.: Норма, 2003. С. 248 – 251. 702с.
207. Кельзен Г. Чистое учение о праве. 2-е изд / пер. с нем. М.В. Антонова и С.В. Лёзова. СПб.: ООО Издательский Дом «Алеф-Пресс», 2015. 542 с.

208. Козлов Ю.М. Административное право: Учебник. М.: Юристъ, 1999. 271 с.
209. Козырева Т.И. Административное принуждение и его виды. Москва, 1957. 47 с.
210. Козырин А.Н., Глушко Е.К., Штатина М.А. Публичная администрация и административные реформы в зарубежных странах: учеб. пособие. Гос. ун-т - Высш. шк. экономики. М.: ТЕИС, 2006. 287 с.
211. Конин Н.М. Административное право России в вопросах и ответах: учебное пособие. Москва: Проспект, 2013. 256 с.
212. Курашвили Б.П. Очерк теории государственного управления / отв. ред.: Пискотин М.И. М.: Наука, 1987. 292 с.
213. Лазарев Б.М. Компетенция органов управления. М.: Юрид. лит., 1972. 280 с.
214. Манохин В.М. Административное право России: учебник. Саратов: Ай Пи Эр Медиа, 2011. 137 с.
215. Манохин В.М. Правотворческая деятельность в субъектах Российской Федерации: Вопросы методики. Саратов: СГАП, 2000. 81 с.
216. Попова Н. Ф. Правовое обеспечение государственного и муниципального управления: учебник и практикум для вузов / под общей редакцией Г. Ф. Ручкиной. М.: Юрайт, 2023. 239 с.
217. Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М.: ЗАО «Юстицинформ», 2009. 344 с.
218. Публичная власть: система, компетенции: монография / под общ. ред. М.Н. Кобзарь-Фроловой; отв. ред. И.В. Глазунова. Воронеж: Издательско-полиграфический центр «Научная книга», 2021. 237 с.
219. Рябов Ю.С. Административно-предупредительные меры. Теоретические вопросы. Пермь: Книжное издательство, 1974. 82 с.
220. Семененко И.И. Административное принуждение. Ростов-на-Дону, 1999. 134 с.
221. Тихомиров Ю.А. Теория компетенции. М.: Юстицинформ, 2001. 351 с.
222. Тихомиров Ю.А. Научная организация управления. М.: Сов. Россия, 1973. 173 с.
223. Формы государственного управления / отв. ред. Б.М. Лазарев. М.: ИГПАН, 1983. 149 с.
224. Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. N 1-ФКЗ "О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти". Москва: Норма, ИНФРА-М, 2020. 240 с.
225. Чиркин В.Е. Публичная власть. М.: Юристъ, 2005. 174 с.
226. Якуба О.М. Административная ответственность. М.: Юридическая литература, 1972. 152 с.
227. Ямпольская Ц.А. Органы советского государственного управления в современный период / Отв. ред.: Коток В.Ф. М.: Изд-во АН СССР, 1954. 228 с.

228. Camp J.L. Economics of Identity Theft: Avoidance, Causes and Possible Cures // Springer Science+Business Media, LLC, 2007. 199 p.
229. Chemerinsky E. Constitutional law: principles and policies. Fifth Edition. 2015. 1520 p.
230. Kalpokas I. Algorithmic Governance. Politics and Law in the Post-Human Era. Cham: Palgrave Pivot, 2019. 120 p.

Диссертации и авторефераты диссертаций

231. Агеев А.С. Право на доступ к информации, находящейся в распоряжении государственных органов (особенности конституционно-правового регулирования в России и в Германии): автореф. дис. ... к.ю.н. Москва, 2016. 28 с.
232. Аляутдинов Ф.М. Конституционно-правовой статус органов исполнительной власти в Российской Федерации: дис. ... к.ю.н. Москва, 2001. 188 с.
233. Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: дис. ... к.ю.н. Москва, 2004. 289 с.
234. Архипов В.В. Семантические пределы права в условиях медиального поворота: теоретико-правовая интерпретация: дис. ... д.ю.н. Санкт-Петербург, 2019. 354 с.
235. Бондарец Е.Б. Конституционно-правовой статус главы государства в системе власти современной России: автореф. дис. ... к.ю.н. Москва, 2014. 27 с.
236. Бондарь И.В. Тайна по российскому законодательству (Проблемы теории и практики): дис. ... к.ю.н. Н. Новгород, 2004. 203 с.
237. Бочарников Ю.Ф. Конституционно-правовой статус органов административной юстиции Италии: дис. ... к.ю.н. Москва, 2007. 158 с.
238. Ганя Д.В. Административно-правовой статус органов государственного управления Республики Молдова: дис. ... к.ю.н. Москва, 1999. 189 с.
239. Гунин Д.И. Транспарентность и тайна информации: теоретико-правовой аспект: автореф. дис. ... к.ю.н. Екатеринбург, 2008. 31 с.
240. Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: автореф. дис. ... д.ю.н. Москва, 2021. 37 с.
241. Жирнова Н.А. Банковская и налоговая тайны как объекты финансово-правового регулирования: автореф. дис. ... к.ю.н. Саратов, 2013. 26 с.
242. Исаева Н.В. Правовая идентичность (теоретико-правовое исследование): дис. ... докт. юрид. наук. М., 2014. 49 с.
243. Каплунов А.И. Административное принуждение, применяемое органами внутренних дел (системно-правовой анализ): автореф. дис. ... д.ю.н. Москва, 2005. 58 с.

244. Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении: автореф. дис. ... д.ю.н. Саратов, 2014. 54 с.
245. Коркин А.В. Институт административно-правового принуждения: меры, применяемые сотрудниками милиции: автореф. дис. ... к.ю.н. Челябинск, 2004. 23 с.
246. Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... к.ю.н. Челябинск, 2010. 23 с.
247. Лопатин В.Н. Информационная безопасность России: дис. ... д.ю.н. СПб., 2000. 433 с.
248. Наумов В.Б. Институт идентификации в информационном праве: автореф. дис. ... д.ю.н. Москва. 2020. 52 с.
249. Пермяков М.В. Категория «тайна» в системе правового регулирования: дис. ... к.ю.н. Екатеринбург, 2006. 234 с.
250. Пилия Д.Э. Правовой статус органов исполнительной власти Республики Абхазия: дис. ... к.ю.н. Москва, 2010. 172 с.
251. Потапов Н.А. Правовое регулирование коммерческой тайны в Российской Федерации: автореф. дис. ... к.ю.н. Москва, 2010. 24 с.
252. Сорокин Д.С. Реформирование системы и структуры федеральных органов исполнительной власти Российской Федерации: автореферат дис. ... к.ю.н. Москва, 2004. 24 с.
253. Талапина Э.В. Модернизация государственного управления в информационном обществе: автореф. дис. ... д.ю.н. Москва, 2015. 53 с.
254. Терещенко Л.К. Правовой режим информации: дис. ... д.ю.н. Москва, 2011. 415 с.
255. Туликов А.В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): дис. ... к.ю.н. Москва. 2017. 180 с.
256. Щербович А.А. Конституционные гарантии свободы слова и права доступа к информации в сети Интернет: автореф. дис. ... к.ю.н. Москва, 2013. 27 с.

Научные статьи

257. Абрамова А.И. Подзаконное правотворчество в современном понимании: реалии и перспективы // Журнал российского права. 2019. № 8. С. 25–35.
258. Алпаткина Е.С. Государственный Совет Российской Федерации: мифы и реальность // Государственная власть и местное самоуправление. 2021. № 5. С. 55–60.
259. Андрущенко Е.С. Проблема идентификации субъектов Интернет-отношений. Виртуальное лицо // Информационное общество: проблемы развития законодательства. Сборник научных работ. М.: ИГП РАН, ЮРКОМПАНИ, 2012. С. 79–86.

260. Архипов В.В., Наумов В.Б., Смирнова К.М. Пределы принятия юридически значимых решений с использованием искусственного интеллекта // Вестник Санкт-Петербургского университета. Право. 2021. № 4. С. 882-906.
261. Бахрах Д.Н. Субъекты российского права // Экономика региона. 2006. № 2. С. 121–131.
262. Бачило И.Л. Правовая платформа построения электронного государства // Информационное право. М.: Юрист, 2008, № 4. С. 3-8.
263. Белясов С.Н. Возмещение вреда государством и должностными лицами в решениях Конституционного Суда Российской Федерации // Право и государство: теория и практика. 2017. № 6. С. 21-24.
264. Богдановская И.Ю. Понятие «электронного государства»: правовые аспекты // Информационное общество и социальное государство: сборник научных работ. М.: ИГП РАН, 2009. С. 45-55.
265. Бондарь Н.С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25–42.
266. Бучакова М.А. Административно-правовое регулирование координации как функции государственного управления // Вестник Омского университета. Серия «Право». 2014. № 2 (49). С. 60–64.
267. Варламова Н.В. Цифровые права – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Том 14. № 4. С. 9–46;
268. Виноградова Е.В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е.В. Виноградова, Т.А. Полякова, А.В. Минбалеев // Правоприменение. 2021. Т. 5. № 4. С. 5–19;
269. Гриценко В.В. Доктрина информационной безопасности Российской Федерации: сущность, современное значение и организационно-правовые основы // Вестник ВГУ. Серия: Право. 2017. №1 (28). С. 78–88.
270. Гуляков А.Д. Логика развития федерализма в США (историко-государствоведческая и историко-правовая оценка) // Lex Russica. 2016. № 7. С. 116–129.
271. Дамм И. А., Акунченко Е. А., Щедрин Н. В. Открытость публичной власти: вопросы понятийно-категориального аппарата // Вестник Санкт-Петербургского университета. Право. 2019. № 2. С. 226–242.
272. Дмитрик Н.А. Корпорации в своем праве // Закон. 2021. № 12. С. 103 – 114.
273. Добробаба М.Б., Чаннов С.Е., Минбалеев А.В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина. № 4 (92). 2022. С. 25-37.
274. Дугаржапов А.Г. Полномочия Госсовета КНР // Проблемы современной науки и образования. 2015. № 2. С. 81–85.
275. Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О. Е. Кутафина. №. 4 (92). 2022. С. 46-58.

276. Жарова А. К. Правовое обеспечение цифрового профилирования деятельности человека // Вестник ЮУрГУ. Серия «Право». 2020. Т. 20. № 2. С. 80–87;
277. Зверев М.А. Тенденции развития административной реформы на примере реформирования системы федеральных органов исполнительной власти // Бизнес, менеджмент и право. 2020. № 3 (47). С. 57–63.
278. Злобин А.В. Общая характеристика органов государства с особым правовым статусом // Вестник Саратовской государственной военной юридической академии. 2014. № 6. С. 66–71.
279. Исаков В. Б. Преимущество правовых норм в сфере технического регулирования // Юридическая техника. 2011. № 5. С. 184–191.
280. Калинин А. О реформировании системы и структуры органов исполнительной власти в РФ // Общество и экономика. 2019. № 5. С. 78–86.
281. Калмыкова А.В., Кабытов П.П. «Гибкие» структуры государственного управления // Журнал российского права. 2019. № 8. С. 107–120.
282. Колосова Н.М., Колосов К.М. Президент Российской Федерации как гарант информационной безопасности личности // Журнал российского права. 2020. № 4. С. 17–27.
283. Конькова А.Ю. Документирование удостоверения личности в дореволюционной России // Вестник РГГУ. 2016. № 2 (4). С. 18–26.
284. Кравец И.А. Цифровое гражданство и конституционные вызовы в информационном и алгоритмическом обществе // Сравнительное конституционное обозрение. 2023. N 2. С. 93 - 123.
285. Лескина Э.И. Квантовые технологии и перспективы правового регулирования защиты данных // Юрист. 2022. № 11. С. 2 - 6.
286. Липень С. В. Сетевая парадигма и современное государство в юридических исследованиях начала XXI в. // Актуальные проблемы российского права. 2020. Т. 15. № 10. С. 11—19.
287. Максуров А.А. Координационная юридическая технология в Соединенном Королевстве (на примере отдельных регионов) // Вестник Санкт-Петербургского университета. 2018. Т. 9. № 3. С. 278–290.
288. Мартынова Н.А., Хмельков А.Б. Цифровые технологии в государственном управлении: опыт России и Республики Индия // Среднерусский вестник общественных наук. 2019. № 1. С. 127–144.
289. Меликов А.В. Основные этапы конституционно-правового развития Греции // Известия высших учебных заведений. Поволжский регион. 2020. № 3. С. 15–30.
290. Мешков П.В. О проблемах понимания и реализации обеспечительных мер в производстве по делам об административных правонарушениях в России и за рубежом // Юрист. 2018. № 10. С. 64–69.
291. Минервин И.Г. Эволюция электронного правительства в США // Экономические и социальные проблемы России. 2015. № 2. С. 48–75.

292. Михеева Т.Н. Государственный Совет Российской Федерации: история и современность // Государственная власть и местное самоуправление. 2021. N 4. С. 51–55.
293. Мочалов А.Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica (Русский закон). 2021. № 9. С. 88–101.
294. Нарутто С.В. Конституция, федерализм и единство государственно-правовой системы России // Lex Russica. 2018. № 11. С. 83-92.
295. Наумов В.Б. Негативные закономерности формирования понятийного аппарата в сфере регулирования Интернета и идентификации // Информационное право. 2018. № 1. С. 32-39.
296. Петров А.Ю. «Право на хорошее управление» (right to good administration): традиции и современность // Вестник ЮУрГУ. Серия «Право». 2013. Т. 13. № 3. С. 88–92.
297. Пехтерева Е.А. Электронное правительство Сингапура // Экономические и социальные проблемы России. 2015. № 2. С. 107–125.
298. Путило Н.В., Волкова Н.С. Феномен «Nannystate»: новый вид государства или модификация государственного патернализма в современных условиях? // Журнал российского права. 2020. № 12. С. 19–31.
299. Редких С.В. Понятие правового статуса: формально-правовой контекст. Пробелы в российском законодательстве // Юридический журнал. 2009. № 3. С. 42–44.
300. Смирнова А.А. О соотношении государственных услуг, функций и полномочий органов исполнительной власти // Журнал российского права. 2015. № 3. С. 120–130.
301. Стырин Е.М., Дмитриева Н.Е., Синятуллина Л.Х. Государственные цифровые платформы: от концепта к реализации // Вопросы государственного и муниципального управления. 2019. № 4. С. 31–60.
302. Стырин Е.М., Родионова Ю.Д. единая информационная система в сфере закупок как государственная цифровая платформа: современное состояние и перспективы // Вопросы государственного и муниципального управления. 2019. № 3. С. 49–70.
303. Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. 2019. Том 14. № 3. С. 122–145;
304. Терещенко Л.К. Государственное регулирование и дерегулирование в сфере связи // Журнал российского права. 2019. № 10. С. 98–108.
305. Терещенко Л.К. Реестровая модель оказания государственных и муниципальных услуг // Журнал российского права. 2021. N 7. С. 110–120.
306. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. № 8 (224). С. 100–109;
307. Туманов В.А. Права человека и исполнительная власть // Советское государство и право. 1990. № 2. С. 44 - 51.

308. Холодная Е.В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина. № 4 (92). 2022. С. 38-45.
309. Цветков В.В. Правовая природа открытого метода координации в сфере социального права Европейского союза // Вестник Санкт-Петербургского университета. 2016. № 4. С. 29–35.
310. Цюсэнь Л. Система и развитие законодательства Китайской Народной Республики // Вестник СПбГУ. Право. 2020. Т. 11. Вып. 3. С. 666–678.
311. Чаннов С.Е. Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. 2018. N 9. С. 48–54.
312. Чепус А. В. Организация работы Правительства в России и США // Право и современные государства. 2012. № 3. С. 30-38.
313. Штатина М.А. Административные реформы в Индии // Труды Института государства и права РАН. 2019. Том 14. № 1. С. 166–190.
314. Шулакова А.А. Значение государственных услуг в реализации основных прав человека // Вопросы управления. № 3 (9). 2014. С. 38–45.
315. Щербович А.А. Конституционное право на доступ к Интернету: мировой опыт и выводы для России // Копирайт. 2015. № 3. С. 57–70.
316. Abu-Shanab E., Harb Y. E-government research insights: Text mining analysis // Electronic Commerce Research and Applications. 2019.
317. Albataineh, H., Nijim, M. Enhancing the Cybersecurity Education Curricula Through Quantum Computation. In: Daimi, K., Arabia, H.R., Deligiannidis, L., Hwang, MS., Tinetti, F.G. (eds) Advances in Security, Networks, and Internet of Things. Transactions on Computational Science and Computational Intelligence. Springer, Cham. 2021.
318. Alvares C. et al. Media in Europe: New questions for research and policy // Strasbourg: European Science Foundation ESF, 2014.
319. Aneesh A. Technologically Coded Authority: The Post-Industrial Decline in Bureaucratic Hierarchies, 2002.
320. Autin J.L. Autorités administratives indépendantes, démocratie et État de droit // Droit et société. 2016. № 93. P. 285–295.
321. Bach-Golecka D. The Emerging Right to Good Governance // American Journal of International Law. 2018. 112. P. 89-93.
322. Barbas S. From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption // Buffalo Law Review. 2013. Vol. 61. P. 1119–1189.
323. Barkow R.E. The Ascent of the Administrative State and the Demise of Mercy // Harvard Law Review. Vol. 121. 2008. P. 1332–1365.
324. Bartholomae F.W., Nam Ch.W., Steinhoff P. Does Federalism Affect E-Government in Germany? // CESifo Working Paper. 2023. № 10260.
325. Bender B., Heine M. Government as a Platform? Constitutive Elements of Public Service Platforms. In: Kö A., Francesconi E., Kotsis G., Tjoa A.M., Khalil I. (eds) Electronic Government and the Information Systems Perspective. Springer. 2021. Vol. 12926. P. 3–20.

326. Brilingaitė A., Bukauskas L., Juozapavičius A., Kutka E. Overcoming information-sharing challenges in cyber defence exercises // *Journal of Cybersecurity*. Volume 8. Issue 1. 2022. URL: <https://academic.oup.com/cybersecurity/article/8/1/tyac001/6516499> (дата обращения: 15.05.2023).
327. Brown A. et al. Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: Towards a Platform Assessment Framework (PAF) // *Government Information Quarterly*. 2017. Issue 34. P. 167–182.
328. Chevallier J. Autorités administratives indépendantes et État de droit // *Civitas Europa*. 2016. Vol. 37. № 2. P. 143-154;
329. Chevallier J. Le Défenseur des droits: unité ou diversité? // *Revue française d'administration publique*. 2011/3. № 139. P. 433 - 445.
330. China. Ministry of Industry and Information Technology. URL: http://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm (дата обращения: 05.03.2023).
331. Dapel M.E., Asante M., Uba C.D., Agyeman M.O. Artificial Intelligence Techniques in Cybersecurity Management. In: Jahankhani, H. (eds) *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*. Springer, Cham. 2023.
332. Dawes S.S., Vidiasova L., Parkhimovich O. Planning and designing open government data programs: An ecosystem approach // *Government Information Quarterly*. 2016. Volume 33. Issue 1. P. 15-27.
333. Dykstra J., Gordon L.A., Loeb M.P., Zhou L. Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments // *Journal of Cybersecurity*. Volume 9. Issue 1. 2023. URL: <https://academic.oup.com/cybersecurity/article/9/1/tyad003/7100879> (дата обращения: 06.03.2023).
334. Friedman B. Lawless Surveillance // *New York University Law Review*. 2022. Vol. 97. P. 1143 – 1214.
335. Harrison T.M., Pardo T.A., Cook M. Creating open government ecosystems: a research and development agenda // *Future Internet*. 2012. № 4(4). P. 900–928.
336. Hetcher S. The De Facto Federal Privacy Commission // *Marshall J. Computer & Info. L.* V. 19. Issue 1. 2000. P. 109–132. URL: <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1152&context=jitpl> (дата обращения: 05.03.2023).
337. Janssen M., Estevez E. Lean government and platform-based governance—Doing more with less // *Government Information Quarterly*. 2013. Issue 30. P. S1–S8.
338. Joinson A.N., Paine C., Buchanan T., Reips U. Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom // *Journal of Information Science*. 2006. № 32 (4). P. 334 – 343.

339. Killingsworth S. Minding Your Own Business: Privacy Policies in Principle and in Practice // *Journal of Intellectual Property Law*. 1999. Vol. 7. Issue 1. P. 56–97.
340. Lonergan E.D., Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation // *Journal of Cybersecurity*. Volume 9. Issue 1. 2023. URL: <https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988> (дата обращения: 05.05.2023).
341. Lowens E. Accuracy Is Not Enough: The Task Mismatch Explanation of Algorithm Aversion and Its Policy Implications // *Harvard Journal of Law & Technology*. 2020. Vol. 34. № 1. P. 259–278.
342. Mason S. Electronic Signatures in Practice // *J. High Tech L*. 2006. 148. P. 149–164.
343. Napoli P. Qu'est-ce qu'une mesure de police? Considérations historiques après Gênes 2001 // *Multitudes*, 2003/1. № 11. P. 49-56.
344. Nugraha Y., Martin A. Cybersecurity service level agreements: understanding government data confidentiality requirements // *Journal of Cybersecurity*. Volume 8. Issue 1. 2022. URL: <https://academic.oup.com/cybersecurity/article/8/1/tyac004/6588067> (дата обращения: 06.03.2023).
345. O'Reilly T. Government as a Platform // *innovations*. 2010. Vol. 6. № 1. P. 13–40.
346. Oakley K. The Limit Does Not Exist: How Smartphone Technology Expands Electronic Monitoring and a Proposed Limitation // *Harvard Journal of Law & Technology*. 2022. Volume 36. № 1. P. 263–289.
347. Perri 6 Should We Be Compelled to Have Identity Cards? Justifications for the Legal Enforcement of Obligations // *Political Studies*. 2005. № 53. P. 243–261.
348. Pouillaude H.-B. L'échange des données publiques entre administrations // *Le droit administratif au défi du numérique*. AFDA. 2019. P. 25–42.
349. Reichel J. Regulating Automation of Swedish Public Administration // *CERIDAP. Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*. 2023. № 1. P. 75–94.
350. Selbst A.D. An Institutional View of Algorithmic Impact Assessments // *Harvard Journal of Law & Technology*. 2021. Volume 35. № 1. P. 117–191.
351. Singapore. Ministry of communications and information. Agencies. URL: <https://www.mci.gov.sg/agencies> (дата обращения: 05.03.2023).
352. Smorgunov L. Government as a Platform: Critics of a Technocratic Culture of Public Governance in Digital Era. In: Alexandrov D., Boukhanovsky A., Chugunov A., Kabanov Y., Koltsova O., Musabirov I. (eds) *Digital Transformation and Global Society*. DTGS 2019. Communications in Computer and Information Science. Springer. 2019. Vol. 1038. P. 41-54.
353. Snider K.L.G., Shandler R., Zandani S., Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies // *Journal of Cybersecurity*. Volume 7. Issue 1. 2021. URL:

- <https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745> (дата обращения: 06.03.2023).
354. Solove D.J., Hartzog W. The FTC and the New Common Law of Privacy // *Columbia Law Review*. Vol. 114. 2014. P. 583–676.
355. Sullivan C. The United Kingdom Identity Cards Act 2006 – Civil or Criminal? // *International Journal of Law and Information Technology*. 2006. № 3 (15). P. 320–361.
356. Sun P.-L. et al. An implementation framework for E-Government 2.0. // *Telematics and Informatics*. 2015. Issue 32. P. 504–520.
357. Sunstein C. R. The Office of Information and Regulatory Affairs: Myths and Realities Article // *Harvard Law Review*. Vol. 126. №. 7. 2013. P. 1838-1878.
358. Thomas Ph. A. Identity Cards // *Modern Law Review*. 1995. I. 58. № 5. P. 702–713.
359. Vanlandingham K.E. Municipal Home Rule in the United States // *William & Mary Law Review*. 1968. Vol. 10. Issue 2. P. 269–314.
360. Volokh H.M. The Two Appointments Clauses: Statutory Qualifications for Federal Officers // *Journal of Constitutional Law*. 2008. Vol. 10. № 4. P. 745–789.
361. Youssef M. Here’s Your Number, Now Please Wait in Line: The Asylum Backlog, Federal Court Litigation, and Artificial Intelligence in Agency Adjudication // *The University of Chicago Law Review*. 2022. Vol. 89.8. P. 2013–2066.

Иные источники

362. Департамент информационных технологий города Москвы. URL: <https://www.mos.ru/dit/> (дата обращения: 05.03.2023).; Министерство информационного развития и связи Пермского края. URL: <https://mirs.permkrai.ru> (дата обращения: 05.03.2023).
363. Дмитрий Чернышенко: Разработка стратегии отрасли связи на базе современных и надёжных решений позволит России обеспечить свой технологический суверенитет. URL: <http://government.ru/news/48031/> (дата обращения: 16.05.2023). Дата опубликования: 18.03.2023.
364. Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2020 год. URL: <https://ombudsmanrf.org/storage/74a0484f-7d5a-4fe4-883d-a1b5ba1dd5f8/documents/ezhagodnye-doklady/docs/doklad2020.pdf> (дата обращения: 06.03.2023).
365. Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2021 год. URL: <https://ombudsmanrf.org/storage/74a0484f-7d5a-4fe4-883d-a1b5ba1dd5f8/documents/14493f2b-4975-49d0-86dd-c9ac917436fe/0447a931-4bc9-4ceb-ae92-b32f8d741412.pdf> (дата обращения: 06.03.2023).
366. Доклад о правоприменительной практике организации и проведения федерального государственного контроля (надзора) за обработкой

- персональных данных в 2021 году (Приложение № 2 к Приказу Роскомнадзора от 31.03.2022 № 55). URL: https://rkn.gov.ru/docs/doklad_po_pravoprimereniju_2022_PD.pdf (дата обращения: 05.03.2023).
367. Интернет-омбудсмен. URL: <https://www.iombudsman.ru/about/> (дата обращения: 06.03.2023).
368. Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р). URL: <http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf> (дата обращения: 05.05.2023).
369. Минстрой России. Базовые и дополнительные требования к умным городам (стандарт «Умный город»). Опубликовано: 4 марта 2019 г. URL: <https://minstroyrf.gov.ru/docs/18039/> (дата обращения: 05.03.2023).
370. Минцифры России. Уведомления Госуслуг и оплата штрафов ГИБДД теперь доступны ВКонтакте. 18.01.2023. URL: <https://digital.gov.ru/ru/events/42384/> (дата обращения: 05.03.2023).
371. Молодёжный цифровой омбудсмен. Первый ЦифроЗащитник российской молодёжи. URL: <https://www.youthombudsman.ru/team> (дата обращения: 06.03.2023).
372. Новости Государственного Совета Российской Федерации. URL: <http://www.kremlin.ru/events/state-council/page/2> (дата обращения: 05.03.2023).
373. Обзор правоприменительной практики контрольно-надзорной деятельности в 2017 году (утвержден Приказом Роскомнадзора от 19.02.2018 № 31). URL: <https://rkn.gov.ru/p582/p984/> (дата обращения: 05.03.2023).
374. Обзор правоприменительной практики контрольно-надзорной деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2019 год (утвержден Приказом Роскомнадзора от 28.02.2020 № 25). URL: https://rkn.gov.ru/docs/obzor_2019_1.pdf (дата обращения: 05.03.2023).
375. Обзор правоприменительной практики контрольно-надзорной деятельности в 2020 году (утвержден Приказом Роскомнадзора от 26.02.2021 № 19). URL: https://rkn.gov.ru/docs/obzor_pravoprimerenija_2020.pdf (дата обращения: 05.03.2023).
376. Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года. URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 06.03.2023).
377. Описание сервиса GOV.UK VERIFY на официальном сайте. URL: <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify> (дата обращения: 05.03.2023).
378. Официальная страница Комитета Государственной Думы по информационной политике, информационным технологиям и связи. URL:

- <http://www.komitet4-4.km.duma.gov.ru/Polozhenie> (дата обращения: 05.03.2023).
379. Официальная страница Комитета Совета Федерации по конституционному законодательству и государственному строительству. URL: <http://legislation.council.gov.ru> (дата обращения: 05.03.2023).
380. Официальная страница описания сервиса «service public d'identité numérique». URL: <https://france-identite.gouv.fr/questions-frequentes/> (дата обращения: 05.03.2023).
381. Официальный сайт FCDO. URL: <https://www.cdo.gov/about-agency-cdos/> (дата обращения: 05.03.2023).
382. Письмо Роскомнадзора от 07.12.2021 № 08-82967 «О государственном контроле (надзоре) за обработкой персональных данных» // СПС «КонсультантПлюс».
383. Письмо Роскомнадзора от 19.10.2021 № 08-71063 «О разъяснении законодательства» // СПС «КонсультантПлюс»;
384. Правила и процедуры работы в Единой системе межведомственного электронного взаимодействия по Методическим рекомендациям версии 3.XX. URL: https://info.gosuslugi.ru/docs/section/СМЭВ_3/ (дата обращения – 26.10.2023).
385. Президент РФ. О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства. 20 мая 2022 года. URL: <http://www.scrf.gov.ru/council/session/3241/> (дата обращения: 05.03.2023).
386. Протокол заседания совета по вопросам распространения социальной рекламы в информационно-телекоммуникационной сети «Интернет» от 22.12.2022. URL: <https://digital.gov.ru/ru/documents/8623/> (дата обращения: 05.03.2023).
387. РБК. Путин призвал сделать Россию одним из мировых центров «больших данных». 01.03.2018. URL: <https://www.rbc.ru/rbcfreenews/5a97d1bd9a79476b19eab85c> (дата обращения: 12.05.2023)
388. Регламент обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде (версия 3.5) от 30.05.2013. URL: <https://smev.gosuslugi.ru/portal/> (дата обращения – 28.05.2023).
389. Роскомнадзор. Доклад о видах государственного контроля (надзора) в 2021 году. URL: https://rkn.gov.ru/plan-and-reports/reports/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 05.03.2023).
390. Роскомнадзор. Разъяснения: Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве. URL: <https://pd.rkn.gov.ru/library/p195/> (дата обращения: 06.03.2023).

391. Сборник лучших муниципальных практик по итогам 2021 года. URL: <https://russiasmartcity.ru/documents> (дата обращения: 05.03.2023).
392. Соглашение об информационном обмене между Министерством промышленности и торговли Российской Федерации и Федеральной таможенной службой (Заключено в г. Москве, 26.08.2009 № 01-12/0026, № ХВ-9888/07) // СПС «КонсультантПлюс».
393. Соглашение о взаимодействии при обеспечении предоставления государственных услуг и исполнении государственных функций в электронном виде (Заключено в г. Москве 13.04.2011 № ИЩ-П13-8684) // СПС «КонсультантПлюс».
394. Состоялось заседание Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности. 19 апреля 2023 года. URL: <http://www.scrf.gov.ru/news/allnews/3476/> (дата обращения: 05.03.2023).
395. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения». 12 ноября 2018 г. URL: <http://www.fsb.ru/fsb/npd/more.htm%21id%3D10437602%40fsbNpa.html> (дата обращения: 06.03.2023).
396. Тасс. Путин считает, что нужно вывести на качественно новый уровень эффективность управления. 16.03.2023. URL: <https://tass.ru/ekonomika/17284875> (дата обращения - 12.05.2023);
397. Управление информационных и коммуникационных технологий. URL: <https://udprf.ru/content/upravlenie-informacionnyh-i-kommunikacionnyh-tehnologiy> (дата обращения: 05.03.2023).
398. Управление информационных технологий и связи Исполнительного комитета г. Казани. URL: <https://kzn.ru/meriya/ispolnitelnyy-komitet/uits/> (дата обращения: 05.03.2023).
399. ФСТЭК России. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Национальные стандарты. Обновлено: 19 февраля 2015 г. URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty> (дата обращения: 06.03.2023).
400. IQ городов. Проект «Умный город». URL: <https://russiasmartcity.ru/iq#statistics> (дата обращения: 05.03.2023).
401. About What Works Cities. URL: <https://whatworkscities.bloomberg.org/about/> (дата обращения: 05.03.2023).
402. American Data Privacy and Data Protection Act. Draft Legislation. Section by section summary. URL: <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50> (дата обращения: 08.08.2022).

403. Assemblée nationale. Commission des affaires économiques. URL: [https://www2.assemblee-nationale.fr/15/commissions-permanentes/commission-des-affaires-economiques/\(block\)/54070](https://www2.assemblee-nationale.fr/15/commissions-permanentes/commission-des-affaires-economiques/(block)/54070) (дата обращения: 08.08.2022).
404. Assemblée nationale. Rapport d'information sur l'identité numérique. 08.07.2020. URL: https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/115b3190_rapport-information#_Toc256000062 (дата обращения: 05.03.2023).
405. Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public. October 04, 2022. URL: <https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/> (дата обращения: 06.03.2023).
406. Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public. October 04, 2022. URL: <https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/> (дата обращения: 05.03.2023).
407. Cabinet du Président de la République. URL: <https://www.elysee.fr/la-presidence/cabinet-du-president-de-la-republique-et-services-de-l-elysee> (дата обращения: 05.03.2023).
408. CDOC. Recommendations for improving the methods to access and share data within and between agencies. 2022. URL: https://resources.data.gov/resources/2021_DS WG%20Recommendations_and_Findings_508/ (дата обращения: 05.03.2023).
409. CIO Council - CISO Committee. URL: <https://www.cio.gov/about/members-and-leadership/ciso-council/> (дата обращения: 05.03.2023).
410. CIO Council - CISO Committee. URL: <https://www.cio.gov/about/members-and-leadership/ciso-council/> (дата обращения: 06.03.2023).
411. Citizencard. URL: <https://www.citizencard.com/about-us> (дата обращения: 05.03.2023).
412. Closing the Data Gap: How Cities Are Delivering Better Results for Residents. June 30, 2021. URL: <https://results4america.org/tools/closing-the-data-gap-how-cities-are-delivering-better-results-for-residents/#:~:text=Public%20engagement%3A%20The%20percentage%20of,from%2018%25%20to%2067%25> (дата обращения: 05.03.2023).
413. CNIL, Rapport annuel, 2021. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf (дата обращения: 05.03.2023).
414. Coalition letter to President Bush urging him to reject National ID Card, February 11, 2002. URL: <https://www.aclu.org/legal-document/coalition-letter-president-bush-urging-him-reject-national-id-card?redirect=technology-and->

- liberty/coalition-letter-president-bush-urging-him-reject-national-id-card (дата обращения: 05.03.2023).
415. Collectivités locales : bénéficiez d'outils digitaux de diagnostics pour la réalisation de vos projets. URL: <https://www.banquedesterritoires.fr/solutions-diagnostic-gestion-territoriale-collectivites> (дата обращения: 05.03.2023).
416. Communiqué de presse du Conseil des ministres du 18 juillet 2001. URL: <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000017759386/> (дата обращения: 06.03.2023).
417. Daubresse M.-Ph., de Belenet A. et Durain J. La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance. Rapport d'information, fait au nom de la commission des lois. № 627 (2021-2022). 10 mai 2022. URL: <http://www.senat.fr/notice-rapport/2021/r21-627-notice.html> (дата обращения: 05.03.2023).
418. Défenseur des droits. Le rapport d'activité de l'année 2021. URL: <https://www.defenseurdesdroits.fr/fr/dossier-de-presse/2022/07/rapport-annuel-dactivite-2021> (дата обращения: 06.03.2023).
419. DHS Announces Extension of REAL ID Full Enforcement Deadline. Release Date: April 27, 2021 [Электронный ресурс]. URL: <https://www.dhs.gov/real-id/news/2021/04/27/dhs-announces-extension-real-id-full-enforcement-deadline> (дата обращения: 05.03.2023).
420. Electronic Privacy Information Center. Real ID Implementation Review: Few Benefits, Staggering Costs. Analysis Of The Department Of Homeland Security's National ID Program. May, 2008. URL: https://epic.org/privacy/id_cards/epic_realid_0508.pdf (дата обращения: 05.03.2023);
421. En croisant les données, le Loiret identifie les zones accidentogènes de son réseau routier. Publié le 9 mars 2021. URL: <https://www.banquedesterritoires.fr/en-croisant-les-donnees-le-loiret-identifie-les-zones-accidentogenes-de-son-reseau-routier> (дата обращения: 05.03.2023).
422. Etude sur les plateformes téléphoniques de quatre services publics : 40% des appels n'aboutissent pas. 26 Janvier 2023. URL: <https://www.defenseurdesdroits.fr/fr/a-la-une/2023/01/etude-sur-les-plateformes-telephoniques-de-quatre-services-publics-40-des-appels> (дата обращения: 06.03.2023).
423. EU-U.S. Privacy Shield Framework Principles. Issued by the U.S. Department of Commerce. URL: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> (дата обращения: 06.03.2023).
424. European Commission. E-Government in Austria, January 2015, Edition 18.0. URL: https://joinup.ec.europa.eu/sites/default/files/document/2015-03/egov_in_austria_-_january_2015_-_v_18_0_final.pdf (дата обращения: 05.03.2023).
425. European Commission. E-Government in Germany, February 2016, Edition 18.0. URL: <https://joinup.ec.europa.eu/sites/default/files/inline->

- files/eGovernment%20in%20Germany%20-%20February%202016%20-%202018_00%20-%20v2_00.pdf (дата обращения: 05.03.2023).
426. Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems. URL: <https://science.house.gov/hearings/exploring-cyber-space-cybersecurity-issues-for-civil-and-commercial-space-systems> (дата обращения: 08.08.2022).
427. France services : les services publics près de chez vous ! URL: <https://www.economie.gouv.fr/particuliers/france-services#> (дата обращения: 06.03.2023). Дата опубликования: 06.09.2022.
428. France transfert. URL: <https://www.numerique.gouv.fr/outils-agents/france-transfert/> (дата обращения: 05.03.2023).
429. FTC Report to Congress on Privacy and Security. A Report to Congress. September 13, 2021. URL: https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (дата обращения: 05.03.2023).
430. FTC. In the Matter of Everalbum, Inc. 06.05.2021. URL: <https://www.ftc.gov/enforcement/cases-proceedings/1923172/everalbum-inc-matter> (дата обращения: 06.03.2023).
431. FTC. In the Matter of GEOCITIES, a corporation. File № 9823015. 1998. URL: <https://www.ftc.gov/sites/default/files/documents/cases/1998/08/geo-ord.htm> (дата обращения: 06.03.2023).
432. FTC. Privacy Online: a Report to Congress. June, 1998. URL: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> (дата обращения: 06.03.2023).
433. FTC. Privacy Online: Fair Information Practices in The Electronic Marketplace. A Report to Congress. May 2000. URL: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf> (дата обращения: 06.03.2023).
434. India. Council of Ministers. URL: <https://www.india.gov.in/my-government/whos-who/council-ministers> (дата обращения: 05.03.2023).
435. India. Ministry of communications. URL: <https://dot.gov.in/vision-mission> (дата обращения: 05.03.2023).
436. India. Ministry of electronics & information technology. URL: <https://www.meity.gov.in> (дата обращения: 05.03.2023).
437. Intervention du Président de la République à l'occasion de la convention managériale de l'Etat. URL: <https://www.elysee.fr/emmanuel-macron/2021/04/08/intervention-du-president-de-la-republique-emmanuel-macron-a-loccasion-de-la-convention-managériale-de-letat> (дата обращения: 05.03.2023).
438. Joinup. E-Government in Sweden, February 2016, Edition 18.0. URL: <https://joinup.ec.europa.eu/sites/default/files/inline->

- files/eGovernment%20in%20Sweden%20-%20February%202016%20-%2018_0_v1_00.pdf (дата обращения: 05.03.2023).
439. Le rapport du Défenseur des droits dématérialisation et inégalités d'accès aux services publics. 2022. URL: <https://www.defenseurdesdroits.fr/fr/rapports/2022/02/rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-on> (дата обращения: 06.03.2023).
440. Lyon D. National ID Cards: Crime-Control, Citizenship and Social Sorting // Policing. January 2007. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.605.4170&rep=rep1&type=pdf> (дата обращения: 05.03.2023).
441. Mézard J. Un État dans l'État : canaliser la prolifération des autorités administratives indépendantes pour mieux les contrôler. Rapport № 126 (2015-2016), fait au nom de la CE Autorités administratives indépendantes, déposé le 28 octobre 2015. URL : <http://www.senat.fr/rap/r15-126-1/r15-126-1.html> (дата обращения: 05.03.2023).
442. MyGov: An Overview. URL: <https://www.mygov.in/overview/> (дата обращения: 05.03.2023).
443. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 April 16, 2018. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (дата обращения: 06.03.2023).
444. OECD Recommendation of The Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 23 September 1980. URL: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (дата обращения: 05.03.2023).
445. Osmose, plateforme des communautés professionnelles de l'État. URL: <https://www.numerique.gouv.fr/outils-agents/osmose/> (дата обращения: 05.03.2023).
446. Pallone Applauds Committee Passage of Five Health and Telecommunication Bills. URL: <https://energycommerce.house.gov/newsroom/press-releases/pallone-applauds-committee-passage-of-five-health-and-telecommunication> (дата обращения: 08.08.2022).
447. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Document 52021PC0206. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> (дата обращения: 14.05.2023).
448. Rapport du Conseil national du numérique. Identités numériques. Clés de voûte de la citoyenneté numérique. Juin 2020. URL: <https://cnumerique.fr/files/uploads/2020/2020.06.19.ra-cnum-idnum-web3.pdf> (дата обращения: 25.10.2023).
449. Rabinowicz C. Approaches to Regulating Government Use of Facial Recognition Technology // Harvard Journal of Law and Technology Digest. URL: <https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of->

- facial-recognition-technology (дата обращения: 05.05.2023). Дата опубликования: 04.05.2023.
450. Restatement of the Law, Second, Torts, § 652C. The American Law Institute. 1977. URL: https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (дата обращения: 05.03.2023);
451. Safe Harbor Privacy Principles. Issued by the U.S. Department of Commerce on July 21, 2000. URL: <https://rm.coe.int/16806af271> (дата обращения: 06.03.2023).
452. Sénat. Commission de la culture, de l'éducation et de la communication. URL: <https://www.senat.fr/commission/cult/index.html> (дата обращения: 05.03.2023).
453. Sénat. Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale. URL: <https://www.senat.fr/commission/loi/index.html> (дата обращения: 05.03.2023).
454. Sénat. Groupe Numérique. URL: https://www.senat.fr/groupe-etude/etu_1008.html (дата обращения: 05.03.2023).
455. Senate. List of the committees for the 117th Congress. URL: <https://www.senate.gov/committees/> (дата обращения: 08.08.2022).
456. Senator Blumenthal, et al., Letter to Federal Trade Commission Chair Lina Khan (Sept. 20, 2021). URL: <https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf> (дата обращения: 05.03.2023).
457. Speech by Barry Steinhardt concerning the use of uniform driver's licenses as a national ID, February 10, 2002. URL: <https://www.aclu.org/other/speech-barry-steinhardt-concerning-use-uniform-drivers-licenses-national-id?redirect=technology-and-liberty/speech-barry-steinhardt-concerning-use-uniform-drivers-licenses-national-id> (дата обращения: 05.03.2023);
458. Testimony of Legislative Counsel Katie Corrigan on the Establishment of a National ID Card System Before The House Government Reform Subcommittee on Government Efficiency, Financial Management And Intergovernmental Relations. November 16, 2001. URL: <https://www.aclu.org/other/testimony-legislative-counsel-katie-corrigan-establishment-national-id-card-system-house?redirect=technology-and-liberty/testimony-legislative-counsel-katie-corrigan-establishment-national-id-card-s> (дата обращения: 05.03.2023);
459. The California Department of Technology (CDT). URL: <https://cdt.ca.gov> (дата обращения: 05.03.2023).
460. The City of the New York. Office of the Mayor. Executive order № 3. January 19, 2022 URL: <https://www.nyc.gov/assets/home/downloads/pdf/executive-orders/2022/eo-3.pdf> (дата обращения: 05.03.2023).
461. The New York State Office of Information Technology Services (ITS). URL: <https://its.ny.gov/about-us> (дата обращения: 05.03.2023);
462. The New York State Office of Information Technology Services (ITS). Policies. URL: <https://its.ny.gov/policies> (дата обращения: 05.03.2023).

463. The Parliamentary Ombudsmen (JO). Annual reports. Summary in English of the annual reports. URL: <https://www.jo.se/en/About-JO/Annual-reports/> (дата обращения: 06.03.2023).
464. The Parliamentary Ombudsmen (JO). Decision № 568-2021, 19.06.2022. Swedish Pensions Agency criticised for lack of accessibility and service. URL: <https://www.jo.se/en/> (дата обращения: 06.03.2023).
465. The Parliamentary Ombudsmen (JO). Decision № 961-2020. 28.06.2022. The Swedish Police Authority forcibly photographed a person's motorcycle vest and driving licence with no legal grounds for doing so, thereby violating his right to privacy under Article 8 of the European Convention. URL: <https://www.jo.se/en/> (дата обращения: 06.03.2023).
466. The Prime Minister's Office. Singapore. URL: <https://www.pmo.gov.sg/About-Us> (дата обращения: 05.03.2023).
467. U.S. Dep't of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 41–42. 1973. URL: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> (дата обращения: 05.03.2023).
468. UN E-Government Survey 2022. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%202.pdf> (дата обращения: 05.03.2023).
469. Une plateforme open data au service des agriculteurs en Pays basque. Publié le 18 octobre 2021. URL: <https://www.banquedesterritoires.fr/une-plateforme-open-data-au-service-des-agriculteurs-en-pays-basque-64> (дата обращения: 05.03.2023).
470. Washington Technology Solutions. URL: <https://watech.wa.gov> (дата обращения: 05.03.2023).
471. What is digital citizenship? URL: <https://www.cyberwise.org/digital-citizenship#:~:text=Digital%20Citizenship%2C%20which%20is%20%22the,favor%20of%20positive%20online%20interactions.&text=Our%20mission%20is%20to%20help,and%20wise%20users%20of%20technology> (дата обращения: 25.10.2023).

Приложение. Предлагаемые изменения в Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

- дополнить статью 19 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» частью 4.1 в следующей редакции: «4.1. Государственный орган или орган местного самоуправления вправе ограничить использование предоставленной информации на основании соглашения, заключаемого с пользователем информации, в случаях, если ее распространение может повлечь угрозу причинения ущерба интересам общества, государства и личности»;

- изложить пункт 6 части 1 статьи 20 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» в следующей редакции: «б) в запросе ставится вопрос о правовой оценке актов, принятых государственным органом, органом местного самоуправления, проведении анализа деятельности государственного органа, его территориальных органов, органа местного самоуправления либо подведомственных организаций»;

- дополнить часть 1 статьи 20 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» пунктом 7 в следующей редакции: «7) в запросе ставится вопрос о проведении иной аналитической работы, непосредственно не связанной с защитой прав направившего запрос пользователя информацией, за исключением случаев платного предоставления такой информации»;

- изложить часть 1 статьи 22 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» в следующей редакции: «Плата за предоставление информации о деятельности государственных органов и органов

местного самоуправления взимается в случае ее предоставления по запросу, если объем запрашиваемой и полученной информации превышает определенный Правительством Российской Федерации объем информации, предоставляемой на бесплатной основе, либо в случае необходимости проведения дополнительной аналитической работы. Порядок взимания платы устанавливается Правительством Российской Федерации»;

- дополнить статью 22 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» частью 5 в следующей редакции: «5. Государственный орган или орган местного самоуправления вправе определить размер платы за предоставление информации в случаях, если поиск необходимой информации требует дополнительной аналитической работы, в соответствии с порядком взимания платы, определяемом Правительством Российской Федерации».