МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Борисов Михаил Анатольевич

Правовое регулирование допуска и доступа к информации в условиях цифровой экономики

специальность 5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук,
доцент Северин В.А.

Москва - 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Возникновение человеческой цивилизации, формирование и развитие общества и государства, напрямую связано с получением и использованием информации. Появление информационных (цифровых) технологий, вычислительной техники и информационно-телекоммуникационных сетей позволило обрабатывать информацию в больших объёмах и получать неограниченный доступ к ней. В современном информационном обществе существует сложная дилемма: с одной стороны необходимо обеспечить свободный поиск, получение и использование информации (идей, знаний и т.п.), а с другой стороны обеспечить информационную безопасность личности, общества и государства, что становится возможным только путём правового регулирования порядка допуска и доступа к информации.

В Российской Федерации принята национальная программа "Цифровая экономика Российской Федерации"[1], реализация которой, предполагает ускоренный переход к новой экономической формации, основанной на повсеместном использовании информационных технологий.

Однако формирование единого информационно-правового пространства отстаёт от развития цифровых технологий, в результате чего в должной мере не обеспечивается правовое регулирование инновационных процессов информатизации. С упрочением позиций науки информационного права, определившей основную часть регулирования общественных отношений в информационной среде, все более отчётливо проявляется тенденция к исследованию в качестве самостоятельной проблемы вопросов доступа к

[1] Постановление Правительства РФ от 02.03.2019 № 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации") // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1119.

информации, к разработке ключевых аспектов развития правового института допуска и доступа к информации в современных условиях.

Переход России к цифровой экономике привел к накоплению большого числа нерешённых проблем в области допуска и доступа к информации, возникновение которых объясняется сложным комплексом взаимосвязей государственных и частных интересов, касающихся использования сведений, составляющих государственную тайну, охраны конфиденциальности информации производственно-технического, финансового, коммерческого и иного характера, а также обработки персональных данных. В дополнение обострилось глобальное мировое противостояние, кроме вооружённого конфликта в отношении Российской Федерации ведётся "гибридная война", в период с 17.03.2014 года по 25.02.2023 года принято десять пакетов санкций (более 15 тыс. санкций), которые затронули научные, политические, правовые, экономические сферы деятельности[2] государства, а также отдельных физических и юридических лиц.

Действующие законы и подзаконные акты, разрабатываемые проекты нормативных правовых актов в рассматриваемой области информационного права зачастую не учитывают возникающие коллизии с правовыми нормами других отраслей права, с установленными техническими требованиями в сфере информационных технологий, с устоявшимися обычаями делового оборота в информационной сфере. Также в указанных правовых актах отмечается отсутствие разнообразия в использовании терминов и определений, зачастую и их вольное толкование, что влечёт за собой правовую неопределённость при урегулировании допуска и доступа к информации в условиях цифровой экономики и, соответственно, тормозит развитие цифровой экономики России.

Подобная тенденция в определенной мере сохраняется и после принятия Национальной программы "Цифровая экономика", что требует концептуального переосмысления и укрепления действующего механизма правового регулирования отношений в области допуска и доступа к информации современных условиях.

---

[2] Анализ НП "ЦМАПК" "Наука, технологии, высокотехнологичное оборудование" // URL: http://www.forecast.ru.

Всё вышеизложенное определило актуальность выбранной темы настоящего диссертационного исследования в целях совершенствования законодательства в области допуска и доступа к информации, а также развития науки информационного права.

Степень научной разработанности темы. Изучение материалов исследования показывает, что определенный опыт теоретического анализа вопросов правового регулирования в области допуска и доступа к информации в Российской Федерации имеется. Значительное количество публикаций посвящено отдельным вопросам правового регулирования отношений в сфере доступа субъектов к информации, в области информационной безопасности, обеспечения безопасности информации, защиты государственной, служебной и коммерческой тайны, правового регулирования персональных данных.

Эти проблемы в разное время в той или иной мере исследовались в работах многих ученых, в частности: А.Б. Агапова[3], И.Л. Бачило[4], Ю.М. Батурина[5], М.А. Вуса[6], А.С. Дёмушкина[7], Т.Д. Зражевской[8], В.А. Герасименко[9], О.А. Городова[10], В.А. Копылова[11], П.У. Кузнецова[12], А.П. Курило[13], В.Н. Лопатина[14], В.А. Мазурова[15], А.В. Минбалеева[16], А.А. Малюк[17],

---

[3] Агапов А.Б. Основы федерального информационного права России. М.: Экономика, 1995. 230 с.

[4] Бачило И.Л. Информационное право: учебник для академического бакалавриата. 5-е изд. пер. и доп. М.: Юрайт, 2019. 419 с.

[5] Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991. 272 с.

[6] Информационное общество: Информационные войны. Информационное управление. Информационная безопасность. / Под ред. М.А. Вуса. СПб.: СПбГУ, 1999. 212 с.

[7] Дёмушкин А.С. Документы и тайна. М.: Городец, 2003. 400 с.

[8] Зражевская Т.Д., Савченко С.А. Воздействие конституционного законодательства на формирование правовой системы России // Вестник ВГУ. Серия: Право. 2011. № 1 (10).

[9] Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997. 537 с.

[10] Городов О.А. Информационное право. 2-е изд. М.: Проспект, 2018. 304 с.

[11] Копылов В.А. Информационное право. 2-е изд., перераб. и доп. М.: Юристъ, 2005. 512 с.

[12] Информационные технологии в юридической деятельности: учебник для академического бакалавриата / П.У.Кузнецов [и др.]. / Под общ. ред. П.У.Кузнецова. 3-е изд., перераб. и доп. М.: Юрайт, 2018. 325 с.

[13] Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой И.А. Основы управления информационной безопасностью. М.: Горячая линия - Телеком, 2013. 244 с.

[14] Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство / МВД России, Санкт-Петербургский ун-т. СПб.: Университет, 2000. 424 с.

[15] Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. М.: Палеотип, 2002. 148 с.

А.В. Морозова[18], Т.А. Поляковой[19], И.М. Рассолова[20], В.А. Северина[21], А.А. Стрельцова[22], А.А. Тедеева[23], Л.К. Терещенко[24], А.А. Фатьянова[25], Д.С. Черешкина[26], В.И. Ярочкина[27] и других учёных.

Объектом диссертационного исследования являются отношения в области информационного права, складывающиеся в процессе допуска и доступа к информации в условиях "цифровой экономики".

Предметом диссертационного исследования являются нормы информационного права, регулирующие вопросы допуска и доступа к охраняемой законом информации в условиях цифровой экономики.

Цель диссертационного исследования заключается в рассмотрении особенностей допуска и доступа к информации как категории информационного права, а также в разработке научно обоснованных положений, выводов и

---

[16] Минбалеев А.В. Правовое регулирование рекламной деятельности: учебное пособие для студентов вузов, обучающихся по специальности 030501 "Юриспруденция" / Под ред. В.В.Кваниной. М.: Юриспруденция, 2010. 223 с.

[17] Малюк А.А., Королёв В.И., Фомичёв В.М. Введение в информационную безопасность: Учебное пособие для вузов / Под ред. В.С.Горбатова. М.: Горячая линия - Телеком, 2011. 288 с.

[18] Морозов А.В. Проблемы правового регулирования цифровых технологий в России и за рубежом // Вестник университета имени О.Е.Кутафина (МГЮА), 2019, № 12. С. 170-172.

[19] Цифровая трансформация: вызовы праву и векторы научных исследований: монография [Электронный ресурс] / Под общ. ред. А.Н.Савенкова, / Отв. ред. Т.А.Полякова, А.В.Минбалеев. Электрон. дан. (1,3 Мб). М.: Институт государства и права РАН, 2020.

[20] Рассолов И.М. Информационное право: учебник и практикум для академического бакалавриата. 5-е изд., перераб. и доп. М.: Юрайт, 2017. 347 с.

[21] Северин В.А. Комплексная защита информации на предприятии: Учебник для вузов / Под ред. проф. Б.И.Пугинского. М.: Городец, 2008. 368 с.; Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право, 2016. № 4. С. 13-19.

[22] Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Под ред. Т.А.Поляковой, А.А.Стрельцова. М.: Юрайт, 2016. 325 с.

[23] Информационное право: учебник для бакалавриата, специалитета и магистратуры / М.А.Федотов, А.А.Тедеев [и др.] / Под ред. М.А.Федотова. М.: Юрайт, 2019. 497 с.

[24] Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: ИНФРА-М, 2016. 227 с.

[25] Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие. М.: Юрист, 2001. 412 с.

[26] Смолян Г.Л., Черешкин Д.С. О формировании информационного общества в России. // Информационное общество. Вып. 6, 1998. С. 8-13.

[27] Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. 2-е изд. М.: Академический Проект, Гаудеамус, 2004. 544 с.

рекомендаций, направленных на совершенствование правовых норм, регулирующих вопросы допуска и доступа субъектов к охраняемой законом информации в условиях цифровой экономики. Достижению указанной цели служит решение следующих **задач**:

- выявление сущности правового режима допуска и доступа к информации в условиях формирующейся "цифровой экономики";

- установление современного состояния правового регулирования допуска и доступа к информации в условиях перехода к "цифровой экономике";

- определение путей модернизации правового регулирования допуска и доступа к информации в условиях "цифровой экономики".

Теоретическая основа диссертационного исследования представлена результатами исследований, проведённых не только в праве, но и в других отраслях знаний, прежде всего информационных технологий.

Нормативную основу настоящей диссертации образуют положения Конституции Российской Федерации, федеральные законы и подзаконные нормативные правовые акты в сфере информационных технологий, законодательные и подзаконные нормативные правовые акты субъектов Российской Федерации в сфере информационных технологий, международные и национальные стандарты в сфере информационных технологий, а также опыт правового регулирования отношений в информационной сфере в зарубежных странах.

Эмпирическая основа диссертационного исследования образована судебными актами Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, материалами отечественной судебной практики. В рамках настоящего исследования также были изучены материалы научных исследований, аналитические и информационные материалы, документы Евразийского экономического союза.

Методологическую основу настоящего диссертационного исследования составляют общенаучные и специально-юридические методы.

Обращение к методам анализа и синтеза позволило на основании изучения обширной интерпретационной практики судебных органов выявить и сформулировать общие характеристики автономного толкования.

Метод формально-юридического анализа с учётом сформулированной темы работы являлся важной частью исследовательского процесса. На основании данного метода осуществлялось разграничение сходных юридических (конституционных) понятий, выявлялись сущностные признаки понятия "автономное толкование" и т.д.

Существенное значение для диссертационного исследования имел и сравнительно-правовой метод, который позволил на основании сопоставления требований различных федеральных законов и подзаконных нормативных правовых актов проанализировать и выявить специфические характеристики автономного толкования исследуемых понятий.

Теоретическая значимость работы состоит в том, что результаты диссертационного исследования могут быть использованы в учебном процессе при преподавании информационного права, а также при подготовке учебно-методических рекомендаций, учебников и пособий по курсу "Информационное право".

Практическая значимость работы заключается в возможности использования её результатов, в процессе совершенствования информационного законодательства, а также их реализации при разработке и принятии соответствующих подзаконных актов в области допуска и доступа к информации в условиях "цифровой экономики".

Научная новизна диссертационной работы определяется тем, что автором выполнено одно из первых комплексных исследований правовой сущности допуска и доступа к информации в условиях цифровой экономики. Автором, проведена унификация терминов и определений, а также представлены предложения по совершенствованию действующих нормативных правовых актов в области допуска и доступа субъектов к информации.

На защиту выносятся следующие, **основные положения диссертационного исследования, являющиеся новыми или обладающие элементами научной новизны**:

1. Установлено, что в условиях цифровой экономики в организациях существует единый подход к порядку допуска и доступа лиц к информации в зависимости от особенностей правового положения обладателей информации и использования информационных (цифровых) технологий, что подтверждает вывод о тенденции нормативно организованной интеграции в единый правовой институт допуска и доступа лиц к информации.

2. Обоснована правовая модель, связанная с формированием отдельного терминологического аппарата для обозначения правовых и технических процессов, протекающих в информационной системе в части допуска и доступа субъектов к информации. Автор доказывает необходимость применения терминов "идентификация" и "аутентификация" вместо терминов "допуск" и "доступ", а также обосновывает применение дополнительных терминов "идентификатор", "уникальный идентификатор", "транзакция", "верификация", "валидация" и "авторизация" для описания процессов допуска и доступа в информационных системах.

3. Предлагается системно рассматривать и классифицировать информацию ограниченного доступа, обрабатываемую вне государственной информационной системы, путём выделения отдельных групп: 1) информация, составляющая государственную тайну; 2) информация, составляющая коммерческую тайну, служебную тайну и иную тайну; 3) информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна); 4) информация о частной жизни гражданина (физического лица), в том числе составляющая личную и семейную тайну (персональные данные). В тоже время, информацию ограниченного доступа, обрабатываемую в государственной информационной системе, с учётом различного правового режима необходимо разделить на две группы:

1) информация, составляющая государственную тайну; 2) информация, составляющая служебную тайну.

4. Показывается, что правовой механизм, оптимизирующий требования к процедуре оформления допуска субъектов (физических лиц) к государственной и служебной тайне непосредственно связан с использованием государственных информационных систем и базируется на использовании информационных технологий.

5. Обосновывается вывод о необходимости расширения категории лиц, за счёт физических лиц, допускаемых или допущенных к сведениям, составляющим государственную тайну, в отношении которых по запросу предоставляются сведения о проведённых медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты, в том числе и наличия медицинских показаний и медицинских противопоказаний.

6. Доказана необходимость отнесения информации, относящейся к персональным данным и обрабатываемой в государственных информационных системах "Единая информационная система персональных данных Российской Федерации" и "Федеральная база данных геномной информации", к сведениям, составляющим государственную тайну, с установлением соответствующего правового режима в целях обеспечения безопасности личности, общества и государства.

Личный вклад автора. Выносимые на защиту результаты получены лично автором.

Достоверность результатов диссертационного исследования подтверждается анализом правового регулирования, российской и зарубежной научной литературы, а также судебной практики в области допуска и доступа к информации.

Апробация результатов диссертационного исследования. Диссертационная работа обсуждена на заседании кафедры Правовой информатики Юридического факультета Московского государственного университета имени М.В. Ломоносова. Результаты диссертационного

исследования получили отражение в шестнадцати научных и учебно-методических работах, в том числе: два учебных пособия, одна монография, восемь статей в научных журналах, четыре доклада на конференциях.

Материалы исследований, а также полученные результаты и выводы используются в учебном процессе на Юридическом факультете Московского государственного университета имени М.В. Ломоносова с 2016 года по магистерской программе "Информационные правоотношения в инновационной экономике". Автор является разработчиком учебных курсов "Защита интересов государства в информационной сфере и инновационная экономика", "Информационное общество и защита персональных данных", "Контроль в сфере обращения с информацией".

Структура диссертации обусловлена предметом, целями и задачами исследования и состоит из введения, трёх глав, которые включают десять параграфов, заключения, списка использованной литературы и нормативных правовых актов, двух приложений к диссертационной работе, в одном из которых проанализированы основные виды конфиденциальной информации, принятые в законодательстве Российской Федерации, а в другом - представлен перечень предложений по совершенствованию (изменению / уточнению) нормативных правовых актов Российской Федерации.

ГЛАВА 1. СУЩНОСТЬ ПРАВОВОГО РЕЖИМА ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

1.1. Предпосылки влияния цифровой экономики на развитие информационных отношений в России

Переживаемое в последнее время развитие информационного общества, связанно с появлением и существенным развитием трансграничных глобальных информационно-телекоммуникационных сетей, охватывающих все страны и континенты, проникающие в каждый дом и воздействующие одновременно как на каждого человека в отдельности, так и на огромные массы людей, что даёт возможность к практически неограниченному доступу к информации. В результате чего современное информационное общество развивается по двум взаимоисключающим направлениям.

С одной стороны, для успешного развития мирового сообщества необходимо:

- устранить все межгосударственные барьеры на пути достижения равноправного доступа к информации для осуществления деятельности в области экономики, в социальной сфере, политике, здравоохранении, культуре, образовании и науке;

- упростить доступ к информации, являющейся публичным достоянием, в том числе путём обеспечения универсального дизайна и использования ассистивных технологий;

- обеспечить каждому представителю мирового сообщества свободу поиска, получения, передачи и использования информации (идей, знаний и т.п.) для создания, накопления и распространения знаний;

- соблюсти принципы свободы печати и свободы информации, а также независимости, плюрализма и разнообразия средств массовой информации, которые являются основной составляющей информационного общества;

- обеспечить информационную и кибербезопасность глобальных информационно-телекоммуникационных сетей, а также аутентификацию, защиту неприкосновенности частной жизни и прав потребителей.

Как видно из вышеизложенного, в настоящее время развитие мирового сообщества пошло по пути создания единого открытого информационного пространства, которые отражены в "Окинавской хартии глобального информационного общества"[28] (принята на о. Окинава 22.07.2000), Декларации принципов "Построение информационного общества - глобальная задача в новом тысячелетии"[29] (принята в гор. Женева 12.12.2003) и "Программе для информационного общества"[30] (принята в гор. Тунис 15.11.2005), а также в "Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы"[31].

С другой стороны, необходимо обеспечить надёжную защиту национальных интересов в информационной сфере, в частности:

- обеспечить закрытость информационного (медийного) пространства Российской Федерации от деятельности радикальных общественных объединений и группировок, использующих националистическую и религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций (в том числе действующих под крылом различных специальных служб отдельных государств), финансовых и экономических структур, а также частных лиц, направленной на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование "цветных революций", разрушение традиционных российских духовно-нравственных ценностей;

---

[28] Дипломатический вестник. 2000. № 8. С. 51-56.

[29] URL: http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf.

[30] URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf.

[31] Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901.

- обеспечить устойчивую и бесперебойную работу критической информационной инфраструктуры Российской Федерации[32] в мирное время, в период непосредственной угрозы агрессии и в военное время;

- доводить до российской и международной общественности достоверную информацию о государственной политике Российской Федерации и её официальной позиции по социально значимым событиям в стране и мире, исключив подмену информации (ввод заведомо ложной информации) со стороны специальных служб ряда иностранных государств;

- эффективно противодействовать компьютерной преступности, прежде всего в кредитно-финансовой сфере, в защите конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;

- обеспечить защиту информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счёт повышения защищённости соответствующих информационных технологий;

- активно развивать национальную систему управления российским сегментом сети "Интернет"[33];

- способствовать развитию искусственного интеллекта в системе государственного управления Российской Федерации[34];

- соблюдать баланс между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере.

---

[32] Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // "Собрание законодательства РФ", 31.07.2017, № 31 (ч. I), ст. 4736.

[33] Постановление Правительства РФ от 15.04.2014 № 313 "Об утверждении государственной программы Российской Федерации "Информационное общество" // "Собрание законодательства РФ", 05.05.2014, № 18 (ч. II), ст. 2159.

[34] Указ Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // "Собрание законодательства РФ", 14.10.2019, № 41, ст. 5700.

Вышеуказанные требования по обеспечению надёжной защиты национальных интересов в информационной сфере изложены в "Стратегии национальной безопасности Российской Федерации"[35], в "Доктрине информационной безопасности Российской Федерации"[36], целом ряде нормативно-правовых актов Российской Федерации, в руководящих документах Федеральной службы безопасности Российской Федерации, Службы внешней разведки Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также в рекомендациях Межведомственной комиссии по защите государственной тайны.

В декабре 2016 года Президент РФ в послании к Федеральному собранию предложил запустить в Российской Федерации "Программу цифровой экономики"[37]. При этом глава государства подчеркнул, что в то же время в цифровых технологиях кроются значительные риски. Подобные программы принимаются и в других государствах[38].

Впервые концепцию "цифровой экономики" в 1995 году сформулировал американский информатик Массачусетского университета США Николас Негропонте[39]. До настоящего времени мировое сообщество не выработало единого понимания "цифровой экономики", основные направления её дальнейшего развития только формируются[40]. Так, в научной литературе применяются следующие термины: "сетевая экономика" (англ. "network economy"), "цифровая экономика" (англ. "digital economy"), "электронная

---

[35] Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (ч II), ст. 5351.

[36] Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.

[37] URL: http://tass.ru/ekonomika/3830997.

[38] Например, Декрет Президента Республики Беларусь от 21.12.2017 № 8 "О развитии цифровой экономики" // URL: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716.

[39] Матвеев И.А. Электронная экономика: сущность и этапы развития // Управление экономическими системами: электронный научный журнал. 2012. Вып. 6 (42).

[40] Лапидус Л.В. Эволюция цифровой экономики // Ежегодная Международная Научная конференция Ломоносовские чтения-2018. Секция экономических наук. "Цифровая экономика: человек, технологии, институты".

экономика" (англ. "electronic economy" или "e-Economy"), "виртуальная экономика" (англ. "virtual economy"), которые в том числе содержат и разные определения.

В Российской Федерации под "цифровой экономикой" понимается хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объёмов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг[41].

В настоящее время внесены изменения в п. "м" ст. 71 Конституции РФ, которой "оборот цифровых данных" отнесён к ведению Российской Федерации. При этом необходимо отметить, что действующее законодательство не содержит определение "цифровые данные". В тоже время обычаи делового оборота под "цифровыми данными" понимают любую информацию, обрабатываемую средствами вычислительной техники.

Анализ показывает, что мировым сообществом, включая Россию, намечен ряд основных направлений развития "цифровой экономики"[42] (см. рисунок 1.1), к которым относятся:

Рис. 1.1. Направления развития "цифровой экономики" в современный период

[41] Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901.

[42] Доклад о мировом развитии "Цифровые дивиденды". World Bank Group, 2016 // URL: https://openknowledge.worldbank.org/handle/10986/23347.

1) *Развитие "цифровых финансов".* В рамках данного направления осуществляется развитие защищённых онлайн-платежей, мобильных денег и цифровой валюты, которые составляют основу для электронной торговли. Для государства данное направление предоставляет возможность использовать бюджетные средства с меньшими затратами, снижая возможности мошенничества и утечки денежных средств. В ст. 128 Гражданского кодекса РФ (часть первая) "цифровые финансы" (безналичные денежные средства, бездокументарные ценные бумаги) признаются в качестве самостоятельного объекта гражданских прав. Также введено понятие "цифровые права"[43], под которыми понимаются обязательственные и иные права субъектов в инвестиционных платформах[44].

Ряд видных учёных В.В. Блажеева, М.А. Егоровой, Н.Н. Черногора, Д.А. Пашенцева, В.Э. Волкова[45] предлагают отнести "цифровое право" к институту отрасли информационного права, что не лишено оснований, однако автором данный институт информационного права в настоящей диссертационной работе не рассматривается.

При этом необходимо отметить, что информация, содержащая сведения о безналичных (цифровых) денежных средствах несёт не описательный характер, а является самостоятельной единицей учёта (т.н. "токен").

2) *Развитие "социальных сетей".* В современных условиях социальные сети являются основой человеческого общества, в настоящее время более одной пятой всех жителей планеты являются участниками одной или нескольких социальных сетей. Социальные сети способствуют выгодному с экономической точки зрения взаимодействию, делают поведение пользователей соответствующим интересам развития, становятся базой для сбора и распространения информации при стихийных бедствиях и в чрезвычайных ситуациях, а также способствуют вовлечению участников в политическую жизнь и социальным изменениям. В

[43] Ст. 141.1 "Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

[44] Федеральный закон от 02.08.2019 № 259-ФЗ "О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 05.08.2019, № 31, ст. 4418.

[45] Цифровое право : учебник / под общ. ред. В.В.Блажеева, М.А.Егоровой. М.: Проспект, 2020. 640 с.

тоже время, будучи источником инновационных идей, социальные сети также остаются каналом распространения сплетен, клеветы, недостоверной информации, домогательств, издевательств и преступлений.

Необходимо отметить, что в "цифровых сетях" информация циркулирует в двух основных формах:

- первая, описывает какие либо события, мнения субъекта (физического лица), официальной позиции субъекта (юридического лица) и т.д. Также, в последнее время в социальных сетях начинает активно функционировать ещё один субъект, "искусственный интеллект", в качестве создателя рекламы, формовщика ленты новостей, контекстной рекламы, бот-чатов, формировщика психологического портрета (определения предпочтений) физических лиц и т.п.;

- вторая, осуществляет сбор формализованных данных о деятельности субъекта (например, данные о посещении определённых информационных ресурсов, геоданные и т.п.), которые несут функцию самостоятельного предмета (товара), т.н. "цифровые права".

3) *Развитие "цифровой идентификации"*. В рамках данного направления осуществляется развитие различных систем подтверждения подлинности субъектов, например, различные электронные системы удостоверения личности, биометрические системы идентификации и т.п. Данные системы применяются для осуществления безопасных банковских операций, голосования, доступа к социальным услугам, оплаты коммунальных платежей, осуществления различных видов государственных и частных транзакций (электронных договоров) и т.п. В рамках данного направления формируется уникальный набор данных каждого субъекта. Для субъекта – физического лица, указанный набор данных входит в понятие "персональные данные". Для субъектов – юридического лица, а в перспективе и искусственного интеллекта, действующее законодательство не предусматривает название для данного набора данных. Таким образом, как покажет последующее исследование, целесообразно понятие "персональные данные" распространить на всех субъектов "цифровой экономики".

4) *Развитие "революции данных"*. В рамках данного направления осуществляется развитие двух взаимосвязанных инноваций – "большие данные" и "открытые данные". Большие данные отличаются огромными объёмами, скоростью передачи и поступают из бесчисленного числа источников, как правило, применяются для совершенствования планирования транспортных потоков, оценки укрупнённых макроэкономических показателей (т.н. "сверхкраткое прогнозирование"), отслеживания хода распространения эпидемий, совершенствования оценки заёмщиков, подбора работы и др. Открытые данные – это данные, находящиеся в свободном и беспрепятственном доступе, машиночитаемые и доступные для использования без каких-либо ограничений. Как правило, большие данные и открытые данные формируются государственными структурами и крупными компаниями (корпорациями).

В настоящее время мировое сообщество, в том числе и Российская Федерация, ускоренными темпами переходят в новую экономическую формацию, основанную на повсеместном использовании информационных технологий[46], однако в силу объективной реальности формирование единого информационно-правового пространства отстаёт от развития "цифровых технологий", в результате чего в должной мере не обеспечивается "правовое обеспечение процессов информатизации"[47].

При этом необходимо учитывать, что вид (формат) информации отличается в зависимости от характера её обработки: непосредственно в информационной системе и вне информационной системы (см. рисунок 1.2).

Анализ работ видных учёных, а также действующих нормативных правовых актов позволяет сделать вывод, что информация, обрабатываемая вне информационной системы, как правило, рассматривается в качестве вспомогательной (описательной) конструкции, характеризующей предмет права, а

[46] Полякова Т.А., Бойченко И.С. Информационная безопасность через призму национального проекта "Цифровая экономика": правовые проблемы и векторы решений // Право и государство. 2019. № 2. С. 97-100; Полякова Т.А., Минбалеев А.В. Цифровые инновации и проблемы развития механизма правового регулирования в России // Информационное право. 2019. № 4. С. 12-15.

[47] Указ Президента РФ от 28.06.1993 № 966 "О Концепции правовой информатизации России" // "Собрание актов Президента и Правительства РФ", 05.07.1993, № 27, ст. 2521.

субъекты разделяются на физических, юридических лиц и государство, обладающих самостоятельной правоспособностью.

Рис. 1.2. Понятие информации в современных условиях

В тоже время, информация, обрабатываемая непосредственно в информационной системе, рассматривается в качестве самостоятельного предмета правоотношений, при этом непосредственно в информационной системе выделение субъекта не представляется возможным. В информационной системе под субъектом понимается "процесс"[48], при этом не важно, какая информационная система его инициировала: физического, юридического лица или государства.

Как правило, подзаконные нормативные правовые акты указанную особенность не учитывают, что влечёт за собой правовую неопределённость при урегулировании допуска и доступа субъектов к информации в условиях "цифровой экономики".

Необходимо отметить, что это общая проблема, касающаяся всех государств, занимающихся развитием цифровой экономики, и её решение видится в необходимости разработки актуальной нормативной правовой базы, а также обеспечения профессиональной компетентности работников, предпринимателей и государственных служащих, работающих в информационной сфере.

[48] Межгосударственный стандарт. "ГОСТ 28270-89 (ИСО 8211-85). Системы обработки информации. Спецификация файла описания данных для обмена информацией" (утв. Постановлением Госстандарта СССР от 27.09.1989 № 2942) // М.: Стандартинформ, 2006.

Указанный выше вид (формат) информации нашёл отражение в национальной программе "Цифровая экономика Российской Федерации[49]", где выделены девять "сквозных цифровых технологий": большие данные, квантовые технологии, компоненты робототехники и сенсорика, нейротехнологии и искусственный интеллект, новые производственные технологии, промышленный Интернет, системы распределённого реестра, технологии беспроводной связи, технологии виртуальной и дополненной реальностей.

Вокруг перечисленных "сквозных цифровых технологий" планируется выстраивать меры поддержки и информационного обеспечения. Одной из мер поддержки является цифровая трансформация государственного управления путём создания "цифрового правительства" (англ. "digital government") на принципах "гибкого управления" (англ. "agile management"), что предполагает внедрение цифровых платформ, систем и облачных решений в государственном управлении и предоставлении государственных услуг:

- электронные государственные услуги, оказываемые "проактивно", в том числе на основе биометрической аутентификации, электронной подписи и "цифрового профиля" граждан и юридических лиц;

- единый электронный документооборот[50] и согласование в государственных органах;

- единая система генерируемых ими данных[51];

- автоматизация контрольной (надзорной) деятельности на основе анализа рисков по большим данным с объектов проверок[52];

---

[49] Постановление Правительства РФ от 02.03.2019 № 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации") // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1119.

[50] "Концепция развития электронного документооборота в хозяйственной деятельности" (утверждена решением президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 25.12.2020 № 34) // URL: https://www.nalog.gov.ru.

[51] Постановление Правительства РФ от 22.06.2021 № 956 "О государственной информационной системе "Цифровая аналитическая платформа предоставления статистических данных" (вместе с "Положением о государственной информационной системе "Цифровая аналитическая платформа предоставления статистических данных") // "Собрание законодательства РФ", 28.06.2021, № 26, ст. 4979.

- единое окно цифровой обратной связи и др.

Таким образом, по мере развития "цифровой экономики" постоянно будут появляться новые виды (форматы) информации, что, безусловно, должно учитываться в процессе совершенствования законодательства и практики применения в области допуска и доступа субъектов к информации, циркулируемой в информационных системах, обеспечивающих потребности "цифровой экономики".

1.2. Правовое понятие информации в современный период

В основе рассматриваемых правоотношений находится информация, понятие "информация" является краеугольным камнем в системе информационного права.

В Российской Федерации предусмотрено несколько определений понятия "информация":

1) В гражданском обороте (в толковом словаре русского языка) под "информацией" понимаются "сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством[53]", либо "сведения независимо от формы их представления[54]".

2) В юридическом обороте (в нормативных актах) под "информацией" понимаются "сведения (сообщения, данные) независимо от формы их представления[55]", "компьютерная информация – информация, находящаяся в

---

[52] Федеральный закон от 31.07.2020 № 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации" // "Собрание законодательства РФ", 03.08.2020, № 31 (ч. I), ст. 5007.

[53] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И. Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

[54] Глоссарий по информационному обществу. / М.Р.Когаловский [и др.]. / Под общ. ред. Ю.Е.Хохлова. М.: Институт развития информационного общества, 2009. 160 с.

[55] Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[56]".

3) В обороте информационных технологий (в "цифровой экономике") под "информацией" понимаются некие "знания о предметах, фактах, идеях и т.д., которыми могут обмениваться люди в рамках конкретного контекста[57]", либо "абсолютное значение разности предельных значений геометрического параметра[58]", либо "сообщение (информация) – блок информации, передаваемый от отправителя к получателю[59]".

Необходимо отметить, что в международных нормативных документах, регулирующих правоотношения в информационной сфере, вместо понятия "информация" применяется более широкое понятие "актив (англ. "asset") – что-либо, что имеет ценность для организации[60]", а также понятие "информационный актив (англ. "information asset") – знания или данные, которые имеют значение для организации[61]", как элемент массива информации введено понятие "данные (англ. "data") – предоставление информации в формальном виде, пригодном для

---

[56] Ст. 1 "Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации" (Заключено в гор. Минске 01.06.2001) // Бюллетень международных договоров. 2009. № 6. С. 12-17.

[57] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 10746-2-2000. Информационная технология. Взаимосвязь открытых систем. Управление данными и открытая распределённая обработка. Часть 2. Базовая модель" (утв. Постановлением Госстандарта РФ от 26.12.2000 № 413-ст) // М.: ИПК Издательство стандартов, 2001.

[58] Международный стандарт. "ГОСТ ISO/IEC 17067-2015. Оценка соответствия. Основные положения сертификации продукции и руководящие указания по схемам сертификации продукции" (утв. Приказом Росстандарта РФ от 24.12.2015 № 2199-ст) // М.: Стандартинформ, 2016.

[59] Межгосударственный стандарт. "ГОСТ 30721-2020 (ISO/IEC 19762:2016). Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь" (утв. Приказом Росстандарта РФ от 22.10.2020 № 660-ст) // М.: Стандартинформ, 2020.

[60] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. Приказом Росстандарта РФ от 19.12.2006 № 317-ст) // М.: Стандартинформ, 2007.

[61] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология" (утв. Приказом Росстандарта РФ от 19.05.2021 № 392-ст) // М.: Стандартинформ, 2021.

передачи, интерпретации или обработки людьми или компьютерами[62]". Для значительных объёмов данных дополнительно введено такое понятие как "большие данные (англ. "big data") – структурированная и (или) неструктурированная информация определённого объёма и многообразия, эффективно обрабатываемая исключительного программными инструментами с возможностью горизонтального масштабирования[63]".

Как видно из вышеизложенного, единого определения понятия "информация" не существует – термин имеет различные значения в различных областях профессиональной деятельности. В рамках информационного права понятие "информация" на протяжении своей эволюции претерпевало ряд изменений. Так, в период с 1995 по 2006 годы под "информацией" понимались – "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления[64]". В действующем Законе об информации термин получил более широкое определение "сведения (сообщения, данные) независимо от формы их представления[65]". Расширение определения информации позволило раздвинуть границы его применения, включив туда формы информации, которые возможно возникнут в будущем. Однако действующая в настоящее время легальная дефиниция информации не учитывает различия между понятиями "сведения", "данные" и "сообщения". В тоже время в условиях "цифровой экономики" мы всё чаще будем пользоваться понятиями, принятыми в информационных технологиях, а в данной области указанные понятия разграничиваются по разным категориям:

Сведения – это информация, рассматриваемая в содержательном аспекте, т.е. безотносительно к её восприятию и использованию.

---

[62] Межгосударственный стандарт. "ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии. Словарь" (утв. Приказом Росстандарта РФ от 22.09.2016 № 1189-ст) // М.: Стандартинформ, 2016.

[63] Min Chen, Shiwen Mao, Yin Zhang, Victor C.M. Leung. Big Data. Related Technologies, Challenges, and Future Prospects. Spinger, 2014. 100 p. (определение адаптировано диссертантом).

[64] Ст. 2 Федерального закона от 20.02.1995 № 24-ФЗ "Об информации, информатизации и защите информации" // "Собрание законодательства РФ", 20.02.1995, № 8, ст. 609.

[65] Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

Сообщение – это информация, рассматриваемую в коммуникативном аспекте, т.е. как обмен сведениями, часть процесса общения между пользователями, например "последовательность битов или символов, которая передаётся как объект[66]".

Данные – это предоставление информации в формальном виде, пригодном для передачи, интерпретации или обработки людьми или компьютерами, а также позволяют идентифицировать субъекта (например, блогера, техническое устройство и т.п.).

С развитием информационных технологий появилось отдельное понятие данных – "токен – это единица учёта, которая используется для представления цифрового баланса в некотором активе[67]". Токены представляют собой запись в регистре, распределённую в блокчейн-цепочке. Также они могут выступать в качестве заменителя ценной бумаги[68].

Необходимо обратить внимание, что кроме Закона об информации понятие "информации" трактуют и судебные органы, которые рассматривают информацию "в виде документа, а также устных и письменных пояснений[69]".

Под "документом" действующее законодательство понимает: "материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения[70]", либо "архивный документ, прошедший экспертизу ценности документов, поставленный на государственный учёт и подлежащий постоянному хранению[71]",

---

[66] Межгосударственный стандарт. "ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии. Словарь" (утв. Приказом Росстандарта РФ от 22.09.2016 № 1189-ст) // М.: Стандартинформ, 2016.

[67] URL: https://forklog.com/chto-takoe-token.

[68] Северин В.А., Коржова И.В. Вопросы безопасности при обращении криптовалюты // Вестник Московского университета. Серия 26. Государственный аудит. 2019. № 4. С. 81-89.

[69] Постановление ФАС Волго-Вятского округа от 09.03.2011 по делу № А82-9212/2010 // URL: http://www.consultant.ru.

[70] Ст. 1 Федерального закона от 29.12.1994 № 77-ФЗ "Об обязательном экземпляре документов" // "Собрание законодательства РФ", 02.01.1995, № 1, ст. 1.

[71] Ст. 3 Федерального закона от 22.10.2004 № 125-ФЗ "Об архивном деле в Российской Федерации" // "Собрание законодательства РФ", 25.10.2004, № 43, ст. 4169.

либо "документированная информация, созданная, полученная и сохраняемая организацией или частным лицом в качестве доказательства и актива для подтверждения правовых обязательств или деловой транзакции[72]".

В рамках информационного права, кроме понятия "документа" (документированной информации) законодатель выделяет ещё два понятия, это "электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети" и "электронный документ" – "документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах", или "документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в соответствии с законодательством Российской Федерации[73]", или "документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах[74]".

Как видно из вышеизложенного, в Российском, да и в мировом законодательстве содержится огромное количество форм выражения информации, число которых постоянно увеличивается, что не позволяет дать их исчерпывающий перечень.

В настоящее время научным сообществом и действующим законодательством информация рассматривается в двух основных состояниях:

---

[72] Национальный стандарт РФ. "ГОСТ Р ИСО 15489-1-2019. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы" (утв. Приказом Росстандарта РФ от 26.03.2019 № 101-ст) // М.: Стандартинформ, 2019.

[73] П. 1.4 "Порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа", утверждённого Приказом Судебного департамента при Верховном Суде РФ от 27.12.2016 № 251 // "Бюллетень актов по судебной системе", № 2, февраль, 2017.

[74] Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

1) Информация – как нечто не определённое, не подлежащее систематизации и классификации (регламентации)[75].

2) Информация – как товар, продукция, предмет труда и объект услуг, подлежащая систематизации и классификации (регламентации)[76].

В целом, автор поддерживает высказанное мнение ученых, но считает, что по мере развития в Российской Федерации "цифровой экономики" доля информации, которая является товаром (предметом труда, объектом услуг), будет только расти[77]. Так как "цифровая экономика" предполагает активное использование информационных систем[78], искусственного интеллекта[79], электронного документооборота[80] и баз данных[81], то использование информации без её систематизации просто невозможно.

Таким образом, видится необходимость в проведении необходимых институциональных изменений с целью унификации терминологического

---

[75] Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. / Под ред. В.А.Садовничего и В.П.Шерстюка. М.: МЦНМО, 2002. 296 с.

[76] Постановление Правительства РФ от 25.12.2009 № 1088 "О государственной автоматизированной информационной системе "Управление" (вместе с "Положением о государственной автоматизированной информационной системе "Управление") // "Собрание законодательства РФ", 04.01.2010, № 1, ст. 101.

[77] Указ Президента РФ от 07.05.2018 № 204 "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" // "Собрание законодательства РФ", 14.05.2018, № 20, ст. 2817.

[78] Постановление Правительства РФ от 27.01.2022 № 60 "О мерах по информационному обеспечению контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, по организации в ней документооборота, о внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившими силу актов и отдельных положений актов Правительства Российской Федерации" // "Собрание законодательства РФ", 07.02.2022, № 6, ст. 872.

[79] Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // "Собрание законодательства РФ", 14.10.2019, № 41, ст. 5700.

[80] Постановление Правительства РФ от 22.09.2009 № 754 "Об утверждении Положения о системе межведомственного электронного документооборота" // "Собрание законодательства РФ", 28.09.2009, № 39, ст. 4614; Постановление Правительства РФ от 15.02.2022 № 172 "О государственной информационной системе "Типовое облачное решение системы электронного документооборота" (вместе с "Положением о государственной информационной системе "Типовое облачное решение системы электронного документооборота") // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1178; Постановление Правительства РФ от 02.03.2022 № 279 "О государственной информационной системе "Платформа "Центр хранения электронных документов" // "Собрание законодательства РФ", 07.03.2022, № 10, ст. 1532.

[81] Ищейнов В.Я. Организация доступа сотрудников к конфиденциальным массивам электронных документов и базам данных. // Делопроизводство. 2018. № 1. С. 63-65.

аппарата "информации" в нормативно-правовых актах с учётом развития "цифровой экономики" в России. Необходимо отметить, что в настоящее время в направлении унификации терминологического аппарата "информации" движется нормотворчество большинства зарубежных государств[82].

1.3. Содержание информационных прав субъектов в условиях формирования цифровой экономики

В Конституции Российской Федерации[83] определены субъекты конституционного права, под которыми понимаются носители конституционных прав и конституционных обязанностей. Применительно к информационной сфере можно выделить группы субъектов права, которые обладают соответствующими полномочиями в процессе обращения информации в силу Конституции РФ и федеральных законов[84]:

1) Физические лица – граждане Российской Федерации, иностранцы, лица с двойным гражданством (бипатриды), лица без гражданства (апатриды), избиратели и депутаты как лица со специальной правоспособностью и их группы.

2) Государственные образования – Российская Федерация в целом, субъекты Российской Федерации (республики, края, области, города федерального значения, автономная область и автономные округа), органы государственного управления на федеральном уровне и на уровне субъектов федерации, государственные предприятия и учреждения.

3) Негосударственные объединения (общности людей) – народ Российской Федерации, народы субъектов Российской Федерации, население

---

[82] "Протокол обозначений маркировки конфиденциальной информации" (англ. Traffic Light Protocol). Официальный сайт Департамента внутренней безопасности США. // URL: https://www.us-cert.gov/tlp; Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27010-2020. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности при обмене информацией между отраслями и организациями" (утв. Приказом Росстандарта РФ от 10.11.2020 № 1041-ст) // М.: Стандартинформ, 2020.

[83] "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) // "Собрание законодательства РФ", 04.08.2014, № 31, ст. 4398.

[84] Новицкий В.А. Теория российского процессуального доказывания и правоприменения: Монография. Ставрополь: Изд-во СГУ, 2002. 584 с.

административно-территориальных единиц и муниципальных образований, органы местного самоуправления, ассоциации граждан (политические партии, массовые общественные организации, религиозные объединения, общественно-политические движения и др.), группы граждан (собрания избирателей, сходы граждан и др.), частные коммерческие и некоммерческие организации.

Рассмотрим подробнее отдельные названные группы.

Регулирование права физических лиц (граждан Российской Федерации) на информацию в конституционном законодательстве является трудной задачей, так как только на конституционном уровне это право рассматривается более чем в двадцати конституционно-правовых установлениях, а на более широком – законодательном уровне, по оценкам специалистов, в этот институт входят нормы свыше трёх десятков законодательных актов[85]. Впервые в Российской Федерации право человека и гражданина на информацию было закреплено в ст. 9 и 13 "Декларации прав и свобод человека и гражданина"[86] в виде права на охрану личной, персональной информации и права на получение общедоступной информации.

В Конституции РФ закреплены права граждан на информацию, причём перечень прав адресован не только физическим лицам, но и их объединениям – юридическим лицам, что вытекает из Постановления Конституционного Суда РФ[87]. Конституционные права, связанные с обращением информации предоставляются физическим и юридическим лицам в самых разных сферах их жизнедеятельности:

---

[85] Хургин В.М. Право на доступ к информации, или Как (и чем) сражаться с бюрократом // Информационное общество. 2001. № 4. С. 35-43.

[86] Постановление ВС РСФСР от 22.11.1991 № 1920-I "О Декларации прав и свобод человека и гражданина" // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 26.12.1991, № 52, ст. 1865.

[87] Постановление Конституционного Суда РФ от 18.07.2012 № 19-П "По делу о проверке конституционности части 1 статьи 1, части 1 статьи 2 и статьи 3 Федерального закона "О порядке рассмотрения обращений граждан Российской Федерации" в связи с запросом Законодательного Собрания Ростовской области" // "Собрание законодательства РФ", 30.07.2012, № 31, ст. 4470; Постановление Конституционного Суда РФ от 03.02.1998 № 5-П "По делу о проверке конституционности статей 180, 181, пункта 3 части 1 статьи 187 и статьи 192 Арбитражного процессуального кодекса Российской Федерации" // "Собрание законодательства РФ", 09.02.1998, № 6, ст. 784.

- право на ознакомление с законодательными актами (ч. 3 ст. 15 Конституции РФ);

- право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23 Конституции РФ);

- право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ);

- право каждого знакомиться с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ч. 2 ст. 24 Конституции РФ);

- право на свободу мысли и слова (ч. 1 ст. 29 Конституции РФ);

- право на свободу выражения своих мнений и убеждений (ч. 3 ст. 29 Конституции РФ);

- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29 Конституции РФ);

- право на свободу массовой информации (ч. 5 ст. 29 Конституции РФ);

- право граждан обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления (ст. 33 Конституции РФ);

- право на доступ к информации о фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей (ч. 3 ст. 41 Конституции РФ);

- право каждого на достоверную информацию о состоянии окружающей среды (ст. 42 Конституции РФ);

- право на свободу всех видов творчества (ч. 1 ст. 44 Конституции РФ);

- право на свободу преподавания (ч. 1 ст. 44 Конституции РФ);

- право на доступ к культурным ценностям (ч. 2 ст. 44 Конституции РФ);

- право на судебную защиту прав и свобод (ч. 1 ст. 46 Конституции РФ);

- право на получение квалифицированной юридической помощи (ст. 48 Конституции РФ).

В указанном перечне необходимо выделить следующие статьи Конституции РФ: ст. 29, предусматривающую возможность широкой реализации права на информацию в обществе и государстве[88], ст. 33, определяющую условия реализации права на доступ к информации, ч. 3 ст. 41 и ст. 42, являющихся продолжением сущности права на доступ к информации, ч. 1 и 2 ст. 44, закрепляющую права на интеллектуальную собственность, полученную в результате творчества, доступ к культурным ценностям.

В свою очередь Конституцией РФ на органы государственного управления возложены следующие функции по обеспечению вышеуказанных прав граждан и организаций, такие как:

- обязанность по предоставлению возможности ознакомления гражданина с общедоступной информацией, а также с информацией, затрагивающей его права и свободы (ч. 3 ст. 15, ч. 2 ст. 24, ч. 4 и 5 ст. 29, ст. 33, ч. 3 ст. 41, ст. 42 Конституции РФ);

- обязанность по предоставлению информации, раскрывающую деятельность органов государственного управления (ч. 2 ст. 24 Конституции РФ);

- обязанность по защите информации, относящейся к гражданину (ч. 1 и 2 ст. 23 Конституции РФ);

- обязанность по ограничению доступа к информации, относящейся к тайне, либо к нежелательной для распространения информации (ч. 2 и 4 ст. 29 Конституции РФ).

Нужно отметить, что в ходе развития "цифровой экономики" происходит изменения регламентации информационного статуса субъектов информационного права и формирование новых прав и обязанностей в сфере обращения информации по следующим основным направлениям[89]:

1) "*Обеспечение открытости и гласности в деятельности органов и учреждений публичной власти*", которая достигается путём формирования

---

[88] Авакьян С.А. Конституционное право России: Учебный курс. В 2-х томах. Том 1. М.: Юристъ, 2005. 617 с.

[89] Кудрявцев М.А. Информационные права личности: проблема институциональных гарантий // Конституционное и муниципальное право. 2018. № 6. С. 26-30.

"открытого правительства"[90], т.е. системы принципов организации государственного управления, основанной на вовлечении граждан, общественных организаций и бизнес-объединений в принятие и реализацию властных решений. Целью этого вовлечения является повышение качества принимаемых решений и достижение баланса интересов[91]. Доступ к информации осуществляется в электронном виде[92].

2) "*Обеспечение доступа граждан к информации как в частном плане (к личным досье), так и в публичном плане (к официальной или открытой информации)*" – достигается путём формирования системы предоставления государственных и муниципальных услуг федеральными органами исполнительной власти, органами государственных внебюджетных фондов, исполнительными органами государственной власти субъектов Российской Федерации, а также местными администрациями и иными органами местного самоуправления, осуществляющими исполнительно-распорядительные полномочия[93], а также организациями, не входящими в указанный перечень[94]. Доступ к услугам осуществляется в электронном виде[95] через государственные информационные системы.

3) "*Обеспечение защиты тайны частной и семейной жизни от посторонних посягательств*" – достигается путём совершенствования системы ограничений на ознакомление с информацией, касающейся тайны корреспонденции (тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений), тайны голосования, а также права на защиту личности (защиту своего имени, чести, достоинства и деловой репутации,

---

[90] Распоряжение Правительства РФ от 30.01.2014 № 93-р "Об утверждении Концепции открытости федеральных органов исполнительной власти" // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 547.

[91] Указ Президента РФ от 31.12.1993 № 2334 "О дополнительных гарантиях прав граждан на информацию" // "Собрание актов Президента и Правительства РФ", 10.01.1994, № 2, ст. 74.

[92] URL: http://open.gov.ru.

[93] Федеральный закон от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

[94] Распоряжение Правительства РФ от 05.09.2002 № 1227-р "О создании федерального государственного унитарного предприятия "Почта России"" // "Собрание законодательства РФ", 09.09.2002, № 36, ст. 3511.

[95] URL: https://www.gosuslugi.ru, https://www.pochta.ru.

национальной принадлежности, вероисповедания и т.д.[96]) со стороны должностных лиц органов государственной власти при осуществлении запросов в государственной информационной системе, в случаях превышения своих полномочий. Остро стоит проблема ограничения доступа к информации, полученной из камер видеонаблюдения и контроля, т.к. имеют место случаи распространения указанной информации в СМИ (в сети Интернет)[97], т.е. необходимо соблюсти право субъекта на свободу располагать собой (в том числе находиться без контроля с чьей-либо стороны).

4) "*Обеспечение защиты персональных данных*" – достигается путём совершенствования государственных информационных систем сбора и обработки персональных данных[98], с целью унификации обрабатываемых в них персональных данных, а также информации, которая прямо не относится к персональным данным субъекта, но косвенно может иметь экономическое, политическое, информационное и др. значение. К данной информации, как правило, относятся "кук-файлы" (англ. "cookie") – небольшие фрагменты данных, отправленные веб-сервером и хранимые на компьютере пользователя, которые применяются для целей[99]:

- аутентификации пользователя;
- хранения персональных предпочтений и настроек пользователя;
- отслеживания состояния сеанса доступа пользователя;
- ведения статистики о пользователях.

Защита персональных данных, как подтверждают данные исследования, обеспечивается путём совершенствования автоматизированной системы анализа персональных данных, распространяемых порой с нарушением закона, а также

---

[96] Ст. 150, 152.2 "Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

[97] Ст. 152.1 Там же.

[98] Ст. 14, 14.1 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

[99] Macmanus M. A guide to recommender systems. January, 2009 // URL: http://readwrite.com/2009/01/26/recommender_ systems.

своевременного удаления недостоверных или неактуальных персональных данных субъекта, фактически реализуется "право на забвение"[100].

Вместе с гарантированными правами граждан на информацию Конституция РФ предусматривает ограничения информационных прав субъектов, которые базируются на положениях "Всеобщей декларации прав человека[101]", "Конвенции о защите прав человека и основных свобод[102]" и "Международного пакта о гражданских и политических правах[103]".

Вышеуказанные нормативные акты предусматривают ограничения информационных прав субъектов:

- в целях обеспечения должного признания и уважения прав, свобод, интересов и репутации других субъектов;

- в целях охраны здоровья, нравственности и морали демократического общества;

- в интересах защиты конституционного строя, государственной безопасности, территориальной целостности и общественного порядка, а также в целях обеспечения общего благосостояния в демократическом обществе;

- для предотвращения разглашения информации, полученной конфиденциально;

- для обеспечения авторитета и беспристрастности правосудия.

Конституция РФ к основаниям для ограничения основных прав и свобод гражданина относит:

- ограничение прав на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ);

---

[100] Ст. 15.3, 15.5 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

[101] Ч. 2 ст. 29 "Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948) // "Российская газета", № 67, 05.04.1995.

[102] Ч. 2 ст. 8, ч. 2 ст. 9, ч. 2 ст. 10, ч. 2 ст. 11, ч. 1 ст. 15 "Конвенции о защите прав человека и основных свобод" (заключена в гор. Риме 04.11.1950) // "Собрание законодательства РФ", 08.01.2001, № 2, ст. 163.

[103] Ч. 1 ст. 4, 17, 19 "Международного пакта о гражданских и политических правах" (принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // "Бюллетень Верховного Суда РФ", № 12, 1994.

- ограничение прав на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ);

- запрет на пропаганду или агитацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду (ч. 2 ст. 29 Конституции РФ);

- запрет на поиск, получение, передачу, производство и распространение информации, составляющую государственную тайну (ч. 4 ст. 29 Конституции РФ);

- право гражданина не свидетельствовать против себя самого, своего супруга и близких родственников (ст. 51 Конституции РФ);

- ограничение прав и законных интересов других лиц в целях защиты основ конституционного строя, нравственности, здоровья, обеспечение обороны страны и безопасности государства (ч. 3 ст. 55 Конституции РФ);

- возможность ограничения прав и свобод с указанием пределов и сроков их действия в условиях чрезвычайного положения (ст. 56 Конституции РФ).

Как видно из вышеизложенного, ограничения информационных прав субъектов в вышеуказанных международных нормативных актах и в Конституции РФ по своему содержанию совпадают, однако основания ограничения информационных прав субъектов не совпадают. С целью унификации механизма ограничения информационных прав субъектов в 2001 году была предпринята попытка принятия Федерального закона "О праве на информацию в Российской Федерации"[104], однако после первого чтения в Государственной Думе РФ своего дальнейшего развития законопроект не нашёл. Представляется важным с учётом зарубежного опыта и нашей отечественной практики ограничения доступа к информации продолжить работу над законопроектом.

[104] Проект Федерального закона от 15.05.2001 "О праве на информацию в Российской Федерации" // URL: http://docs.cntd.ru/document/901799770.

1.4. Классификация и правовой режим общедоступной информации и информации ограниченного доступа в условиях цифровой экономики

В ст. 5 Закона об информации закреплено положение, согласно которому информация может выступать полноправным объектом любых правоотношений: публичных, гражданских и иных правовых отношений. Однако Закон об информации не даёт определения понятию "иных правовых отношений", что позволяет рассматривать "информацию" как самостоятельный объект в отраслях права, которые относятся к частному праву (предпринимательскому, торговому, семейному и др.), где доминирует гражданское право. Другими словами, в рамках и публичного и частного права, возникают правовые отношения по поводу информации. Любое лицо (субъект) может свободно воспользоваться информацией для своих целей, если федеральными законами не установлены ограничения по доступу к этой информации или иные требования к порядку её предоставления или распространения. Причем неважно, кто является правообладателем информации, информационных ресурсов государство (публичное право) или частная коммерческая организация (частное право). Важно другое, лицо (субъект) должно иметь право доступа к информации на законных основаниях.

Закон об информации классифицирует информацию в зависимости от категории доступа на "общедоступную информацию" и "информацию ограниченного доступа" (см. рисунок 1.3).

К "*общедоступной информации*" относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Определение понятия "общеизвестные сведения" Закон об информации не содержит, однако, по общему правилу, для признания факта общеизвестным требуется, чтобы он был известен широкому кругу лиц, например, составу судей при рассмотрению дела (ч. 1 ст. 61 Гражданского процессуального кодекса РФ, ч. 1 ст. 69 Арбитражного процессуального кодекса РФ, ч. 1 ст. 64 Кодекса административного судопроизводства РФ), либо находился в общедоступных источниках

информации, обладающих достаточной степенью надёжности, например, научные издания, сведения, содержащиеся в общедоступных государственных информационных системах[105] (реестрах), официальная статистическая информация[106] и т.д.

Рис. 1.3. Структура информации в Российской Федерации

Под "иной информацией, доступ к которой не ограничен", вероятней всего следует понимать любую иную информацию, которая была обнародована тем или иным способом её обладателем, либо для неё в силу различных причин установить принадлежность конкретному обладателю не представляется возможным, но не попала в разряд общеизвестных сведений[107].

"Общедоступная информация", в зависимости от порядка её предоставления или распространения и смысла Закона об информации, может подразделяться на следующие категории информации:

---

[105] Официальный сайт: "Единая информационная система в сфере закупок" // URL: https://zakupki.gov.ru/epz/main/public/home.html.

[106] Приказ Росстата РФ от 30.05.2019 № 304 "Об утверждении Официальной статистической методологии формирования отдельных показателей деятельности коллективных средств размещения по полному кругу хозяйствующих субъектов с квартальной периодичностью" // URL: http://www.gks.ru.

[107] Савельев А.И. "Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации" (постатейный)". М.: Статут, 2015. 320 с.

1. "*Свободно распространяемую*"[108] – информацию, перешедшую в общественное достояние[109] (при условии, что доступ к информации не ограничен автором в письменной форме), информация, распространяемая средствами массовой информации[110] (СМИ) (при условии, что издательство, блогер и т.п. зарегистрировано установленным порядком) и т.д.

2. "*Предоставляемую*[111] *по соглашению лиц, участвующих в соответствующих отношениях*" – информацию, опубликованную издательством (СМИ) после заключения договора с автором (в т.ч. за плату), общедоступные источники персональных данных (в различных справочниках, телефонных книгах и т.п.), полученные на основании письменного согласия субъектов персональных данных[112], регистрация субъекта на Интернет-ресурсе и проставления в специальной графе электронной формы "галочки", которая является простой электронной подписью[113] и т.д.

3. "*Которая в соответствии с федеральными законами подлежит предоставлению или распространению*" – информацию, ограничивать распространение которой прямо запрещено ч. 3 ст. 15, ч. 3 ст. 41, ст. 42 Конституции РФ, ч. 4 ст. 8, ч. 5 ст. 10 Закона об информации, ст. 7 Закона о государственной тайне[114], ст. 5 Закона о коммерческой тайне[115], п. 1.3 "Положения о порядке обращения со служебной информацией ограниченного

---

[108] Распространение информации – действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц (п. 9 ст. 2 Закона об информации).

[109] Ст. 1282 "Гражданского кодекса Российской Федерации (часть четвертая)" от 18.12.2006 № 230-ФЗ // "Собрание законодательства РФ", 25.12.2006, № 52 (ч. 1), ст. 5496.

[110] Ст. 1, 8, 25, 38 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации" // "Ведомости СНД и ВС РФ", 13.02.1992, № 7, ст. 300.

[111] Предоставление информации – действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц (п. 8 ст. 2 Закона об информации).

[112] Ст. 8 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3451.

[113] Ст. 5 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи" // "Собрание законодательства РФ", 11.04.2011, № 15, ст. 2036.

[114] Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, стр. 8220-8235.

[115] Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне" // "Собрание законодательства РФ", 09.08.2004, № 32, ст. 3283.

распространения[116]", либо возникает обязанность её предоставления (например, предоставление сведений о доходах государственных служащих и членов их семей по запросу СМИ[117], обязательная публикация сообщений[118], обязанность по предоставлению первичной статистической информации для формирования официальной государственной статистики[119] и др.).

Таким образом, под общедоступной информацией можно понимать информацию, доступ к которой не требует наличия особых привилегий (статуса), а также информацию, которая подлежит раскрытию в соответствии с требованиями законодательства. Однако в условиях развития "цифровой экономики" и распространения Интернет-ресурсов, а также мирового глобального противостояния[120] (ведения "гибридной войны"[121]) ценность общедоступной информации, особенно в части её свободного распространения, существенно снижается ввиду распространения заведомо ложных (фейковых) новостей. В тоже время в условиях экономического противостояния и введения против Российской Федерации "санкций" часть общедоступной информации может быть использована противостоящими государствами для усиления экономического и

---

[116] Постановление Правительства РФ от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности" // "Собрание законодательства РФ", 25.07.2005, № 30 (ч. II), ст. 3165.

[117] Указ Президента РФ от 08.07.2013 № 613 "Вопросы противодействия коррупции" (вместе с "Порядком размещения сведений о доходах, расходах, об имуществе и обязательствах имущественного характера отдельных категорий лиц и членов их семей на официальных сайтах федеральных государственных органов, органов государственной власти субъектов Российской Федерации и организаций и предоставления этих сведений общероссийским средствам массовой информации для опубликования") // "Собрание законодательства РФ", 15.07.2013, № 28, ст. 3813.

[118] Ст. 35 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации" // "Ведомости СНД и ВС РФ", 13.02.1992, № 7, ст. 300.

[119] Ст. 8 Федерального закона от 29.11.2007 № 282-ФЗ "Об официальном статистическом учёте и системе государственной статистики в Российской Федерации" // "Собрание законодательства РФ", 03.12.2007, № 49, ст. 6043.

[120] Борисов М.А. "К вопросу о моделировании системы защиты информации в условиях информационного противоборства". Научный журнал "Вестник РГГУ". Серия "Информатика. Защита информации. Математика". // М.: РГГУ, № 12(55)/10, 2010. С. 285-289.

[121] Гибридная война (англ. "hybrid warfare") – вид враждебных действий, при котором нападающая сторона не прибегает к классическому военному вторжению, а подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойны, а также оказывая поддержку повстанцам, действующим на территории противника (Nicu Popescu. Hybrid tactics: neither new nor only Russian // European Union Institute for Security Studies, January 2015).

политического давления, поэтому исходя из сложившейся общемировой политической и экономической обстановки, доступ к определённой части "общедоступной" информации может быть временно ограничен. Так, в действующее законодательство введено понятие "контрсанкционная информация"[122], ограничения на предоставление финансовой отчётности[123], информации о деятельности акционерных обществ[124], к банковской информации[125].

В связи с усиливающейся конкуренцией в научной деятельности, в развитии инновационных технологий, в Российской Федерации наметилась тенденция к ограничению доступа к результатам научных исследований[126]. Так, определён перечень исследований, утечка о которых может нанести ущерб безопасности государства[127], а также установлены ограничения на публикации в изданиях, индексируемых в Web of Science, Scopus[128].

---

[122] Ст. 21.4 Федерального закона от 08.03.2022 № 46-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 14.03.2022, № 11, ст. 1596.

[123] Постановление Правительства РФ от 18.03.2022 № 395 "Об особенностях доступа к информации, содержащейся в государственном информационном ресурсе бухгалтерской (финансовой) отчётности, и раскрытия консолидированной финансовой отчётности в 2022 году" // "Собрание законодательства РФ", 21.03.2022, № 12, ст. 1877.

[124] Постановление Правительства РФ от 12.03.2022 № 351 "Об особенностях раскрытия и предоставления информации, подлежащей раскрытию и предоставлению в соответствии с требованиями Федерального закона "Об акционерных обществах" и Федерального закона "О рынке ценных бумаг", и особенностях раскрытия инсайдерской информации в соответствии с требованиями Федерального закона "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 21.03.2022, № 12, ст. 1837.

[125] Решение Совета директоров Банка России от 14.04.2022 "О перечне информации кредитных организаций (головных кредитных организаций банковских групп), которую они временно не должны раскрывать" // URL: http://www.cbr.ru; Решение Совета директоров Банка России от 23.12.2022 "Об определении перечня информации кредитных организаций, некредитных финансовых организаций, а также организаций, оказывающих профессиональные услуги на финансовом рынке, подлежащей раскрытию в соответствии с законодательством Российской Федерации или нормативными актами Банка России, которую кредитные организации, некредитные финансовые организации, а также организации, оказывающие профессиональные услуги на финансовом рынке, вправе не раскрывать с 1 января 2023 года до 1 июля 2023 года, и перечня информации, предусмотренной законодательством Российской Федерации или нормативными актами Банка России, которую Банк России вправе не раскрывать на своём официальном сайте в информационно-телекоммуникационной сети "Интернет" с 1 января 2023 года до 1 июля 2023 года" // URL: http://www.cbr.ru.

[126] Борисов М.А. "Проблемы публикационной активности в современных условиях" // "Информационное право", М.: РНИ-ИИС, 2023, № 1 (75), С. 24-27.

[127] Постановление Правительства РФ от 07.10.2021 № 1705 "О едином реестре результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального или двойного назначения и признании

С целью обеспечения доступа субъектов к общедоступной информации в условиях "цифровой экономики" Закон об информации вводит такое понятие как "открытые данные". Под "*открытыми данными*" законодатель понимает "информацию, размещённую в сети "Интернет" в виде систематизированных данных, организованных в формате, обеспечивающем её автоматическую обработку без предварительного изменения человеком, в целях неоднократного, свободного и бесплатного использования", а "открытые государственные данные – открытые данные, опубликованные государственными органами, их территориальными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления"[129].

Суть открытых данных сводится не столько к обеспечению возможности ознакомления с информацией, создаваемой различными субъектами, сколько к предоставлению возможности её дальнейшего использования (анализа, визуализации, модификации под новые приложения и т.д.). Для государственных открытых данных – это придание огромному набору данных[130], которым располагает государство, характера экономического блага для стимулирования экономического роста и развития "цифровой экономики"[131].

В настоящее время "открытые данные" развиваются в концепции развития технологии "больших данных", которая позволяет обрабатывать разносторонние и

утратившими силу некоторых актов Правительства Российской Федерации и отдельного положения акта Правительства Российской Федерации" (вместе с "Правилами формирования и ведения единого реестра результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального или двойного назначения") // "Собрание законодательства РФ", 18.10.2021, № 42, ст. 7118.

[128] Постановление Правительства РФ от 19.03.2022 № 414 "О некоторых вопросах применения требований и целевых значений показателей, связанных с публикационной активностью" // "Собрание законодательства РФ", 28.03.2022, № 13, ст. 2076.

[129] "Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных. Версия 3.0" (утв. протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 № 4) // URL: http://data.gov.ru.

[130] Набор открытых данных (набор данных) – совокупность однородных элементов машиночитаемых данных и описывающей их метаинформации (URL: http://data.gov.ru).

[131] Указ Президента РФ от 07.05.2012 № 601 "Об основных направлениях совершенствования системы государственного управления" // "Собрание законодательства РФ", 07.05.2012, № 19, ст. 2338.

плохо структурированные данные во всё время возрастающих объёмах. Необходимо отметить, что это общемировая тенденция. В настоящее время более пятидесяти государств[132] и межгосударственных образований[133] имеют развитые Интернет-ресурсы "открытых данных".

Обеспечение функционирования "Российского портала открытых данных[134]" возложено на Министерство экономического развития РФ, по состоянию на апрель 2023 года портал содержит порядка тысячи тематических разделов и более пятидесяти тысяч наборов данных, предоставленных различными федеральными и региональными органами власти, структурированных по темам с возможностью поиска по ключевым словам. Порядок формирования набора данных и их формат определяется Правительством РФ[135], в котором выделено три главных условия:

1) Такая информация должна быть размещена её обладателем, в качестве которого выступает соответствующее публично-правовое образование, от имени которого принимается решение об отнесении информации к категории открытых данных соответствующим государственным или муниципальным органом власти в установленном порядке.

2) Информация должна быть размещена в формате, допускающем её последующую обработку без вмешательства человека (например, CSV, XML, JSON, ODS и др.). Данное условие необходимо для обеспечения совместимости таких данных с различными информационными системами для целей их последующего использования самими различными способами.

---

[132] См. Портал открытых данных Австралии // URL: https://data.gov.au; Республики Беларусь // URL: https://opendata.by; Марокко // URL: https://data.gov.ma и др.

[133] "Информационный портал Евразийского экономического союза" // URL: https://portal.eaeunion.org/ru-ru/public/main.aspx.

[134] "Портал открытых данных Российской Федерации" // URL: http://data.gov.ru.

[135] Постановление Правительства РФ от 10.07.2013 № 583 "Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети "Интернет" в форме открытых данных" // "Собрание законодательства РФ", 29.07.2013, № 30 (ч. II), ст. 4107; Распоряжение Правительства РФ от 10.07.2013 № 1187-р "О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети "Интернет" в форме открытых данных" // "Собрание законодательства РФ", 29.07.2013, № 30 (ч. II), ст. 4128.

3) Должно быть описание условий использования набора открытых данных (открытая лицензия на использование наборов открытых данных) и обеспечена возможность визуального просмотра и немедленной загрузки опубликованного набора открытых данных без требований по дополнительной авторизации, прохождения CAPTCHA-теста[136] и иных ограничений.

Вместе с тем необходимо отметить следующие недостатки в построении и функционировании порталов открытых данных, как в Российской Федерации, так и зарубежных государств:

- отсутствует синхронизация разработанных документов по ряду концептуальных вопросов, включая размещение и публикацию открытых данных;

- отсутствует общепризнанный межгосударственный (национальный) стандарт качества наборов данных, в результате чего формируются несовместимые наборы данных (например, CSV-файлы имеют невалидный формат, что нарушает работу поисковых систем, данные фактически выпадают из поиска, также наблюдается разное количество колонок в строках данных для табличных форматов и т.п.);

- огромное количество не актуальных (фактически устаревших) данных, например, на "Российском портале открытых данных" последние данные по "Реестру лицензий на осуществление работ по активному воздействию на гидрометеорологические и геофизические процессы и явления" датированы 15.07.2013 года, что явно указывает на ненадлежащую частоту обмена данными[137]. После публикации[138] автора доступ к указанным данным был ограничен. Данное обстоятельство указывает на отсутствие мотивации государственных служащих к размещению на официальных сайтах государственных органов и органов местного самоуправления информации в форме открытых данных. Учитывая вышеизложенное, можно сделать вывод о

---

[136] Компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером.

[137] URL: https://www.meteorf.gov.ru/opendata/7703092752-reestrav.

[138] Борисов М.А. Правовое регулирование допуска и доступа к информации в условиях цифровой экономики № 20. М.: Ленанд. 2021. 224 с.

том, что "Портал открытых данных" является явлением новым и органы государственного и муниципального управления, как правило, не рассматривают его в качестве площадки влияющей на функционирование "открытого правительства". Данное обстоятельство подтверждается ещё и тем, что вышеуказанная информационная площадка не рассматривается как элемент критической информационной инфраструктуры, требующей внимания[139].

Таким образом, доступ к открытым данным, размещённым на порталах открытых данных, осуществляется без каких-либо ограничений для субъектов (как физических лиц, так и технических устройств). Однако необходимо отметить, что ч. 5 и 6 ст. 8 Закона об информации предусматривает следующие случаи, когда размещение информации в форме открытых данных может быть прекращено:

а) в случае, когда размещение такой информации может повлечь разглашение сведений, составляющих государственную тайну, служебную тайну в области обороны[140], контрсанкционную информацию[141] и др. Основанием для прекращения размещения информации выступает решение органа власти, наделённого полномочиями по распоряжению сведениями, составляющими государственную или иную охраняемую законом тайну. Однако в настоящее время не отработан правовой механизм действий: в случае, если накопится критическая масса открытых данных, поданных различными органами исполнительной власти, которая в своей совокупности станет относиться к государственной тайне, к служебной тайне в области обороны и др.;

б) в случае, когда такое размещение информации может повлечь нарушение права обладателей информации, ограничивших доступ к ней. Основанием для прекращения размещения информации выступает решение суда;

---

[139] Приказ ФСТЭК РФ от 06.12.2017 № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации" // URL: http://www.pravo.gov.ru.

[140] См. ст. 3.1 Федерального закона от 31.05.1996 № 61-ФЗ "Об обороне" // "Собрание законодательства РФ", 03.06.1996, № 23, ст. 2750.

[141] Ст. 21.4 Федерального закона от 08.03.2022 № 46-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 14.03.2022, № 11, ст. 1596.

в) в случае, когда размещение такой информации нарушает права субъектов персональных данных. Основанием для прекращения размещения информации выступает решение суда или Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ, выступающей в качестве уполномоченного органа по защите субъектов персональных данных.

В свою очередь "*к информации ограниченного доступа*" относится информация, в отношении которой федеральными законами установлен либо особый порядок доступа, либо наложен полный запрет на доступ[142]. Цель ограничения доступа к информации – защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Определение понятия "информация ограниченного доступа" Закон об информации не содержит, однако имеется соответствующее определение в Модельном законе о праве на доступ к информации – "информация, доступ к которой ограничен в интересах обеспечения национальной безопасности в соответствии с законодательством о государственных секретах и иными нормативно-правовыми актами, регулирующими отношения в области защиты государственных секретов[143]". Стоит отметить, что приведённое определение информации ограниченного доступа является однобоким и не учитывает все нюансы, которые будут исследованы ниже.

Закон об информации рассматривает ограничение доступа к информации как одно из основных условий её защиты. Для целей защиты информации обязательным является соблюдение её конфиденциальности – "обязательного для выполнения лицом, получившим доступ к определённой информации, требование

---

[142] См. ч. 6, 7 ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448; Приказ ФСБ РФ от 04.11.2022 № 547 "Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации" // URL: http://pravo.gov.ru.

[143] "Модельный закон о праве на доступ к информации" (Принят в гор. Санкт-Петербурге 17.04.2004 Постановлением 23-14 на 23-ем пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств, 2004, № 34. С. 258-270.

не передавать такую информацию третьим лицам без согласия её обладателя". При этом в соответствии с ч. 2 ст. 9 Закона об информации доступ к такой информации должен быть ограничен федеральными законами[144], также Президентом РФ утверждён "Перечень сведений конфиденциального характера[145]", который можно считать исчерпывающим.

Необходимо обратить внимание, что Закон об информации рассматривает понятие "конфиденциальности информации" как правовой режим информации, который характеризуется установленным в силу закона или договора ограниченным доступом к информации и запретом на её передачу третьему лицу без согласия правообладателя[146]. Под третьими лицами следует понимать любое лицо, не являющееся обладателем информации, а также лицом, получившим правомерный доступ к информации. В связи с этим при наличии необходимости предоставления таким лицам информации конфиденциального характера необходимо заручиться заранее выраженным согласием обладателя на её передачу таким лицам, которое может быть выражено как в форме отдельного документа, так и в качестве соответствующего договорного условия. Также имеет место и запрет на распространение вышеуказанной информации.

По сути, в отношении информации, распространение которой в Российской Федерации ограничивается, вводится правовой "режим конфиденциальности информации" по аналогии как "режим секретности" либо "режим коммерческой тайны".

В этой связи необходимо отметить, что действующее законодательство Российской Федерации не содержит такого понятия как "конфиденциальная информация", а соответственно и грифа (пометки) "конфиденциально", проставляемой на документах и изделиях. Однако, в ряде документов такое понятие как "конфиденциальная информация" присутствует, например, в

[144] Ст. 8. Федерального закона от 31.05.2002 № 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" // "Собрание законодательства РФ", 10.06.2002, № 23, ст. 2102.

[145] Указ Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера" // "Собрание законодательства РФ", 10.03.1997, № 10, ст. 1127.

[146] См. Постановление ФАС Московского округа от 12.03.2014 № Ф05-1766/2014 по делу № А40-23492/13-138-219 // URL: http://www.consultant.ru.

национальном стандарте, регламентирующем порядок оформления документов[147], решениях судов[148], а также в ряде нормативных документов различных министерств и ведомств.

Учитывая вышеизложенное, целесообразно в Законе об информации термин "конфиденциальность информации" изложить в следующей редакции – "режим конфиденциальности информации – установленный правовой режим ограничения доступа к информации, предусматривающий ограничение на предоставление указанной информации третьим лицам без письменного согласия правообладателя, а также запрет на распространение указанной информации каким либо образом, если иное не установлено законом".

"Информация ограниченного доступа", в зависимости от порядка её предоставления или распространения, согласно смысла Закона об информации, подразделяется на:

1. "*Распространение которой в Российской Федерации ограничивается*" – информацию, в отношении которой введён особый правовой режим её распространения, как это предусмотрено ч. 3 ст. 55 Конституции РФ. К указанной информации в соответствии со ст. 9 Закона об информации можно отнести, т.н. "виды тайн", которые предлагается[149] разбить на следующие группы (см. приложение 1):

а) "*Информация, составляющая государственную тайну*" – к которой относится информация, изложенная в ст. 5 Закона о государственной тайне[150]. Правообладателем данной информации является Российская Федерация, которая и устанавливает соответствующий порядок её использования. Принадлежность

---

[147] Национальный стандарт РФ. "ГОСТ Р 7.0.97-2016. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов" (утв. Приказом Росстандарта РФ от 08.12.2016 № 2004-ст) // М.: Стандартинформ, 2017.

[148] См. Постановление Президиума ВАС РФ от 15.10.2013 № 7070/13 по делу № А28-770/2002; Постановление Арбитражного суда Московского округа от 27.04.2018 № Ф05-5117/2018 по делу № А40-127318/2017 // URL: http://www.consultant.ru.

[149] Борисов М.А., Северин В.А. К вопросу о совершенствовании системы классификации информации в условиях развития цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2019, № 6. С. 234-237.

[150] Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, стр. 8220-8235.

информации к государственной тайне накладывает достаточно большие ограничения на граждан и организации, которые могут столкнуться с такой информацией в процессе осуществления своей деятельности. Так, должностные лица и граждане должны пройти специальную процедуру допуска к государственной тайне (ст. 21 - 25 Закона о государственной тайне), а юридические лица – получить соответствующую лицензию (ст. 27 Закона о государственной тайне).

Следует отметить, что зарубежное законодательство также содержит такое понятие, как "государственная тайна"[151].

б) "*Информация, составляющая коммерческую тайну, служебную тайну и иную тайну*" – к которой относятся информация, обладающая общим признаком, а именно правообладателем данной информации является создатель указанной информации (например, информация, составляющая коммерческую тайну[152] – это коммерческая организация, а информация, составляющая служебную тайну – орган государственного управления). Необходимо обратить внимание, что требования по технической защите информации, составляющие коммерческую и служебную тайну – идентичны[153].

В настоящее время в российском законодательстве отсутствует федеральный закон, регламентирующий единое понятие "служебная тайна"[154], поэтому пока правоотношения регулируются "Положением о порядке обращения со служебной информацией ограниченного распространения[155]", а также актами

---

[151] См. Закон Новой Зеландии. "Закон об официальных секретах 1951 года" (1951 № 77) // URL: http://www.nzlii.org/nz/legis/hist_act/osa19511951n77183. Аналогичные нормативные акты приняты в КНР, Индии, Ирландии, Мьянме, Малайзии, Сингапуре, Великобритании, Канаде и др.

[152] Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне" // "Собрание законодательства РФ", 09.08.2004, № 32, ст. 3283.

[153] Руководящие документы ФСТЭК РФ. "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" и "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (утв. решением Гостехкомиссии РФ от 30.03.1992) // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty.

[154] Паспорт проекта Федерального закона № 124871-4 "О служебной тайне" // URL: http://sozd.duma.gov.ru.

[155] Постановление Правительства РФ от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти,

федеральных органов власти, принятыми в развитие данного положения. Указанные акты не используют термин "служебная тайна", а оперируют понятием "служебная информация ограниченного распространения – несекретная информация, касающаяся деятельности организаций, ограничения, на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами". Как видно из приведённых положений, возможности уполномоченных должностных лиц по отнесению информации к разряду служебной тайны достаточно широки, поскольку понятие "служебная необходимость" никак не раскрывается в законодательстве и может быть истолковано как угодно широко[156].

Так же "служебной тайне" относится и "служебная тайна в области обороны - сведения, которые образуются при осуществлении полномочий органами государственной власти Российской Федерации[157], функций органами государственной власти субъектов Российской Федерации, органами местного самоуправления и организациями по организации и выполнению мероприятий в области обороны, распространение которых может нанести вред при выполнении указанных мероприятий[158]". Порядок обращения со служебной тайной в области обороны определяется Правительством Российской Федерации[159].

уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности" // "Собрание законодательства РФ", 25.07.2005, № 30 (ч. II), ст. 3165.

[156] Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: Автореферат диссертации кандидата юридических наук. – Москва, 2005.

[157] Приказ Министра обороны РФ от 17.01.2022 № 22 "Об утверждении Перечня сведений Вооружённых Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны"; Приказ МЧС РФ от 29.12.2021 № 940 "Об утверждении Перечня сведений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, подлежащих отнесению к служебной тайне в области обороны"; Приказ Росгвардии РФ от 27.12.2021 № 480 "Об утверждении Перечня сведений Федеральной службы войск национальной гвардии Российской Федерации, подлежащих отнесению к служебной тайне в области обороны" // URL: http://pravo.gov.ru.

[158] Ст. 3.1 Федерального закона от 31.05.1996 № 61-ФЗ "Об обороне" // "Собрание законодательства РФ", 03.06.1996, № 23, ст. 2750.

[159] Постановление Правительства РФ от 26.11.2021 № 2052 "Об утверждении Правил обращения со сведениями, составляющими служебную тайну в области обороны" // "Собрание законодательства РФ", 06.12.2021, № 49 (ч. I), ст. 8241.

К "иной тайне" можно отнести "сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них". Они подлежат государственной защите только после регистрации права федеральным органом исполнительной власти по интеллектуальной собственности[160]. До этого момента все мероприятия по обеспечению конфиденциальности о сущности изобретения, полезной модели или промышленного образца возлагаются на автора, за исключением случая, когда сущность изобретения, полезной модели или промышленного образца относится к государственной тайне[161].

Также к "иной тайне" можно отнести исключительные права на "секрет производства (ноу-хау)" (ст. 1465 Гражданского кодекса РФ (часть четвёртая)) и "служебный секрет производства" (ст. 1470 Гражданского кодекса РФ (часть четвёртая)), которые основываются на фактической монополии обладателя секрета производства и которые достигаются, прежде всего, соблюдением конфиденциальности в отношении охраняемых сведений.

Существенным отличием "секрета производства" от сведений "о сущности изобретения, полезной модели или промышленного образца" является тот факт, что режим конфиденциальности информации в первом случае можно поддерживать в течение всего периода действия "секрета производства" (т.е. когда информация утрачивает свою актуальность). При этом мероприятия по обеспечению конфиденциальности "секрета производства" обеспечиваются силами правообладателя и все риски по разглашению, утрате и хищению информации целиком и полностью лежат на правообладателе.

Что касается "сущности изобретения, полезной модели или промышленного образца", то после регистрации права автора в отношении указанной информации вводится режим патентной охраны, который устанавливает монополию

[160] Постановление Правительства РФ от 21.03.2012 № 218 "О Федеральной службе по интеллектуальной собственности" (вместе с "Положением о Федеральной службе по интеллектуальной собственности") // "Собрание законодательства РФ", 02.04.2012, № 14, ст. 1627.

[161] Постановление Правительства РФ от 24.12.2007 № 928 "О порядке проведения проверки наличия в заявках на выдачу патента на изобретение, полезную модель или промышленный образец, созданные в Российской Федерации, сведений, составляющих государственную тайну" // "Собрание законодательства РФ", 31.12.2007, № 53, ст. 6624.

патентообладателя и открывает широкий доступ к запатентованным решениям всем заинтересованным лицам, что и создаёт предпосылки для наиболее эффективного экономического использования этих решений. Однако это даёт возможность и заимствования указанной информации с нарушением авторских прав.

Наиболее рациональным способом защиты вышеуказанных прав является комбинирование двух способов, а именно: производится регистрация права на "сущность изобретения, полезную модель или промышленный образец", но при этом раскрывается только минимально необходимая информация для совершения регистрационных действий. В отношении остальной информации имеющую наибольшую ценность (техническую сущность изобретения, полезной модели или промышленного образца) устанавливается режим конфиденциальности – "секрет производства (ноу-хау)".

Зарубежное законодательство также содержит указанные виды информации. Однако в ряде государств отмечается более сложная классификация, так, например, в США в отношении информации, которая не имеет грифа секретности, но её распространение подлежит ограничению, используется следующая классификация конфиденциальной информации[162]:

- "информация, затрагивающая вопросы безопасности" (англ. "Sensitive Security Information" (SSI));

- "критическая программная информация" (англ. "Critical Program Information" (CPI));

- "только для служебного пользования" (англ. "For Official Use Only" (FOUO));

- "для ограниченного пользования" (англ. "Restricted");

- "распространение ограничено" (англ. "Limited Distribution" (LIMDIS));

- "для правоохранительных органов" (англ. "Law Enforcement Sensitive" (LES)).

---

[162] Закон об информации США. "Classified National Security Information". Executive Order 13526 of December 29, 2009 // URL: https://www.govinfo.gov/content/pkg/FR-2010-01-08/pdf/C1-2009-31418.pdf.

В тоже время, в связи с переходом мирового сообщества в "цифровую экономику", в ряде государств отмечаются попытки унификации указанной информации, так в законодательстве Великобритании[163] с апреля 2014 года в место целого набора классов информации: "конфиденциальная" (англ. "confidential"), "ограниченная" (англ. "restricted"), "защищённая" (англ. "protect") и "незакрытая" (англ. "unclassified"), введён единый класс информации: "официальная" (англ. "official"). В качестве альтернативного варианта в настоящее время в Европейском Союзе внедряется цветовая система классификации информации[164]: "красный" – "крайне конфиденциальная информация, только для конечного получателя", "жёлтый" – "ограниченное распространение", "зелёный" – "широкое распространение", "белый" – "неограниченное распространение".

В Российской Федерации также активно развиваются государственные информационные системы (ГИС) и электронный документооборот[165], поэтому выглядит целесообразным пойти по пути унификации информации, обрабатываемой в ГИС, с присвоением ей статуса "служебной информации" ("служебной тайны"). При этом необходимо отметить, что технически разделить массивы данных, обрабатываемых в информационной системе, довольно сложно, дорого и главное, не рационально. Наиболее оптимальным видится обработка разнородной информации ограниченного доступа единым массивом, с установлением единых требований к её защите.

в) "*Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна)*" – к которой относится информация, обладающая общим признаком, а

---

[163] Закон об информации Великобритании. "Security Policy Framework" (SPF) // URL: https://www.gov.uk/government/publications/security-policy-framework.

[164] "Протокол обозначений маркировки конфиденциальной информации" (англ. Traffic Light Protocol). Официальный сайт Департамента внутренней безопасности США // URL: https://www.us-cert.gov/tlp.

[165] Постановление Правительства РФ от 15.02.2022 № 172 "О государственной информационной системе "Типовое облачное решение системы электронного документооборота" (вместе с "Положением о государственной информационной системе "Типовое облачное решение системы электронного документооборота") // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1178.

именно субъект получил эту информацию в процессе осуществления своей определённой законом профессиональной деятельности и обязан обеспечить конфиденциальность полученной информации в силу требований законов, регулирующих данную профессиональную деятельность[166]. В настоящее время в Российской Федерации ярко выражены тридцать три вида "профессиональной тайны". Всего нормативно-правовые акты содержат около восьмидесяти упоминаний различных видов "профессиональных тайн".

Ряд специалистов по информационному праву к понятию "профессиональная тайна" относит и "служебную тайну", поскольку она полностью подпадает под дефиницию, данную в ч. 5 ст. 9 Закона об информации[167]. Такой же позиции придерживаются и авторы проекта Федерального закона "О служебной тайне". Однако, это неверно, так как не учтены т.с. "производные" из которых появилась "служебная тайна".

Во-первых, до появления Закона о государственной тайне (1993 год) "служебная информация ограниченного распространения" (с ограничительной пометкой "Для служебного пользования") организационно входила в состав государственной тайны и находилась на самой низшей её ступени[168], позволяя делать извлечения из секретных документов и одновременно ограничивая доступ к извлечённой информации посторонних лиц. В настоящее время, хотя в Законе о государственной тайне и отсутствует понятие "служебная информация ограниченного распространения", но по факту в системе защиты государственной тайны активно используется в тех же ролях, в которых применялась до введения в действие вышеуказанного закона[169].

---

[166] Перечень видов профессиональной тайны представлен в прил. 4 Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. № 2. 6-е изд., стереотип. М.: Ленанд, 2022. 368 с.

[167] Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. 2008. № 4 // URL: http://lawinfo.ru/catalog.

[168] Постановление Секретариата ЦК РКП(б) от 30.08.1922 "О порядке хранения и движения секретных документов" // М.: Издание, 1925, а также последующие нормативные правовые акты.

[169] Постановление Правительства РФ от 05.01.2004 № 3-1 "Об утверждении Инструкции по обеспечению режима секретности в Российской Федерации" // М.: Издание, 2011.

Во-вторых, "служебная информация ограниченного распространения" традиционно применялась и в настоящее время активно применяется различными органами государственного и муниципального управления при исполнении Закона о мобилизации[170]. Необходимо отметить, что в обоих случаях речь идёт об информации, собственником которой является Российская Федерация, которая реализует свои права через федеральные органы исполнительной власти. Таким образом, отнесение "служебной тайны" в рассматриваемый раздел классификации информации некорректно, тем более что современное законодательство выделило отдельную область, "служебная тайна в области обороны[171]".

В ч. 7 ст. 9 Закона об информации содержится норма: "Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе", которую предлагается из закона исключить как излишествующую по следующим основаниям:

- в законодательных актах, регулирующих различные виды профессиональной тайны, не содержится требования к срокам исполнения обязанностей по соблюдению, конфиденциальности сведений, составляющих профессиональную тайну, т.е. конфиденциальность профессиональной тайны имеет бессрочный характер;

- в случае если гражданин (физическое лицо) даёт своё согласие на снятие режима конфиденциальности, то рассматриваемый субъект реализует своё право как обладателя информации по определению порядка и условий доступа к ней. Тем более что рассматриваемые правоотношения регулируются Законом о персональных данных, положения которого не противоречат нормативным актам, регулирующим правоотношения соответствующей профессиональной тайны.

---

[170] Федеральный закон от 26.02.1997 № 31-ФЗ "О мобилизационной подготовке и мобилизации в Российской Федерации" // "Собрание законодательства РФ", 03.03.1997, № 9, ст. 1014.

[171] Ст. 3.1 Федерального закона от 31.05.1996 № 61-ФЗ "Об обороне" // "Собрание законодательства РФ", 03.06.1996, № 23, ст. 2750.

г) "*Информация о частной жизни гражданина (физического лица), в том числе составляющая личную и семейную тайну (персональные данные)*" – к которой относится информация, обладающая общим признаком, а именно она наиболее тесно связана с субъектом и содержит наиболее полное описание гражданина (физического лица) (см. рисунок 1.4).

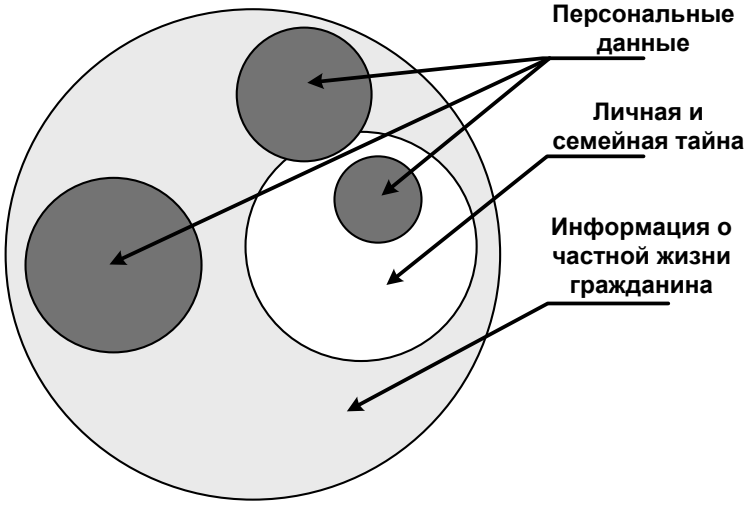

Рис. 1.4. Классификация информации о частной жизни гражданина

Необходимо отметить, что Российское законодательство не содержит определения понятий "информация о частной жизни гражданина (физического лица)" и "личная и семейная тайна"[172]. Под "информацией о частной жизни гражданина (физического лица)" понимается информация, относящаяся к т.н. "нематериальным благам", включающая в себя информацию "о жизни и здоровье, о достоинстве личности, обеспечивающую личную неприкосновенность, честь и доброе имя, деловую репутацию, неприкосновенность частной жизни, неприкосновенность жилища, о личной и семейной тайне, обеспечивающую свободу передвижения, свободу выбора места пребывания и жительства, имя гражданина, авторство, иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом[173]". Законодатель предусмотрел и защиту указанной информации, в частности ст. 152 Гражданского кодекса РФ (часть первая) обеспечивает защиту

[172] Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. № 8. 3-е изд., стереотип. М.: Ленанд, 2020. 224 с.

[173] Ч. 1 ст. 150 Гражданского кодекса РФ (часть первая) // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

чести, достоинства и деловой репутации, ст. 152.1 Гражданского кодекса РФ (часть первая) обеспечивает охрану изображения гражданина, а ст. 152.2 Гражданского кодекса РФ (часть первая) предусмотрена охрана частной жизни гражданина, при этом срок ограничения на доступ к документам, содержащим указанную информацию, ограничен "на срок 75 лет со дня создания указанных документов[174]". За незаконное собирание или использование информации о частной жизни гражданина предусмотрена уголовная ответственность[175]. Что касается "персональных данных", то, несмотря на широкое по смыслу определение, это "любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)"[176], по своей природе они ограничены целью сбора и возможностями информационной системы.

В виду того, что в настоящее время активно развивается "цифровая экономика" предлагается понятия "информация о частной жизни гражданина", "личная и семейная тайна" и "персональные данные" не разделять, так как в ближайшее время характер их обработки (базы данных, массивы информации и т.д.) будет максимально унифицирован – фактически это будут единые данные.

2) "*Предоставляемую по соглашению лиц, участвующих в соответствующих отношениях*" – информацию ограниченного доступа, которая может быть передана либо другой стороне на основе договорных отношений (см. ст. 421 Гражданского кодекса РФ (часть первая), ст. 1465 Гражданского кодекса РФ (часть четвёртая), п. 3, 4 ч. 2 ст. 6.1 Закона о коммерческой тайне, п. 5 ч. 1 ст. 6, 12 Закона о персональных данных), либо на основании мотивированного требования органа государственной власти (см. ст. 6, 13 Закона о коммерческой тайне, п. 4 ч. 1 ст. 6, 10, 11 Закона о персональных данных). Обязательным условием является соблюдение всеми сторонами режима конфиденциальности информации.

---

[174] Ч. 3 ст. 25 Федерального закона от 22.10.2004 № 125-ФЗ "Об архивном деле в Российской Федерации" // "Собрание законодательства РФ", 25.10.2004, № 43, ст. 4169.

[175] Ст. 137 Уголовного кодекса РФ // "Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954.

[176] П. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3451.

3) "*Распространение которой в Российской Федерации запрещается*" – информацию, которая "направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность" (см. ст. 280, 280.1, 280.3, 280.4 Уголовного кодекса РФ, ст. 13.15, 13.41, 13.48 Кодекса РФ об административных правонарушениях), также "запрещается распространение сообщений и материалов иностранного средства массовой информации, выполняющего функции иностранного агента[177]". При этом на Министерство юстиции России[178] возложено ведение "Единого реестра физических лиц и организаций, признанных иностранными агентами в Российской Федерации"[179].

Перечень запрещённой к распространению информации составлен на основе ч. 2 ст. 29, ч. 3 ст. 55 Конституции РФ и детализирован в ч. 6, 7 ст. 10 Закона об информации.

Для информации, распространение которой в сети Интернет запрещено, в ст. 15.1 Закона об информации содержится дополнительный исчерпывающий перечень, размещённый в единой автоматизированной информационной системе "Единый реестр доменных имён, указателей страниц сайтов в сети "Интернет"[180] (Далее по тексту – Реестр). В реестр включаются информационные ресурсы содержащие детскую порнографию, пропаганду наркотиков, пропаганду суицида,

---

[177] См. ст. 25.1 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации" // "Ведомости СНД и ВС РФ", 13.02.1992, № 7, ст. 300; Федеральный закон от 14.07.2022 № 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием" // "Собрание законодательства РФ", 18.07.2022, № 29 (ч. II), ст. 5222.

[178] Приказ Минюста РФ от 29.11.2022 № 307 "Об утверждении Порядка ведения реестра иностранных агентов и размещения содержащихся в нем сведений на официальном сайте Министерства юстиции Российской Федерации в информационно-телекоммуникационной сети "Интернет", Порядка принятия решения об исключении физического лица, впервые включённого в реестр иностранных агентов, из реестра иностранных агентов, формы заявления иностранного агента об исключении из реестра иностранных агентов" // URL: http://pravo.gov.ru.

[179] URL: https://minjust.gov.ru/uploaded/files/reestr-inostrannyih-agentov-01-12-2022.pdf.

[180] Постановление Правительства РФ от 26.10.2012 № 1101 "О единой автоматизированной информационной системе "Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" // "Собрание законодательства РФ", 29.10.2012, № 44, ст. 6044.

персональные данные о несовершеннолетнем потерпевшем, информацию об организации и проведении азартных игр и лотерей с использованием сети Интернет и иных средств связи. Необходимо обратить внимание, что реестр не урегулирует информацию, относящуюся к экстремистской деятельности. Недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности предусмотрено ст. 12 Закона о противодействии экстремистской деятельности[181] и п. 3.2.3 "Правил регистрации доменных имён"[182]. Общий перечень заблокированных ресурсов в реестре[183] является закрытым, и ознакомиться со всем содержимым реестра не представляется возможным. Доступ пользователей к реестру осуществляется только по запросу, содержащему конкретный адрес интересующего Интернет-ресурса.

[181] Федеральный закон от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности" // "Собрание законодательства РФ", 29.07.2002, № 30, ст. 3031.

[182] Решение Координационного центра национального домена сети "Интернет" от 05.10.2011 № 2011-18/81 "Правила регистрации доменных имён в доменах .RU и .РФ" (ред. от 06.09.2018 № 2018-06/26) // URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf.

[183] URL: http://eais.rkn.gov.ru.

ГЛАВА 2. ИССЛЕДОВАНИЕ РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА К ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

2.1. Определение понятия допуск и доступ в информационном праве

В научной литературе и в Российском законодательстве содержатся самые различные определения понятия "допуск".

В общем виде без привязки к какой-либо деятельности под "допуском" понимается "право входа или доступа куда-нибудь[184]", либо "разрешение на проведение определённой работы или на получение определённых документов и сведений, а также проход (проезд) в охраняемые зоны опасного объекта[185]".

В информационном праве под "допуском" понимается "допуск к секретной информации – процедура оформления права физических лиц на доступ к секретной информации, а уполномоченных органов - на проведение работ с использованием такой информации[186]" или "допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений[187]".

В технической сфере "допуск" понимается как некий "интервал, в котором допускается отклонение числовой характеристики некоего параметра от его номинального (расчётного) значения[188]".

---

[184] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И.Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

[185] Российская энциклопедия по охране труда: В 3-х томах. / Рук. проекта М.Ю.Зурабов / Отв. ред. А.Л.Сафонов. 2-е изд., перераб. и доп. М.: НЦ ЭНАС, 2007.

[186] "Соглашение между Правительством Российской Федерации и Правительством Словацкой Республики о взаимной защите секретной информации" (Заключено в гор. Москве 07.11.2006) // Бюллетень международных договоров. 2016. № 10. С. 53-58.

[187] Ст. 2 Закона РФ от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, стр. 8220-8235.

[188] Апарин Г.А., Городецкий И.Е. Допуски и технические измерения. 4-е изд. М., 1956.

В финансово-экономической сфере под "допуском" понимается "факт признания акций фирмы на бирже. Установление курса акций. С этого момента акции начинают котироваться на бирже[189]", либо "допуск на рынок нового поставщика. Новый поставщик может представлять собой вновь учреждённую фирму либо фирму, которая ранее действовала на других рынках[190]".

Как видно из вышеизложенного, обобщённо можно определить, что под "допуском" следует понимать установленное право субъекта на совершение заранее определённых (оговорённых) действий и оформленное заранее определённым образом.

Как показывают результаты проведённого исследования, в международных нормативных актах понятие "допуск" (англ. "admission") как самостоятельное понятие не используется, вместо него применяется термин "доступ" (англ. "access")[191], который также широко используется в литературе и в Российском законодательстве.

Так, в толковых словарях русского языка под "доступом" понимается "возможность проникновения куда-нибудь[192]", либо "разрешение заниматься, пользоваться чем-нибудь[193]".

В информационном праве под "доступом" понимается "доступ к информации – возможность получения информации и её использования[194]", "доступ к информации, составляющей коммерческую тайну, – ознакомление определённых лиц с информацией, составляющей коммерческую тайну, с согласия её обладателя или на ином законном основании при условии сохранения

---

[189] Словарь финансово-экономических терминов / под ред. И.З. Ярыгиной, Н.Г. Кондрахиной. М: Финансовый университет, 2012. 172 с.

[190] Словарь финансово-экономических терминов / под общ. ред. д.э.н., проф. М.А. Эскиндарова. 2-е изд. М.: Издательско-торговая корпорация "Дашков и К°", 2017. 1168 с.

[191] "Standard Protection Profile for Enterprise Security Management Access Control", October 24, 2013 // URL: https://www.commoncriteriaportal.org/files/ppfiles/pp_esm_ac_v2.1.pdf.

[192] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И. Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

[193] Ушаков Д.Н. Толковый словарь русского языка в 3-х томах на основе 4-томного издания 1948 г., М.: Вече, Си ЭТС, 2001. 890 с.

[194] Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

конфиденциальности этой информации[195]", "доступ к секретной информации – санкционированное в соответствии с законодательством государств сторон ознакомление с секретной информацией физического лица, имеющего допуск к секретной информации[196]", либо "доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного работника со сведениями, составляющими государственную тайну[197]".

В технической сфере понятие "доступ" к информации увязано с техническими средствами накопления и распространения информации. Чаще всего доступ понимается как процесс "извлечения информации из компьютерной памяти или помещение информации в компьютерную память[198]" либо "право, возможность, средства для поиска, извлечения или использования информации[199]", "ознакомление с информацией, её обработка, в частности, копирование модификация или уничтожение информации[200]".

Своеобразное понимание доступа к информации через экономические конкурентные отношения отмечается в финансово-экономической сфере, где под "доступом" понимается "выход на рынок нового поставщика. Барьерами для доступа (англ. "barriers to entry") называются факторы, препятствующие проникновению на рынок[201]".

---

[195] Ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ "О коммерческой тайне" // "Собрание законодательства РФ", 09.08.2004, № 32, ст. 3283.

[196] "Соглашение между Правительством Российской Федерации и Правительством Словацкой Республики о взаимной защите секретной информации" (Заключено в гор. Москве 07.11.2006) // Бюллетень международных договоров. 2016. № 10. С. 53-58.

[197] Ст. 2 Закона РФ от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, стр. 8220-8235.

[198] Бизнес: толковый словарь / Г.Бетс [и др.] / Общ. ред. И.М.Осадчей. М.: ИНФРА-М, 1998. 760 с.

[199] Национальный стандарт РФ. "ГОСТ Р ИСО 15489-1-2019. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы" (утв. Приказом Росстандарта РФ от 26.03.2019 № 101-ст) // М.: Стандартинформ, 2019.

[200] Руководящий документ ФСТЭК РФ. "Защита от несанкционированного доступа к информации. Термины и определения" (утв. решением Гостехкомиссии РФ от 30.03.1992) // URL: https://fstec.ru/component/attachments/download/298.

[201] Словарь финансово-экономических терминов / Под ред. И.З. Ярыгиной, Н.Г. Кондрахиной. М: Финансовый университет, 2012. 172 с.

Обобщая указанные выше определения, автор считает, что под "доступом" следует понимать разрешение субъекту, имеющему соответствующий допуск, совершить определённые (установленные) действия.

Анализ показывает, что в настоящее время федеральными органами исполнительной власти активно проводится работа по нормативному регулированию порядка использования различных информационных систем. Однако, прежняя терминология понятий "допуск" и "доступ", предусмотренная "аналоговым правом", не может быть использована в полном объеме, поскольку не учитывает всех особенностей функционирования информационных систем. Поэтому нужно применять новую терминологию, которая определена в технической документации, однако пока не закреплена в "цифровом праве"[202].

На основании результатов изучения материалов, автор считает, что вместо терминов "допуск" и "доступ" в "цифровой экономике" необходимо применять следующие основные термины и определения, которые необходимо включить в ст. 2 Закона об информации (см. рисунок 2.1):

1) Вместо термина "допуск" необходимо применять термин "идентификация" (англ. "identifico") – "присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов[203]", "процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку[204]" или "процесс, при котором осуществляется поиск[205] в регистрационной базе данных и

---

[202] Борисов М.А., Заводцев И.В. "Проблемы совершенствования допуска и доступа субъектов в информационные системы в условиях цифровой экономики" // "Проблемы экономики и юридической практики", М.: "Юр-ВАК", 2019, № 2, С. 267-270.

[203] Руководящий документ ФСТЭК РФ. "Защита от несанкционированного доступа к информации. Термины и определения" (утв. решением Гостехкомиссии РФ от 30.03.1992) // URL: https://fstec.ru/component/attachments/download/298.

[204] Национальный стандарт РФ. "ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. Приказом Росстандарта РФ от 17.12.2008 № 430-ст) // М.: Стандартинформ, 2009.

[205] Под термином "поиск" в контексте настоящего определения подразумевается процесс последовательного сравнения признаков передаваемого пользователем образца с множеством шаблонов, зарегистрированных в базе данных.

предоставляется список кандидатов, содержащий от нуля до одного или более идентификаторов[206]".

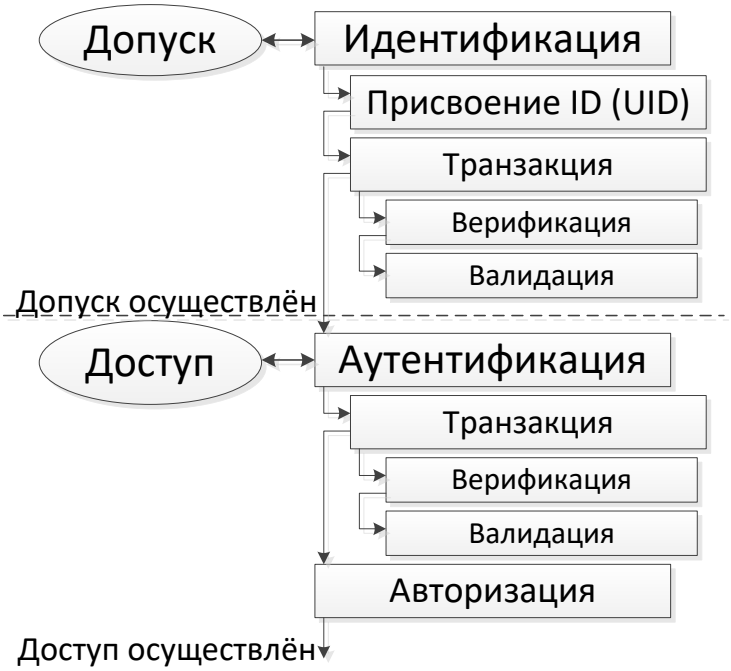

Рисунок 2.1. Алгоритм допуска и доступа в информационных системах

Как видно из вышеизложенных определений идентификации данный процесс предусматривает два основных действия:

Первое – это регистрацию субъекта в информационной системе путём присвоения специального "идентификатора (носителя идентификационного признака)" – "уникального признака субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код, – предмет, в который (на который) с помощью специальной технологии занесён идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и др. устройства)[207]".

---

[206] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура" (с Изменением № 1) (утв. Приказом Росстандарта РФ от 25.12.2007 № 403-ст) // М.: Стандартинформ, 2019.

[207] Национальный стандарт РФ. "ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. Приказом Росстандарта РФ от 17.12.2008 № 430-ст) // М.: Стандартинформ, 2009.

Идентификаторы по степени их надёжности (безопасности) различаются на "идентификатор" (англ. "identifier" (ID)) и "уникальный идентификатор" (англ. "unique identifier" (UID)).

"Идентификатор", как правило, присваивается вручную и не является секретным, т.к. может быть известен широкому кругу лиц. Всегда существует возможность его подмены. Доступ в информационную систему с применением только одного идентификатора не допускается. В настоящее время действующим законодательством не предусмотрен единый перечень идентификаторов. Наиболее полный перечень содержится в национальном стандарте ГОСТ Р ИСО/МЭК 29100-2013[208] и содержит 36 позиций (начиная с фамилии, имени и отчестве и заканчивая религиозными и философскими убеждениями).

"Уникальный идентификатор", как правило, присваивается автоматически с помощью технических устройств, которые позволяю выделить субъекта с достаточной степенью вероятности. Необходимо обратить внимание, что современные технологии не позволяют однозначно идентифицировать субъект и вероятностные отклонения варьируются в диапазоне 91 – 97% (в зависимости от вида используемых технологий), т.е. всегда существует вероятность ошибки[209].

В настоящее время действующим законодательством не предусмотрен единый перечень уникальных идентификаторов. Наиболее полный перечень направлений развития уникальных идентификаторов содержится в межгосударственном стандарте ГОСТ ISO/IEC 15459-2016 (части с 1 по 6)[210].

В качестве примера, уникальные идентификаторы применяются по следующим направлениям:

---

[208] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 29100-2013. Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности" (утв. Приказом Росстандарта РФ от 08.11.2013 № 1539-ст) // М.: Стандартинформ, 2014.

[209] URL: https://sites.google.com/site/biometriy/home.

[210] Межгосударственный стандарт. "ГОСТ ISO/IEC 15459-(1-6)-2016. Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 1. Индивидуальные транспортируемые единицы. Часть 2. Порядок регистрации. Часть 3. Общие правила. Часть 4. Штучные изделия и упакованные единицы продукции. Часть 5. Индивидуальные возвратные транспортные упаковочные средства. Часть 6. Группы" (принят Межгосударственным советом по стандартизации, метрологии и сертификации по переписке, протокол от 27.07.2016 № 89-П) // М.: Стандартинформ, 2018.

а) в качестве вещественных носителей:

- в авиационных, железнодорожных и других билетах – в качестве уникального идентификатора заказа;

- в системе оплаты общественного транспорта (например, "Социальная карта Москвича") и банковских услуг (банковские карты) – в качестве индивидуального заводского серийного номера карты;

- в платёжных документах федеральных органов исполнительной власти – в качестве уникального идентификатора начисления (УИН);

- для маркировки каких-либо изделий (продукции)[211], например сотовых телефонов, шуб, лекарственных препаратов, обуви, автомобильных покрышек, табачной продукции[212] и других товаров[213], так и для последующей их регистрации в информационной системе[214];

б) в качестве электронных носителей (маркеров, меток):

- в операционных системах (например, UNIX-подобные операционные системы) – в качестве регистрации субъекта (пользователя) по его уникальному номеру, который обозначается, как UID;

- в информационных ресурсах ГИС Интернет – в качестве регистрации информационных ресурсов (сайтов) по уникальному номеру UID (сетевому

---

[211] Распоряжение Правительства РФ от 28.04.2018 № 792-р "Об утверждении перечня отдельных товаров, подлежащих обязательной маркировке средствами идентификации" // "Собрание законодательства РФ", 07.05.2018, № 19, ст. 2773.

[212] Постановление Правительства РФ от 26.09.2019 № 1251 "О проведении эксперимента по маркировке средствами идентификации и мониторингу оборота отдельных видов табачной продукции, подлежащих обязательной маркировке с 1 июля 2020 г." (вместе с "Положением о проведении эксперимента по маркировке средствами идентификации и мониторингу оборота отдельных видов табачной продукции, подлежащих обязательной маркировке с 1 июля 2020 г.") // "Собрание законодательства РФ", 07.10.2019, № 40, ст. 5553.

[213] Постановление Правительства РФ от 28.03.2022 № 493 "Об утверждении Правил взаимодействия Федеральной государственной информационной системы прослеживаемости пестицидов и агрохимикатов и иных государственных информационных систем" // "Собрание законодательства РФ", 04.04.2022, № 14, ст. 2274.

[214] Постановление Правительства РФ от 26.04.2019 № 515 "О системе маркировки товаров средствами идентификации и прослеживаемости движения товаров" (вместе с "Правилами маркировки товаров, подлежащих обязательной маркировке средствами идентификации", "Положением о государственной информационной системе мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации") // "Собрание законодательства РФ", 13.05.2019, № 19, ст. 2279.

адресу, доменному имени, указателю страницы сайта)[215]. В настоящее время создаётся "Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено[216]";

в) в базах данных (массивах данных)[217] и т.п.;

г) в информационных системах обмена мгновенными сообщениями[218];

д) при использовании систем сотовой связи[219];

---

[215] Постановление Правительства РФ от 31.12.2022 № 2560 "Об утверждении Правил размещения государственными органами, органами местного самоуправления и подведомственными организациями информации на своих официальных страницах, получения доступа к информации, размещаемой на официальных страницах, и осуществления взаимодействия с пользователями информацией на официальных страницах с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, предусмотренной Федеральным законом "Об организации предоставления государственных и муниципальных услуг", и Правил взаимодействия официальных сайтов и официальных страниц с федеральной государственной информационной системой "Единый портал государственных и муниципальных услуг (функций)", включая требования, предъявляемые к такому взаимодействию" // "Собрание законодательства РФ", 09.01.2023, № 2, ст. 518.

[216] Приказ Роскомнадзора РФ от 14.12.2017 № 249 "Об утверждении требований к способам (методам) ограничения доступа к информационным ресурсам, а также требований к размещаемой информации об ограничении доступа к информационным ресурсам"; Приказ Роскомнадзора РФ от 11.02.2019 № 21 "Об утверждении Порядка идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам" // URL: http://www.pravo.gov.ru.

[217] Приказ Минсельхоза РФ от 01.10.2021 № 687 "Об утверждении порядка и формата представления в форме электронного документа деклараций об объёме винограда, использованного для производства винодельческой продукции, в том числе российской винодельческой продукции защищённых наименований, и полного цикла производства дистиллятов, формы и порядка заполнения таких деклараций" // URL: http://www.pravo.gov.ru; Положение Банка РФ от 18.08.2019 № 690-П "О порядке передачи банками в таможенные органы, а также таможенными органами в банки электронных документов, подписанных усиленной квалифицированной электронной подписью, и информации в электронном виде, предусмотренных статьёй 61 Федерального закона от 3 августа 2018 года № 289-ФЗ "О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации" (вместе с "Графиком обмена архивными файлами и сообщениями") // "Вестник Банка России", № 66, 03.10.2019.

[218] Постановление Правительства РФ от 20.10.2021 № 1801 "Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети "Интернет" организатором сервиса обмена мгновенными сообщениями" // "Собрание законодательства РФ", 25.10.2021, № 43, ст. 7291; Информация Роскомнадзора РФ от 07.05.2019 "О вступлении в силу новых правил идентификации пользователей мессенджеров" // URL: https://rkn.gov.ru.

е) в качестве биометрических носителей[220]:

- в различных системах биометрической идентификации, где используются индивидуальные физические признаки субъекта (физического лица)[221];

- в настоящее время перспективно развиваются системы геномной идентификации[222].

Второе – это процесс опознавания субъекта или объекта по ранее присвоенному ему идентификационному признаку, который в технических документах обозначается как "транзакция" (англ. "transaction") – "последовательность попыток (логических связанных действий для обработки запроса, поступившего в систему) со стороны пользователя для регистрации,

---

[219] Постановление Правительства РФ от 22.07.2022 № 1313 "Об утверждении Правил представления операторами подвижной радиотелефонной связи информации, необходимой для осуществления мониторинга соблюдения операторами связи обязанности по проверке достоверности сведений об абонентах и сведений о пользователях услугами связи абонентов - юридических лиц либо индивидуальных предпринимателей" // "Собрание законодательства РФ", 01.08.2022, № 31, ст. 5707.

[220] Постановление Правительства РФ от 16.06.2022 № 1089 "Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица"// "Собрание законодательства РФ", 27.06.2022, № 26, ст. 4475; Приказ Минцифры РФ от 10.09.2021 № 930 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации" // URL: http://www.pravo.gov.ru.

[221] Межгосударственный стандарт. "ГОСТ ISO/IEC 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура" (утв. Приказом Росстандарта РФ от 20.11.2015 № 1928-ст) // М.: Стандартинформ, 2018 (в настоящее время введено 14 частей); Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 29109-1-2012. Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определённых в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщённая методология испытаний на соответствие" (утв. Приказом Росстандарта РФ от 18.09.2012 № 349-ст) // М.: Стандартинформ, 2014 (в настоящее время введено 8 частей).

[222] Федеральный закон от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740; Постановление Правительства РФ от 11.10.2011 № 828 "Об утверждении Положения о порядке проведения обязательной государственной геномной регистрации лиц, осуждённых и отбывающих наказание в виде лишения свободы" // "Собрание законодательства РФ", 17.10.2011, № 42, ст. 5926; Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19794-14-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК" (утв. Приказом Росстандарта РФ от 09.06.2017 № 528-ст) // М.: Стандартинформ, 2018.

верификации или идентификации[223]". Процесс опознавания субъекта в информационных системах осуществляется в два основных этапа[224]:

вначале осуществляется "верификация" (англ. "verification") – "процесс, при котором происходит сравнение представленного пользователем образца с шаблоном, зарегистрированным в базе данных, при этом признаки передаваемого пользователем образца сравниваются с зарегистрированным шаблоном и по результатам сравнения возвращается положительное или отрицательное решение о запрошенной идентичности[225]";

далее осуществляется "валидация" (англ. "validation") – "документальное подтверждение того, что процесс, проводимый в пределах установленных параметров, может осуществляться эффективно и с воспроизводимыми результатами[226]" или "валидация компьютеризированной системы" (англ. "validation of a computerized system") – "документальное подтверждение высокой степени гарантии соответствия компьютеризированной системы определённым характеристикам, а данных, получаемых с помощью этой компьютеризированной системы, - заданному уровню качества и достоверности[227]".

Вышеуказанные процессы в информационных системах осуществляются в автоматическом режиме[228] (без участия физического лица). Если все необходимые

---

[223] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура" (утв. Приказом Росстандарта РФ от 25.12.2007 № 403-ст) // М.: Стандартинформ, 2008.

[224] Национальный стандарт РФ. "ГОСТ Р ИСО 11064-7-2016. Эргономическое проектирование центров управления. Часть 7. Принципы верификации и валидации" (утв. Приказом Росстандарта РФ от 02.11.2016 № 1583-ст) // М.: Стандартинформ, 2016.

[225] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура" (утв. Приказом Росстандарта РФ от 25.12.2007 № 403-ст) // М.: Стандартинформ, 2008.

[226] Решение Совета Евразийской экономической комиссии от 03.11.2016 № 81 "Об утверждении Правил надлежащей лабораторной практики Евразийского экономического союза в сфере обращения лекарственных средств" // URL: http://www.eaeunion.org.

[227] Там же.

[228] Межгосударственный стандарт. "ГОСТ 30721-2020 (ISO/IEC 19762:2016). Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь" (утв. Приказом Росстандарта РФ от 22.09.2020 № 6606-ст) // М.: Стандартинформ, 2020.

условия выполнены, то далее осуществляется следующий процесс – аутентификация.

2) "Аутентификация" (англ. "authentication") является альтернативной термина "доступ" и представляет собой "проверку принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности)[229]", "процесс опознавания субъекта или объекта путём сравнения введённых идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта[230]" или "подтверждение того, что отправитель полученных данных соответствует заявленному[231]".

Процесс аутентификации аналогичен процессу идентификации, изложенному выше, т.е. с использованием тех же самых физических принципов осуществляется процесс ввода информации в информационную систему[232]. Так, например, при предъявлении банковской карты осуществляется идентификация, а при вводе PIN-кода – авторизация, или применение связки "логин" – "пароль" в вычислительной технике[233]. В настоящее время активно развиваются биометрические системы аутентификации[234].

В случае выполнения всех необходимых условий по "идентификации" и "аутентификации" в отношении субъекта (физического лица, технического

---

[229] Руководящий документ ФСТЭК РФ. "Защита от несанкционированного доступа к информации Термины и определения" (утв. решением Гостехкомиссии РФ от 30.03.1992) // URL: https://fstec.ru/component/attachments/download/298.

[230] Национальный стандарт РФ. "ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. Приказом Росстандарта РФ от 17.12.2008 № 430-ст) // М.: Стандартинформ, 2009.

[231] Национальный стандарт РФ. "ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации" (утв. Постановлением Госстандарта РФ от 18.03.1999 № 77) // М.: ИПК Издательство стандартов, 1999.

[232] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 9594-8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации" (утв. Постановлением Госстандарта РФ от 19.05.1998 № 215) // М.: ИПК Издательство стандартов, 1998.

[233] См. главу 3 Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации. № 1. 5-е изд., сущ. пер. и доп. М.: Либроком, 2019. 456 с.

[234] Сабанов А.Г., Смолина С.Г. Сравнительный анализ методов биометрической идентификации личности // М.: Труды ИСА РАН. Том 66. 3/2016.

механизма и т.п.) "системой контроля и управления доступом[235]" осуществляется "авторизация" (англ. "authorization") или санкционированный доступ – "предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ[236]".

В случае если необходимые условия по авторизации не выполнены – доступ в информационную систему не предоставляется. Как было отмечено выше, развитие современных технологий допускает возможность обхода системы контроля и управления доступом[237], т.е. осуществляется "несанкционированный доступ (НСД) – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации[238]".

Необходимо отметить, что автором в мае 2019 года в журнале "Проблемы экономики и юридической практики"[239] были опубликованы настоящие предложения о включении в терминологический аппарат терминов "идентификация", "идентификатор", "уникальный идентификатор", "транзакция", "верификация", "валидация", "аутентификация", "авторизация" в ст. 2 Закона об информации и их унификации во всех издаваемых (изданных) нормативных правовых актах.

Начиная с 01.01.2021 года в ст. 2 Закона об информации были введены[240] следующие определения:

---

[235] Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

[236] Рекомендации по стандартизации РФ. "Р 50.1.056-2005. Техническая защита информации. Основные термины и определения" (утв. Приказом Росстандарта РФ от 29.12.2005 № 479-ст) // М.: Стандартинформ, 2006.

[237] Заводцев И.В., Борисов М.А., Бондаренко Н.Н., Мелешко В.А. Моделирование угроз безопасности информации и определение их актуальности для информационных систем объектов информатизации федеральных органов исполнительной власти // Computational nanotechnology, М.: Юр-ВАК, 2022, Т. 9, № 1, С. 106-114.

[238] Рекомендации по стандартизации РФ. "Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации" (утв. Приказом Росстандарта РФ от 06.04.2005 № 77-ст) // М.: Стандартинформ, 2005.

[239] Борисов М.А., Заводцев И.В. "Проблемы совершенствования допуска и доступа субъектов в информационные системы в условиях цифровой экономики" // "Проблемы экономики и юридической практики", М.: "Юр-ВАК", 2019, № 2, С. 267-270.

[240] См. Федеральный закон от 29.12.2020 № 479-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", "Собрание законодательства РФ", 04.01.2021, № 1 (ч. 1), ст. 18.

"21) идентификация – совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица (далее - идентификатор)";

"22) аутентификация – совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным".

Однако, с 29.12.2022 года вышеуказанные определения были исключены из ст. 2 Закона об информации и включены в ст. 2 Закона о биометрической идентификации[241].

Как видно и вышеизложенного, законодатель принял предложение автора о замене в терминологическом аппарате терминов "допуск" и "доступ" к информации на термины "идентификация" и "аутентификация" при правовом урегулировании порядка использования информационных систем, в тоже время - об оставлении терминов "допуск" и "доступ" при правовом регулировании вне информационных систем.

Можно предположить, что в дальнейшем законодатель продолжит указанную работу.

---

[241] 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 утратившими силу отдельных положений законодательных актов Российской Федерации" // "Собрание законодательства РФ", 02.01.2023, № 1 (ч. I), ст. 19.

2.2. Проблемы правового регулирования допуска и доступа к информации в современный период

Правовое регулирование отношений в области допуска и доступа к информации осуществляется по двум основным направлениям.

Первое, это регулирование отношений в области допуска и доступа к информации вне информационной системы, где понятия "допуск" и "доступ" были исторически определены на основе сложившихся правоотношений между государством, юридическими и физическими лицами с учётом сложившихся видов тайн и различных ограничений в работе с информацией.

Второе, новое направление начало формироваться с момента появления автоматизированной обработки информации, в рамках которого существенно изменилось содержание традиционного понятия "допуск" и "доступ". Эти процессы в информационной сфере возникли в 1976 году[242], когда впервые был нормативно разграничен доступ к информации в информационных (вычислительных) системах. Начиная с 1992 года, когда в нормативных документах Федеральной службы по техническому и экспортному контролю РФ[243] впервые стала применяться терминология, принятая в зарубежных нормативных документах, стандартах и т.п., в Российском правовом регулировании отношений по поводу допуска и доступа информации возникли проблемы.

До начала создания "цифровой экономики" данное разночтение понятий для дальнейшего развития нормотворчества вреда не представляло, так как информационные потоки обработки информации вне информационных систем и непосредственно в информационных системах практически не пересекались. Однако в настоящее время, когда рушится система традиционных

[242] Постановление Секретариата ЦК КПСС и Совета Министров СССР от 04.12.1976 "Об обеспечении безопасности в автоматизированных системах управления войсками и вычислительной техники общего применения от утечки информации за счёт побочных электромагнитных излучений и наводок и несанкционированного доступа" // М.: Издание, 1977.

[243] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty.

правоотношений в области обращения информации и всё больше заменяется обработкой информации в информационных системах[244], различия в терминах и определениях требуют унификации.

Анализ результатов проведенного исследования подтверждает наличие таких проблем в различных сферах деятельности государства. Так, например, в Законе о противодействии терроризму[245] предусмотрено такое понятие как "упрощённая идентификация клиента - физического лица (далее также - упрощённая идентификация) – осуществляемая в случаях, установленных настоящим Федеральным законом, совокупность мероприятий по установлению в отношении клиента - физического лица фамилии, имени, отчества (если иное не вытекает из закона или национального обычая), серии и номера документа, удостоверяющего личность, и подтверждению достоверности этих сведений одним из следующих способов:

- с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

- с использованием информации из информационных систем органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определённой Правительством Российской Федерации;

- с использованием единой системы идентификации и аутентификации при использовании усиленной квалифицированной электронной подписи или простой электронной подписи при условии, что при выдаче ключа простой электронной подписи личность физического лица установлена при личном приёме".

Таким образом, законодатель ввёл в обиход самостоятельное понятие "упрощённая идентификация" которое является симбиозом понятий

---

[244] Постановление Правительства РФ от 30.07.2019 № 984 "Об утверждении Правил информационного взаимодействия единой автоматизированной системы страхования жилых помещений с информационными ресурсами федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и Центрального банка Российской Федерации" // "Собрание законодательства РФ", 05.08.2019, № 31, ст. 4649.

[245] Ст. 3 Федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" // "Собрание законодательства РФ", 13.08.2001, № 33 (ч. I), ст. 3418.

"идентификатор" и "уникальный идентификатор", рассмотренных выше, и фактически нивелирующее термины и определения целого ряда нормативных документов, а введённое понятие "идентификация – совокупность мероприятий по установлению определённых настоящим Федеральным законом сведений о клиентах, их представителях, выгодоприобретателях, бенефициарных владельцах и подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем" является ни чем иным как интерпретацией понятия "допуск".

На уровне подзаконных актов, например, по инициативе Федеральной службы безопасности РФ в "Правилах хранения информации в ГИС "Интернет"[246]" было введено самостоятельное понятие "регистрация – первичное внесение пользователем сети "Интернет" или организатором распространения информации в сети "Интернет" информации о пользователе сети "Интернет" в коммуникационный интернет-сервис, после которого у пользователя сети "Интернет" появляется возможность осуществлять приём, передачу, доставку и (или) обработку электронных сообщений с использованием такого коммуникационного интернет-сервиса". Фактически представленное определение является ничем иным как "идентификацией" в части регистрации субъектов.

Анализ указанных выше и других нормативных правовых актов свидетельствует, что в настоящее время применяются различные по содержательному смыслу понятия "допуск" и "доступ", которые вносят путаницу в единое понимание терминологии и ведут к несогласованности различных нормативных документов, а в некоторых случаях к резкому скачку

[246] Постановление Правительства РФ от 23.09.2020 № 1526 "О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети "Интернет" информации о фактах приёма, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети "Интернет" и информации об этих пользователях и предоставления её уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации" // "Собрание законодательства РФ", 05.10.2020, № 40, ст. 6258.

коррупционной составляющей[247]. С целью дальнейшего нормативного урегулирования "цифровой экономики" необходимо провести унификацию терминов "допуск" и "доступ".

К вышеизложенному следует добавить, что имеет место и несогласованность в нормативном правовом регулировании вопросов подтверждения подлинности документов[248].

Так, в судебной системе Российской Федерации предусмотрено электронное подписание судебного акта в "Системе автоматизации судопроизводства[249]" (САС), где электронному документу автоматически присваивается уникальный идентификационный номер (УИН)[250] и размещается QR-код, который позволяет его однозначно идентифицировать[251].

В настоящее время Российской Федерации функционирует "Государственная информационная система о государственных и муниципальных платежах" (ГИС ГМП), которая позволяет любому федеральному органу исполнительной власти проверить наличие государственных платежей[252].

Однако, в случае возврата излишне уплаченной государственной пошлины, Федеральная налоговая служба РФ истребует только документы[253], оформленные в бумажном виде, в том числе и платёжный документ, заверенный банком, даже если он осуществлялся онлайн.

---

[247] Борисов М.А. "К вопросу о совершенствовании системы лицензирования деятельности в области криптографической защиты информации в условиях развития цифровой экономики" // "Пробелы в российском законодательстве", М.: "Юр-ВАК", 2018, № 6, С. 286-288.

[248] Борисов М.А. "Совершенствование системы доступа субъектов к электронным документам" // "Пробелы в российском законодательстве", М.: "Юр-ВАК", 2019, № 2, С. 213-215.

[249] Приказ ВАС РФ от 26.02.2008 № 21 "О вводе в эксплуатацию системы автоматизации судопроизводства в арбитражных судах Российской Федерации" // URL: http://docs.cntd.ru/document/902089092.

[250] Ст. 170, 185 "Арбитражного процессуального кодекса Российской Федерации" от 24.07.2002 № 95-ФЗ // "Собрание законодательства РФ", 29.07.2002, № 30, ст. 3012.

[251] П. 9.4 "Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)" (утв. Постановлением Пленума ВАС РФ от 25.12.2013 № 100) // URL: http://www.consultant.ru.

[252] См. п. 2 ч. 1 ст. 73 Федерального закона от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

[253] См. абз. 2 п. 3 ст. 333.40 "Налогового кодекса Российской Федерации (часть вторая)" от 05.08.2000 № 117-ФЗ // "Собрание законодательства РФ", 07.08.2000, № 32, ст. 3340.

При вынесении своего решения должностные лица налоговых органов руководствуются действующими на настоящий момент нормативными документами[254], которые по своей сути являются репликами более ранних нормативных документов и не отражают тех изменений, которые сопутствуют появлению электронного документооборота и новому формату обмена данными "цифровая экономика". Необходимо отметить, что после соответствующей публикации[255] Федеральной налоговой службой РФ были внесены соответствующие изменения[256].

С целью урегулирования создавшейся коллизии целесообразно обязать федеральные органы исполнительной власти проверять подлинность судебных документов, выполненных в форме электронных документов и размещённых на официальном сайте суда в информационно-телекоммуникационной сети "Интернет" в режиме ограниченного доступа, посредством сличения их уникальных идентификационных номеров (УИН) и QR-кодов, а заявителям предъявлять на них ссылку. Для этого необходимо внести изменения в соответствующие нормативно-правовые документы[257] и обязать федеральные органы исполнительной власти, в т.ч. судебные органы, самостоятельно проверять наличие информации о платежах государственных пошлин в "Государственной информационной системе о государственных и муниципальных платежах" (ГИС ГМП).

---

[254] Приказ ФНС РФ от 14.02.2017 № ММВ-7-8/182@ "Об утверждении форм документов, используемых налоговыми органами и налогоплательщиками при осуществлении зачёта и возврата сумм излишне уплаченных (взысканных) налогов, сборов, страховых взносов, пеней, штрафов" (отменён с 09.01.2023 года) // URL: http://www.pravo.gov.ru.

[255] Борисов М.А. "Совершенствование системы доступа субъектов к электронным документам" // "Пробелы в российском законодательстве", М.: "Юр-ВАК", 2019, № 2, С. 213-215.

[256] Приказ ФНС РФ от 30.11.2022 № ЕД-7-8/1133@ "Об утверждении форм и форматов представления документов, используемых налоговыми органами и налогоплательщиками, плательщиками сборов, плательщиками страховых взносов и (или) налоговыми агентами при осуществлении зачёта и возврата сумм денежных средств, формирующих положительное сальдо единого налогового счета, а также излишне уплаченной (взысканной) государственной пошлины" // URL: http://www.pravo.gov.ru.

[257] Ст. 7 Федерального закона от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

2.3. Механизм обеспечения допуска и доступа к информации в условиях цифровой экономики

В условиях "цифровой экономики" прослеживается тенденция формирования механизма "допуска" и "доступа" субъектов к информации, в зависимости от особенностей правового положения субъектов и их роли в процессе обращения информации. Учитывая названные критерии, имеющие влияние и лежащие в основе распределения прав и обязанностей по допуску и доступу к информации, рассмотрим отдельные группы субъектов применительно к процессам допуска (1-я группа) и доступа (2-я группа) субъектов к информации.

Первая группа, правоотношения, которые возникают по "допуску" к информации (в информационные системы) реализуются субъектами в следующем порядке:

1) *Юридическими лицами (индивидуальными предпринимателями)*:

а) путём получения лицензии – "специального разрешения на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью[258]";

б) путём прохождения добровольной сертификации деятельности (например, "Система менеджмента бережливого производства[259]" или "Система менеджмента информационной безопасности[260]");

---

[258] Ст. 3 Федерального закона от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности" // "Собрание законодательства РФ", 09.05.2011, № 19, ст. 2716.

[259] Приказ Минпромторга РФ от 20.06.2017 № 1907 "Об утверждении Рекомендаций по применению принципов бережливого производства в различных отраслях промышленности" // URL: http://www.consultant.ru.

[260] Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (утв. Приказом Росстандарта РФ от 30.11.2021 № 1653-ст) // М.: Стандартинформ, 2021.

в) путём регистрации в "Единой системе идентификации и аутентификации" – федеральной государственной информационной системе, порядок использования которой устанавливается Правительством РФ[261] и которая обеспечивает санкционированный доступ к информации, содержащейся в информационных системах. Необходимо отметить, что в данной системе регистрируются не сами юридические лица, а физические лица (работники), действующие в интересах юридического лица (представляющие его интересы).

2) *Физическими лицами (работниками):*

а) путём регистрации в "Единой системе идентификации и аутентификации" – федеральной государственной информационной системе, порядок использования которой устанавливается Правительством РФ[262] и которая обеспечивает санкционированный доступ к информации, содержащейся в информационных системах. Необходимо отметить, что при идентификации и аутентификации субъектов в данной системе применяются биометрические данные[263] и (или) специально выданные идентификаторы (например, ИНН[264], СНИЛС[265], идентификационный модуль (SIM-карта) с номером телефона подвижной радиотелефонной связи[266], адрес почтового ящика в ГИС Интернет,

---

[261] 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" // "Собрание законодательства РФ", 05.12.2011, № 49 (ч. 5), ст. 7284.

[262] Постановление Правительства РФ от 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" // "Собрание законодательства РФ", 09.07.2018, № 28, ст. 4234.

[263] Ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

[264] П. 7 ст. 84 "Налогового кодекса Российской Федерации (часть первая)" от 31.07.1998 № 146-ФЗ // "Собрание законодательства РФ", № 31, 03.08.1998, ст. 3824.

[265] П. 1 ч. 2 ст. 11 Федерального закона от 01.04.1996 № 27-ФЗ "Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования" // "Собрание законодательства РФ", 01.04.1996, № 14, ст. 1401.

[266] П. 3.2 ст. 2, 44 Федерального закона от 07.07.2003 № 126-ФЗ "О связи" // "Собрание законодательства РФ", 14.07.2003, № 28, ст. 2895.

медицинские документы о рождении[267], биосовместимая метка, наносимая на кожу[268] и др.);

б) путём предоставления паспортных данных при личном обращении физического лица (работника) как на территории Российской Федерации[269], так и за рубежом[270];

в) путём предоставления доверенности[271] о праве представления интересов другого субъекта (при условии соблюдения условий, изложенных в п. "б" (см. выше));

г) путём получения специального разрешения (например, оформление допуска к государственной тайне[272]);

д) путём прохождения обязательной сертификации (например, для осуществления определённого вида профессиональной деятельности, в том числе выполнения определённой трудовой функции, необходимо наличие профессионального образования, соответствующего условиям профессионального

---

[267] Постановление Правительства РФ от 05.02.2022 № 116 "Об утверждении Правил ведения Федерального реестра медицинских документов о рождении" // "Собрание законодательства РФ", 14.02.2022, № 7, ст. 974.

[268] URL: https://stm.sciencemag.org/content/11/523/eaay7162.

[269] Указ Президента РФ от 13.03.1997 № 232 "Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации" // "Собрание законодательства РФ", 17.03.1997, № 11, ст. 1301; Постановление Правительства РФ от 08.07.1997 № 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" // "Собрание законодательства РФ", 14.07.1997, № 28, ст. 3444.

[270] Указ Президента РФ от 29.12.2012 № 1709 "О паспорте гражданина Российской Федерации, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем на электронном носителе информации дополнительные биометрические персональные данные его владельца" // "Собрание законодательства РФ", 31.12.2012, № 53 (ч. 2), ст. 7861; Постановление Правительства РФ от 04.03.2010 № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию" // "Собрание законодательства РФ", 08.03.2010, № 10, ст. 1103.

[271] Ст. 185 "Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

[272] Постановление Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

стандарта[273]. Если работник не имеет соответствующего профессионального образования, то ему необходимо пройти независимую оценку квалификации на соответствие профессиональному стандарту[274]);

е) путём прохождения добровольной сертификации по эксплуатации информационных систем, в т.ч. и систем информационной безопасности (например, система сертификации ООО "Доктор Веб"[275] или ОАО "Информационные Технологии и Коммуникационные Системы"[276]);

ж) путём допуска физических лиц к определённой информации только при достижении ими определённого возраста[277].

3) *Для информационных систем (технических устройств, программного обеспечения и т.п.):*

а) путём применения программного обеспечения, включённого в "Единый реестр российских программ для электронных вычислительных машин и баз данных[278]" Министерства цифрового развития, связи и массовых коммуникаций РФ и ограничением допуска на территорию Российской Федерации программного обеспечения, происходящего из иностранных государств[279];

---

[273] Ст. 195.1 "Трудового кодекса Российской Федерации" от 30.12.2001 № 197-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 3.

[274] Федеральный закон от 03.07.2016 № 238-ФЗ "О независимой оценке квалификации" // "Собрание законодательства РФ", 04.07.2016, № 27 (ч. I), ст. 4171.

[275] URL: https://training.drweb.ru.

[276] URL: http://edu.infotecs.ru/learning.

[277] Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" // "Собрание законодательства РФ", 03.01.2011, № 1, ст. 48; "Рекомендации по применению Федерального закона от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в отношении печатной (книжной) продукции" (утв. Минкомсвязи РФ от 22.01.2013 № АВ-П17-531) // URL: http://www.consultant.ru.

[278] URL: https://reestr.minsvyaz.ru/reestr.

[279] Постановление Правительства РФ от 16.11.2015 № 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд" (вместе с "Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации", "Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включённого в единый реестр программ для электронных вычислительных машин и баз данных из

б) путём получения необходимого сертификата соответствия программного обеспечения и (или) технического устройства[280] на соответствие установленным требованиям.

В Российской Федерации предусмотрена система обязательной и добровольной сертификации информационной продукции. Обязательной сертификации подлежат информационные продукты (технические устройства и программное обеспечение) применяемые для защиты информации[281]. За обязательную сертификацию указанных информационных продуктов в рамках своих полномочий отвечает Федеральная служба безопасности РФ[282] и Федеральная служба по техническому и экспортному контролю РФ[283].

Система добровольной сертификации может быть создана юридическим лицом и (или) индивидуальным предпринимателем или несколькими юридическими лицами и (или) индивидуальными предпринимателями[284]. Добровольная сертификация осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации соответствия национальным стандартам, стандартам организаций, системам добровольной сертификации, условиям договоров.

Объектами добровольной сертификации могут быть продукция, процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации, работы и услуги, а также иные объекты, в отношении которых стандартами,

---

государств - членов Евразийского экономического союза, за исключением Российской Федерации), для целей осуществления закупок для обеспечения государственных и муниципальных нужд") // "Собрание законодательства РФ", 23.11.2015, № 47, ст. 6600.

[280] Приказ Минсвязи РФ от 29.06.1995 № 79 "О сертификации оборудования сотовой связи с учётом временных технических решений" // URL: http://www.consultant.ru.

[281] Постановление Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации" // "Собрание законодательства РФ", 03.07.1995, № 27, ст. 2579.

[282] Приказ ФСБ РФ от 13.11.1999 № 564 "Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о её знаках соответствия" // "Бюллетень нормативных актов федеральных органов исполнительной власти", № 3, 17.01.2000.

[283] Приказ ФСТЭК РФ от 03.04.2018 № 55 "Об утверждении Положения о системе сертификации средств защиты информации" // URL: http://www.pravo.gov.ru.

[284] См. "Реестр зарегистрированных систем добровольной сертификации" // URL: https://www.gost.ru/portal/gost/home/activity/compliance/VoluntaryAcknowledgement/reestr.

системами добровольной сертификации и договорами устанавливаются требования. В информационной сфере предусмотрены системы добровольной сертификации "Цифровые инновации[285]", "Цифровая экономика[286]", "Военный регистр[287]", "Управление производствами и ремонтами[288]" и др. Обработка персональных данных также предусматривает международную добровольную систему сертификации на соответствие требованиям "Генерального регламента о защите персональных данных[289]" (GDPR).

Вторая группа – это правоотношения по "доступу" субъектов к информации (в информационные системы), которые возникают и реализуются в следующем порядке:

1) *Юридическими лицами (индивидуальными предпринимателями)*:

а) путём заключения договора с контрагентом (федеральным органом исполнительной власти, юридическим лицом, физическим лицом), в соответствии с которым (на условиях которого) им предоставляется доступ к информации (передача соответствующей информации для дальнейшей обработки);

б) путём получения информации (подтверждения) из "Единой системы идентификации и аутентификации" – федеральной государственной информационной системы, порядок использования которой устанавливается Правительством РФ[290] и которая обеспечивает санкционированный доступ к информации, содержащейся в информационных системах.

---

[285] Свидетельство № РОСС RU.31943.04ФМГ0 от 25.07.2018 года.

[286] URL: http://gagarinstart.ru/sdsekonomika.

[287] URL: https://www.sds-vr.ru/index.php?id=438.

[288] Global Manufacturing Execution Systems (MES) Market 2009-2013 – производственная исполнительная система, которая включает в себя специализированные программные комплексы с элементами "искусственного интеллекта" и "интернета вещей" предназначенные для решения задач оперативного планирования и управления производством // URL: http://www.tadviser.ru/index.php/MES.

[289] Регламент № 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" (Принят в гор. Брюсселе 27.04.2016) // URL: http://eur-lex.europa.eu.

[290] Постановление Правительства РФ от 28.11.2011 № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-

2) *Физическими лицами (работниками):*

а) путём получения информации (подтверждения) из "Единой системы идентификации и аутентификации" – федеральной государственной информационной системы, порядок использования которой устанавливается Правительством Российской Федерации[291] и которая обеспечивает санкционированный доступ к информации, содержащейся в информационных системах. Как правило, для аутентификации субъектов в данной системе применяются биометрические данные[292] и др.;

б) путём получения информации по запросу после подтверждения паспортных данных физического лица (субъекта) или его полномочий при личном обращении в федеральные органы исполнительной власти, к юридическим и физическим лицам;

в) путём получения специальной санкции должностного лица (приказ, резолюция на документе и т.п.) на ознакомление с информацией (например, при осуществлении доступа к государственной тайне[293]).

3) *Для информационных систем (технических устройств, программного обеспечения и т.п.):*

а) применение программного обеспечения и (или) технического устройства, которые имеют соответствующие сертификаты на соответствие установленным требованиям;

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.

[291] Постановление Правительства РФ от 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" // "Собрание законодательства РФ", 09.07.2018, № 28, ст. 4234.

[292] Ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

[293] Постановление Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

б) применение программного обеспечения и (или) технического устройства, которое имеет соответствующее сопряжение (техническую совместимость), а для обрабатываемой информации – соответствующий формат представления.

Как видно из приведённого анализа механизм обеспечения допуска и доступа к информации в условиях "цифровой экономики" обладает широким разнообразием, что не позволяет осуществить его унификацию, однако по мере развития государственных информационных систем[294], такая возможность будет предоставлена.

Необходимо отметить, что в условиях "цифровой экономики" появляются новые технические устройства, занимающиеся обработкой информации (исполнение специализированных функций), например, отдельные из них объединяются общим понятием – "интернет вещей".

Под "интернетом вещей" (англ. Internet of Tings, IoT) понимается "концепция вычислительной сети физических предметов (вещей), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой[295]", "рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, которые исключают из части действий и операций необходимость участия человека[296]".

Анализ литературы позволяет сделать вывод, что в настоящее время "интернет вещей" развивается по трём основным направлениям:

- "промышленный интернет вещей" (англ. "Industrial Internet of Things") – предполагающее создание многоуровневой системы сбора данных, их визуализации, а также мощных аналитических инструментов интерпретации получаемой информации;

---

[294] Федеральный закон от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

[295] Kevin Ashton. "Internet Of Things". Gartner IT glossary. Gartner, 5 May 2012 // URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things.

[296] Kevin Ashton. "That ‘Internet of Things’ Thing. In the real world, things matter more than ideas". RFID Journal, 22 June 2009 // URL: https://www.webcitation.org/6DuYQRsDZ?url=http://www.rfidjournal.com/article/pdf/4986/1/1/rfidjournal-article4986.PDF.

- "бытовой (потребительский) интернет вещей" (англ. "Consumer Internet of Things") – предполагающее оказание услуг населению по обеспечению бытовых потребностей ("Умный дом[297]", "Каршеринг[298]", магазин без касс и продавцов и т.п.);

- "децентрализация вычислений", т.н. технология "блокчейн" (англ. "blockchain") – предполагающая создание систем облачных технологий (вычислений), искусственного интеллекта, больших данных, машинного обучения и т.п.

В настоящее время разработан и активно совершенствуется алгоритм децентрализованных вычислений, который именуется "Цифровая-ДНК" или "Кибер-ДНК"[299].

Данный алгоритм предназначен для решения двух основных задач:

- сбор информации и анализ информации об активности технических устройств (например, их совместное нахождение в одной информационной сети и данные об их использовании). Так, телевизоры и телефоны компании Samsung автоматически (без участия пользователя) оповещаются и взаимодействуют друг с другом[300], что с одной стороны облегчает их настройку и использование, с другой – предоставляет информацию об окружающей технологической среде;

- сбор и анализ активности пользователя в социальных сетях, его "цифровых следов", что позволяет составить психологический портрет физического лица, оценить уровень его интеллекта, проанализировать желания, интересы, взгляды и на основе полученных данных произвести конфигурацию цифровой среды вокруг субъекта.

Несмотря на всё разнообразие технологий "интернета вещей" в рамках рассматриваемой темы они обладают общими чертами:

---

[297] Understanding Building Automation and Control Systems // URL: https:// www.kmccontrols.com/products/Understanding_ Building_Automation_and_Control_Systems.aspx.

[298] Каршеринг (англ. carsharing) – вид пользования автомобилем, когда одна из сторон не является его собственником.

[299] Пази. М. "Кибер-ДНК", "Эксперт", 2019, № 16 // URL: https://expert.ru/russian_reporter/2019/16/kiber-dnk.

[300] URL: https://www.samsung.com/ru/multi-device-experience.

- механизм допуска и доступа в информационную систему, как правило, осуществляется на этапе создания устройства (жёстко прописан в системе);

- если имеется механизм настройки допуска и доступа, то, как правило, осуществляется в весьма ограниченном диапазоне;

- система защиты информации данных технических устройств крайне уязвима.

Так, в отчёте Национального разведывательного совета США (англ. Natio nal Intelligence Council) 2008 года "интернет вещей" фигурирует как "одна из шести подрывных технологий, указывается, что повсеместное и незаметное для потребителей превращение в Интернет-узлы таких распространённых вещей, как товарная упаковка, мебель, бумажные документы, может заметно повысить риски в сфере национальной информационной безопасности[301]".

Вышеизложенный анализ позволяет сделать вывод о необходимости унификации (стандартизации) технологии "интернета вещей". В Российской Федерации, как и во всём мире, такая работа уже началась[302].

---

[301] "Disruptive Civil Technologies. Six Technologies with Potential Impacts on US Interests out to 2025". National Intelligence Council, 11 April 2008 // URL: https://fas.org/irp/nic/disruptive.pdf.

[302] Национальный стандарт РФ. "ГОСТ Р 59026-2020. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе стандарта LTE в режиме NB-IoT. Основные параметры" (утв. Приказом Росстандарта РФ от 15.09.2020 № 649-ст) // М.: Стандартинформ, 2020; Предварительный национальный стандарт РФ. "ПНСТ 516-2021. Информационные технологии. Интернет вещей. Спецификация LoRaWAN RU" (утв. Приказом Росстандарта РФ от 28.01.2021 № 5-пнст) // М.: Стандартинформ, 2021; Предварительный национальный стандарт РФ. "ПНСТ 518-2021 (ИСО/МЭК 20924:2018). Информационные технологии. Интернет вещей. Термины и определения" (утв. Приказом Росстандарта РФ от 28.01.2021 № 7-пнст) // М.: Стандартинформ, 2021.

ГЛАВА 3. СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДОПУСКА И ДОСТУПА К ОХРАНЯЕМОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

3.1. Совершенствование законодательства о допуске и доступе субъектов к государственной тайне в условиях цифровой экономики

Государственная тайна является одной из старейших разновидностей информации, подлежащей правовому регулированию. Первые упоминания о создании системы допуска к государственной тайне относятся ещё к 1724 году[303], когда была введена отдельная правовая категория – "благонадёжные люди" (см. рисунок 3.1).

4418.—Генваря 16. Именный, данный Сенату. — *О порученіи секретныхъ дѣлъ въ Сенатѣ благонадежнымъ людямъ.*

Самимъ вамъ вѣдомо, что секретныя дѣла вынесены отъ подьячихъ Черкассамъ, и зѣло удивительно, что какъ ординарныя, такъ и секретныя дѣла въ Сенатѣ по повытьямъ; того ради, получа сіе, учините по примѣру Иностранной Коллегіи, чтобъ секретныя дѣла были особливо у надежныхъ людей, чтобъ впредь такого скаредства не учинилось.

Рис. 3.1. Указ Петра I от 16.01.1724 года

С течением времени правовое регулирование в рассматриваемой области только совершенствовалось и подстраивалось под существующие нужды, однако принимаемые правовые нормы всегда отличались традиционным консерватизмом. В ст. 2 Закона о государственной тайне[304] под "допуском к государственной тайне" понимается "процедура оформления права граждан на

[303] Указ Петра I от 16.01.1724 "О поручении секретных дел в Сенате благонадёжным людям" // Полное собрание законов Российской империи. Т. 7 (1723–1727). Печат. в Типографии 2-го отд. Собственной Его Императорского Величества Канцелярии. 1830. Ст. 4409.

[304] Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, стр. 8220-8235.

доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений", а под "доступом к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну".

В мае 2010 года в Российской Федерации вступила в силу, действующая в настоящее время, очередная "Инструкция по допуску к государственной тайне[305]" (далее по тексту – Инструкция по допуску). Однако, вместо совершенствования системы допуска к государственной тайне, получился совершенно противоположный эффект.

Основной из главных причин, явилось предоставление Федеральной службе безопасности РФ (далее по тексту – органы безопасности) право давать разъяснения по вопросам применения Инструкции по допуску. Ввиду того, что в настоящее время повсеместно отмечается снижение уровня профессиональной компетентности[306], то территориальные подразделения органов безопасности предъявляют различные по содержанию требования к оформлению установленных документов, в том числе и не соответствующие Закону о государственной тайне и Инструкции по допуску, мотивируя это тем, что органам безопасности предоставлено право разъяснять положения указанной инструкции[307]. Однако, толковый словарь русского языка[308] под понятием "разъяснять" понимает "сделать ясным, понятным", т.е. данное понятие не предполагает "толкование", т.е. "объяснение чего-нибудь, изложение точки зрения на что-нибудь новое", дефиниций нормативных актов. В результате

---

[305] Постановление Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

[306] Борисов М.А. "К вопросу о совершенствовании допуска к государственной тайне в условиях развития цифровой экономики" // "Пробелы в российском законодательстве", М.: "Юр-ВАК", 2018, № 6, С. 289-291.

[307] П. 3 Постановления Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

[308] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И. Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

расширенного толкования действующих норм органами безопасности вместо улучшения системы защиты государственной тайны, фактически созданы бреши для злоупотребления правом и возникновения "коррупционной составляющей".

В ст. 2 и 27 Закона о государственной тайне определён порядок допуска к государственной тайне юридических лиц путём получения соответствующей лицензии. Порядок лицензирования устанавливается "Положением о лицензировании деятельности по защите государственной тайны[309]" (далее по тексту – Порядок лицензирования) (см. рисунок 3.2).

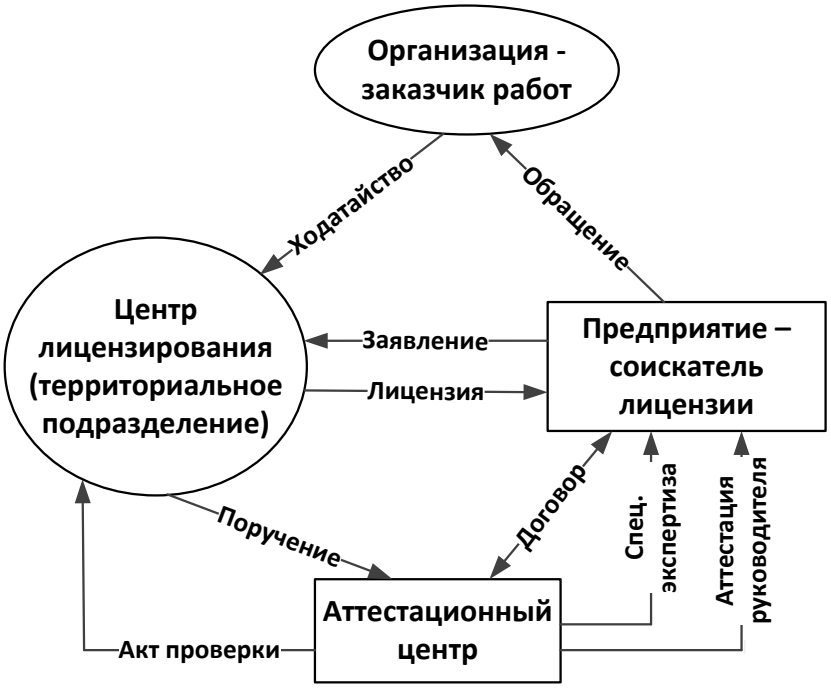

Рис. 3.2. Алгоритм лицензирования юридических лиц
на проведение работ с государственной тайной

В соответствии с п. 5 Порядка лицензирования и п. 13 Инструкции по допуску обязательным условием для получения лицензии является "наличие органа государственной власти или организации, наделённого полномочиями по распоряжению указанными сведениями" (далее по тексту – заказчика работ), который определяет характер сведений, составляющих государственную тайну и с которыми предстоит работать организации – соискателю лицензии (далее по

[309] Постановление Правительства РФ от 15.04.1995 № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" // "Собрание законодательства РФ", 24.04.1995, № 17, ст. 1540.

тексту – лицензиату). Заказчик работ наделён правом принимать решение о допуске к государственной тайне руководителя лицензиата. Документ, подтверждающий допуск к государственной тайне руководителя лицензиата непосредственно хранится у заказчика работ. Такой порядок на практике вызывает проблемы. Заказчик работ и лицензиат могут располагаться экстерриториально, т.е. изъятых из-под действия местного законодательства и подпадающих под действие законодательства государства, что вносит определённые трудности по контролю со стороны территориальных подразделений органов государственной безопасности.

Изучение материалов показывает, что с целью "облегчения своей деятельности" органы безопасности разработали ряд методических рекомендаций, которые на лицензиатов возлагают обязанность включать в "Номенклатуру должностей работников лицензиата, подлежащих оформлению на допуск к государственной тайне[310]", которая направляется в территориальный орган безопасности, первым пунктом должность руководителя лицензиата. Данный документ утверждается руководителем лицензиата. В отдельных случаях ещё и выдвигают требование о хранении карточки-допуска[311] руководителя лицензиата вместе с номенклатурой должностей. Ввиду того, что заказчиком работ, как правило, является государственный орган, который может найти исполнителя работ по обеспечению государственных нужд с использованием государственной тайны только после проведения государственных закупок[312], т.е. одним из условий получения контракта является наличие соответствующей лицензии. В свою очередь для лицензиата основным условием получения лицензии является наличие контракта с заказчиком работ на работу с государственной тайной.

В настоящее время имеются признаки следующей коррупционной схемы:

---

[310] Прил. ф. 3. Инструкции по допуску.

[311] Прил. ф. 1. Там же.

[312] Федеральный закон от 05.04.2013 № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" // "Собрание законодательства РФ", 08.04.2013, № 14, ст. 1652.

1) Лицензиат за отдельное вознаграждение договаривается с каким-либо государственным органом, чтобы он выступил в качестве фиктивного заказчика работ.

2) Получает фиктивный контракт и ходатайство в органы безопасности о необходимости получения лицензии.

3) На законных основаниях органы безопасности выдают лицензию, а на руководителя лицензиата оформляют допуск к государственной тайне.

4) После чего фиктивный заказчик работ расторгает контракт с лицензиатом[313].

В п. 12 Порядка лицензирования одним из оснований для приостановления действия или аннулирования лицензии является заявление лицензиата. При этом обязанности в предоставлении заявления в случае прекращения контракта с заказчиком работ законодательством не предусмотрено. В случае прекращения контракта заказчик работ обязан прекратить допуск к государственной тайне руководителю лицензиата, однако уведомить в этом органы безопасности в соответствии с п. 43, 44 Инструкции по допуску обязан только через шесть месяцев. Таким образом, на рынке появляется организация, которая имеет все необходимые атрибуты для работы с государственной тайной (лицензию и допуск руководителя), однако по факту доступа к государственной тайне не имеет. Вместе с тем, она имеет возможность участвовать в конкурсе по осуществлению государственных закупок, где одним из условий является наличие лицензии на работу с государственной тайной, тем самым расширяется круг участников конкурса, что даёт возможность для демпинга выполнения работ, по меньшей стоимости и с более низким качеством, чем установлено на рынке. При этом органы безопасности данный процесс практически отследить не могут.

Причиной расширения круга организаций, получивших избыточный доступ к государственной тайне, является разрешение организациям оказывать услуги другой организации (аутсорсинг) по обработке государственной тайны в

[313] Ст. 95 Федерального закона от 05.04.2013 № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" // "Собрание законодательства РФ", 08.04.2013, № 14, ст. 1652.

интересах заказчика работ, что предусмотрено в пп. "г" п. 5 Порядка лицензирования. Особенности оказания данной услуги действующим законодательством не урегулированы, что предоставляет организациям, оказывающим соответствующие услуги, получать доступ к государственной тайне за пределами полномочий, установленных соответствующей лицензией. В свою очередь, попытка органов безопасности ограничить круг организаций, осведомлённых в государственной тайне, путём выдачи соответствующих предписаний о принудительном расторжении заключённых договоров на оказание соответствующих услуг, не основана на законе, противоречит условиям лицензирования этих организаций, приводит к конфликту интересов сторон, что противоречит основным принципам трудового и гражданского законодательства.

Анализ содержания положений Инструкции по допуску и Методических рекомендаций, разработанных органами безопасности, показывает, что в процессе формулирования правовых норм были нарушены лексические нормы русского языка, в результате чего был искажён смысл целого ряда дефиниций. Например, ст. 2 Закона о государственной тайне содержит определения понятий "допуска" – как процедуры оформления права на доступ и "доступа" – как уже оформленного права на работу с государственной тайной. Однако в Инструкции о допуске и в Методических рекомендациях активно используется глагол "допустить" ("допускается" и т.п.), причём он применяется в отношении обоих существительных "допуск" и "доступ", тем самым кардинально меняя смысл описываемых дефиниций[314]. Стоит отметить, что по современным правилам русского языка[315] глагол "допустить" применяется только в отношении существительного "доступ", а существительное "допуск" глагола не имеет. В толковом словаре русского языка Даля В.И.[316] содержатся лексические пары "допуск – допустить" и "доступ – доступить", однако в настоящее время они не

[314] П. 11, 33, 39, 64 Инструкции по допуску.

[315] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И.Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

[316] Даль В.И. "Толковый словарь живого великорусского языка. В 4-х томах", 6-е издание, стереотипное, М.: Дрофа, 2011. 2734 с.

употребляются. Безусловно, на практике это вносит путаницу в понимание различия понятий "допуск" и "доступ".

В Российской Федерации предусмотрен порядок допуска к государственной тайне двумя основными способами путём проведения проверочных мероприятий органами безопасности (см. рисунок 3.3) и без проведения соответствующих проверочных мероприятий (см. рисунок 3.4).

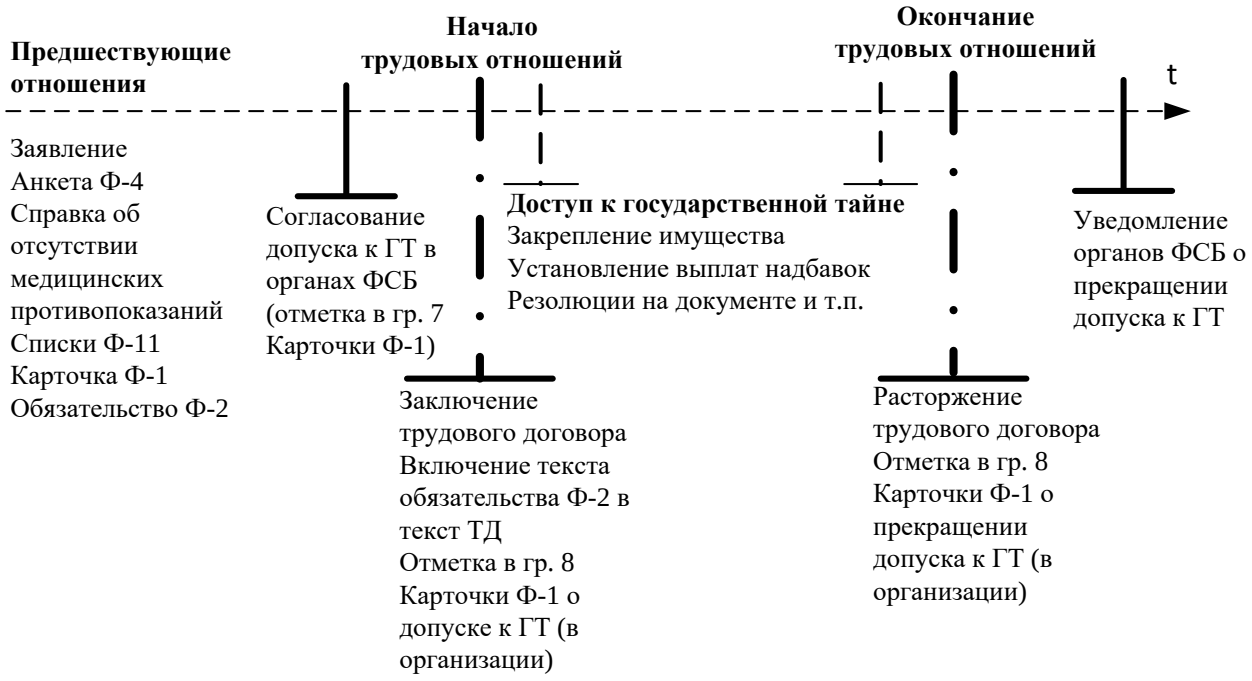

Рис. 3.3. Алгоритм допуска к государственной тайне
с проведением проверочных мероприятий

В попытке уменьшить объём Инструкции о допуске разработчики два способа допуска к государственной тайне не разделили на отдельные разделы, а написали совместно, не разбив на смысловые группы[317]. В результате чего произошла подмена понятий и смешивание различных по правовой природе алгоритмов допуска к государственной тайне: с проведением и без проведения проверочных мероприятий.

Например, в ст. 15 Инструкции по допуску общим основанием прекращения допуска к государственной тайне определено условие "расторжения с работником трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий", однако данное утверждение справедливо только когда

[317] П. 39, 42–46 Инструкции по допуску.

допуск к государственной тайне осуществлён без проведения проверочных мероприятий.

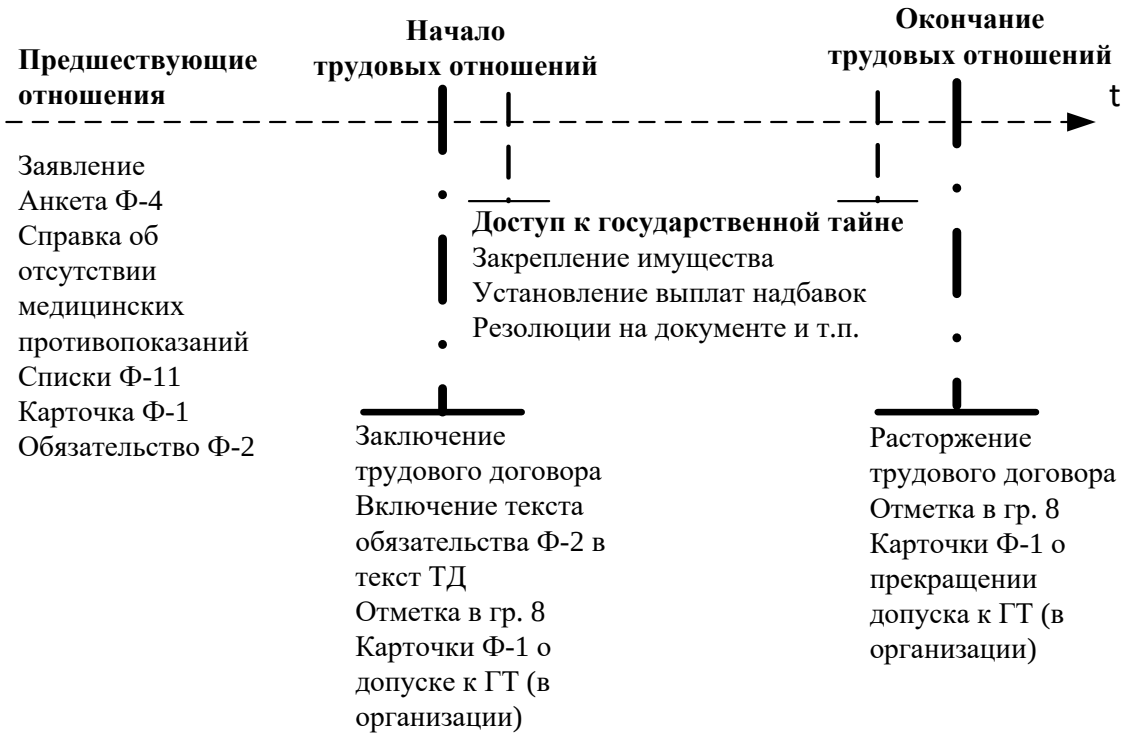

Рис. 3.4. Алгоритм допуска к государственной тайне
без проведения проверочных мероприятий

Аналогичные разночтения содержатся и в связке п. 44 и 46 Инструкции по допуску. Так, основанием для прекращения допуска к государственной тайне является, когда:

- "граждане, которые переведены на должности, не предусматривающие наличие допуска к государственной тайне";

- "уволились из организации, в том числе при расторжении трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий";

- "закончили обучение в учебном заведении и т.п.".

При этом установлено общее условие – "на которых в течение 6 месяцев не затребованы карточки (форма 1), действие допуска прекращается". При прекращении допуска к государственной тайне руководство организации обязано уведомить территориальные органы безопасности в месячный срок, путём направления соответствующего уведомления.

Из дефиниции п. 44 и 46 Инструкции невозможно установить следующее:

1) С какого момента прекращается действие допуска к государственной тайне?

Виду того, что правоотношения между работником (служащим) и организацией устанавливаются условиями трудового договора[318] (служебного контракта[319]), то с момента прекращения трудовых (служебных) правоотношений должен быть прекращён и допуск к государственной тайне в организации работника (служащего) (см. рисунок 3.3.). Однако по смыслу получатся, что допуск к государственной тайне прекращается не ранее чем через 6-ть месяцев после прекращения трудовых (служебных) правоотношений, что противоречит условиям трудового законодательства.

2) Что понимается под понятием "граждане, которые переведены на должности, не предусматривающие наличие допуска к государственной тайне"?

В соответствии со ст. 72.1 Трудового кодекса РФ под переводом работника на другую работу понимается:

а) постоянное или временное изменение трудовой функции работника и (или) структурного подразделения, в котором работает работник (если структурное подразделение было указано в трудовом договоре), при продолжении работы у того же работодателя, а также перевод на работу в другую местность вместе с работодателем. При этом действие трудового договора (служебного контракта) не прекращается, а изменение условий труда урегулируются дополнительными соглашениями;

б) перевод работника по его письменной просьбе или с его письменного согласия на постоянную работу к другому работодателю. При этом действие трудового договора (служебного контракта) по прежнему месту работы (службы) прекращается (см. п. 5 ч. 1 ст. 77 Трудового кодекса РФ). Такой перевод может

---

[318] См. разд. III "Трудового кодекса Российской Федерации" от 30.12.2001 № 197-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 3.

[319] См. гл. 5 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" // "Собрание законодательства РФ", 02.08.2004, № 31, ст. 3215.

быть осуществлён на основе согласованного волеизъявления трёх сторон: работника, прежнего и будущего работодателей[320].

Таким образом, если работник осуществляет перевод внутри организации, то правоотношения между работником и работодателем не прекращаются, условия неопределённости дальнейшей судьбы допуска к государственной тайне отсутствуют, а, соответственно, и нет необходимости в 6-ти месячном сроке ожидания для уведомления контролирующих органов о прекращении допуска к государственной тайне. В тоже время, если работник, перешёл к другому работодателю, то целесообразно ожидать до 6-ти месяцев затребование карточки допуска к новому работодателю.

Для государственных гражданских служащих перевод на иную должность гражданской службы в том же государственном органе, либо перевод гражданского служащего на иную должность гражданской службы в другом государственном органе, либо перевод гражданского служащего в другую местность вместе с государственным органом допускается с письменного согласия гражданского служащего и без прекращения действия служебного контракта[321].

Как видно из вышеизложенного, необходимо производить уточнение п. 44 Инструкции по допуску в следующей части: вместо "граждане, которые переведены на должности, не предусматривающие наличие допуска к государственной тайне" указать "граждане, которые переведены на постоянную работу к другому работодателю".

Также необходимо поменять местам п. 45 и 46 Инструкции по допуску, так как внутри связки п. 44 и 46 Инструкции по допуску содержится: "45. Решение о прекращении допуска гражданина к государственной тайне оформляется записью в позиции 8 карточки (форма 1), которая заверяется подписью соответствующего должностного лица и печатью организации (при наличии печати)", который вносит путаницу в понимание вышеуказанных пунктов.

---

[320] См. Письмо Минтруда РФ от 18.08.2017 № 14-2/В-761 // "Нормативные акты для бухгалтера", 2017, № 20.

[321] См. ст. 28 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" // "Собрание законодательства РФ", 02.08.2004, № 31, ст. 3215.

Ещё одним примером является ст. 60 Инструкции по допуску, в которой определены условия и сроки переоформления допуска к государственной тайне. Так, условием переоформление допуска к государственной тайне является переход гражданина на другое место работы (службы), однако не уточняется, что допуск не подлежит переоформлению в случае, если не менялся развёрнутый перечень сведений, подлежащих засекречиванию[322] (см. ст. 9 Закона о государственной тайне). Статья не конкретизирует понятие "постоянно работающих в организации", не понятно, что законодатель имел ввиду под понятием "организация". Данный термин имеет широкое понятие – это "организованное планомерное, продуманное устройство, внутренняя дисциплина[323]" или "компания, фирма, проект, предприятие, учреждение, завод, фабрика, объединение, орган власти, общественный институт или ассоциация и т.п., либо их части, входящие или не входящие в их состав, различных форм собственности, которые имеют собственные функции и управление. В организациях, имеющих более одного структурного подразделения, каждое отдельно взятое структурное подразделение может рассматриваться как организация[324]". Предложения автора по устранению вышеуказанных коллизий изложены в приложении 2 к настоящей работе.

Соответственно территориальные подразделения органов безопасности по-разному толкуют статьи Инструкции по допуску, внося сумятицу в отлаженную систему допуска к государственной тайне, так как в настоящее время разобраться в особенностях оформления допуска к государственной тайне могут лишь специалисты, имеющие богатый практический опыт.

---

[322] См. Распоряжение Президента РФ от 16.04.2005 № 151-рп "О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне" // "Собрание законодательства РФ", 25.04.2005, № 17, ст. 1547.

[323] Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И.Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

[324] Межгосударственный стандарт. "ГОСТ 12.0.230-2007. Система стандартов безопасности труда. Системы управления охраной труда. Общие требования" (утверждён Приказом Росстандарта РФ от 10.07.2007 № 169-ст) // М.: Стандартинформ, 2007.

Необходимо отметить и проблемы допуска к государственной тайне специальных субъектов – лиц, не являющихся гражданами Российской Федерации, лиц имеющих двойное гражданство, эмигрантов, реэмигрантов, в том числе граждан Российской Федерации, имеющих вид на жительство или иной документ, подтверждающий их право на постоянное проживание на территории иностранного государства. Действующее законодательство выделяет лиц, имеющих двойное гражданство, которые допускаются к государственной тайне с грифом не выше "секретно" только после проведения проверочных мероприятий органами безопасности[325], однако это касается граждан, которые получили двойное гражданство только до 01.07.2002 года[326]. В настоящее время правовой статус двойного гражданства закреплён с Туркменистаном (с 23.12.1993 года по 18.05.2015 года), с Таджикистаном (с 15.12.1996 года по н.в.) и с Южной Осетией (с 20.09.2021 года по н.в.). Порядок допуска указанной категории граждан к государственной тайне регламентирован "Положением о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне[327]", однако по сложившейся практике, как правило, к государственной тайне не допускаются.

Действующим законодательством предусмотрен допуск к государственной тайне и иностранных граждан. Обязательным условием их допуска к государственной тайне является наличие международного договора, предусматривающего обязательства иностранного государства или

---

[325] П. 3 Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // "Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407.

[326] См. Закон РФ от 28.11.1991 № 1948-1 "О гражданстве Российской Федерации" // "Ведомости СНД и ВС РФ", 06.02.1992, № 6, ст. 243; Федеральный закон РФ от 31.05.2002 № 62-ФЗ "О гражданстве Российской Федерации" // "Собрание законодательства РФ", 03.06.2002, № 22, ст. 2031.

[327] Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // "Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407.

международной организации по защите передаваемых им сведений, составляющих государственную тайну[328].

В настоящее время в связи с развитием "Евразийского экономического союза"[329] (далее по тексту – Договор), на государство возложены обязанности по привлечению трудящихся государств-членов союза для осуществления ими трудовой деятельности в Российской Федерации. При этом данным иностранным работникам не требуется получение разрешения на осуществление трудовой деятельности в государстве трудоустройства. Единственным ограничением на использование иностранной рабочей силы является прямой запрет в Договоре и в национальных законодательствах государств-членов в целях обеспечения национальной безопасности (в том числе в отраслях экономики, имеющих стратегическое значение) и общественного порядка, в отношении осуществляемой трудящимися государств-членов трудовой деятельности, рода занятий и территории пребывания.

При решении вопроса о допуске иностранцев к государственной тайне Российской Федерации важно учитывать действие норм, принимаемых в рамках Договора, когда на государство возложены обязанности по привлечению трудящихся из государств-членов союза с целью осуществления ими трудовой деятельности в Российской Федерации. При этом должно действовать ограничение на использование иностранной рабочей силы в целях обеспечения национальной безопасности (в том числе в отраслях экономики, имеющих стратегическое значение) и общественного порядка, что опять же должно вытекать из Договора и быть прописано в национальных законодательствах государств-членов.

---

[328] П. 6 Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // "Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407; Постановление Правительства РФ от 02.08.1997 № 973 "Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или Международным организациям" // "Собрание законодательства РФ", 11.08.1997, № 32, ст. 3786.

[329] "Договор о Евразийском экономическом союзе" (Подписан в гор. Астане 29.05.2014) // URL: http://www.pravo.gov.ru. В настоящее время его членами являются: Казахстан, Россия, Белоруссия, Армения, Киргизия, а кандидатами на вступление: Молдова, Узбекистан, Куба, Иран.

Необходимо обратить внимание, что в Российской Федерации вышеуказанный процесс недостаточно урегулирован, например, если в случае осуществления государственных закупок, связанных с государственной тайной, имеется прямой запрет по её осуществлению у государств-членов (ч. 2 ст. 88 Договора), то в отношении привлечения иностранной рабочей силы государств-членов такие ограничения не предусмотрены (ст. 96 - 98 Договора), лишь косвенно об этом сказано в пп. "в" п. 12 Инструкции по допуску.

Что касается лиц без гражданства, то они могут быть допущены к государственной тайне, как правило, с грифом не выше "секретно", только на основании решения Правительства РФ[330]. Необходимо учесть, что приведённая формулировка "как правило", не носит категоричный характер, что в исключительных случаях позволяет допустить апатридов к государственной тайне с грифами "особой важности" и "совершенно секретно".

Таким образом, в условиях глобальных изменений в современной внешней политике и экономике, когда значительные категории лиц в упрощённом порядке получают гражданство Российской Федерации[331] (не отказываясь от гражданства другого государства), когда между государствами перемещаются огромные массы работников-специалистов в инновационных областях, существующая система допуска к государственной тайне требует серьёзной настройки с учётом современных реалий. Важно чётко закрепить определённые правила допуска работников имеющих двойное гражданство или иностранных граждан к государственной тайне, что будет способствовать развитию инновационной экономики государства и существенно снизит коррупционную составляющую.

---

[330] Ст. 4 Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // "Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407.

[331] См. Федеральный конституционный закон от 21.03.2014 № 6-ФКЗ "О принятии в Российскую Федерацию Республики Крым и образовании в составе Российской Федерации новых субъектов - Республики Крым и города федерального значения Севастополя" // "Собрание законодательства РФ", 24.03.2014, № 12, ст. 1201 и др.; Указ Президента РФ от 24.04.2019 № 183 "Об определении в гуманитарных целях категорий лиц, имеющих право обратиться с заявлениями о приёме в гражданство Российской Федерации в упрощённом порядке" // "Собрание законодательства РФ", 29.04.2019, № 17, ст. 2071.

В действующих нормативно-правовых актах, регулирующих вопросы допуска к государственной тайне, отсутствуют установленные предельные сроки проведения проверочных мероприятий, в отношении граждан, оформляемых на допуск к государственной тайне, в результате чего период оформления допуска в среднем составляет от шести месяцев, и это в условиях развития автоматизированных государственных информационных систем, в которых всю необходимую информацию можно получить в течении нескольких минут.

На фоне перестройки экономики и системы управления[332] система допуска к государственной тайне выглядит анахронизмом и нуждается в кардинальном реформировании. Ст. 21 и 25 Закона о государственной тайне не требуют внесения уточнений, поскольку вопросы правового регулирования допуска и доступа к государственной тайне отнесены к компетенции Правительства Российской Федерации.

Анализ материалов исследования показывает, что при разработке нового порядка допуска и доступа к государственной тайне в условиях "цифровой экономики" целесообразно решить первоочередные задачи (см. приложение 2):

1) С целью снижения количества ошибок при применении установленных правовых норм и исключения "коррупционной составляющей" отменить "право Федеральной службы безопасности РФ давать разъяснения по вопросам применения Инструкции по допуску"[333]. Все необходимые изменения в правоприменение вносить соответствующими постановлениями Правительства Российской Федерации.

2) В ходе разработки нормативно-правовых актов, регулирующих вопросы допуска и доступа к государственной тайне, учесть лексические нормы русского

---

[332] Постановление Правительства РФ от 02.03.2019 № 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации") // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1119.

[333] П. 3 Постановления Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

языка, исключив употребление глагола "допустить", заменив его выражениями типа "осуществить допуск", "осуществить доступ" и т.п.

3) В рамках реализации государственной программы "Цифровая экономика" поэтапно ввести в систему допуска к государственной тайне сбор данных об оформляемом лице[334] в электронной форме через ГИС "Единый портал государственных и муниципальных услуг (функций)[335]" (ЕПГУ) путём заполнения специальной анкеты в электронной форме.

Необходимо отметить, что в соответствии с пп. "б" п. 33 Инструкции по допуску предусмотрена возможность передачи органам безопасности анкетных данных гражданина в электронном виде, однако дальнейшее их использование в информационных системах не осуществляется. В тоже время, если на гражданина оформляется допуск к государственной тайне без проведения проверочных мероприятий[336], то контроль за достоверностью представленных анкетных данных фактически возложена на работодателя, возможности которого в отличие от органов безопасности существенно ограничены[337].

В настоящее время имеется техническая возможность через ЕПГУ получить достоверные (идентифицированные) данные о фамилии, имени, отчестве, дате и месте рождения гражданина, полученных им документах, удостоверяющих личность, сведения о судимости, об образовании и т.п. Необходимо отметить, что в дальнейшем сведения об образовании (цифровые дипломы) планируются к размещению на базе Интернет-ресурса "Современная цифровая образовательная

---

[334] Прил. ф. 4. Инструкции по допуску.

[335] Постановление Правительства РФ от 24.10.2011 № 861 "О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)" // "Собрание законодательства РФ", 31.10.2011, № 44, ст. 6274; Постановление Правительства РФ от 13.05.2022 № 867 "О единой цифровой платформе в сфере занятости и трудовых отношений "Работа в России" (вместе с "Правилами функционирования единой цифровой платформы в сфере занятости и трудовых отношений "Работа в России") // "Собрание законодательства РФ", 23.05.2022, № 21, ст. 3446.

[336] П. 9, 37, 41, 46, 49 Инструкции по допуску.

[337] См. Федеральный закон от 12.08.1995 № 144-ФЗ "Об оперативно-розыскной деятельности" // "Собрание законодательства РФ", 14.08.1995, № 33, ст. 3349; Закон РФ от 11.03.1992 № 2487-1 "О частной детективной и охранной деятельности в Российской Федерации" // "Ведомости СНД РФ и ВС РФ", 23.04.1992, № 17, ст. 888.

среда в Российской Федерации[338]". В перспективе на базе "цифровых дипломов" планируется создать "цифровой портфолио" гражданина, куда кроме сведений об образовании (начальном, среднем и высшем) также будут входить и данные о практике, спортивных достижениях, научных исследованиях, сведения о курсах повышения квалификации и т.п.

С 2020 года в Российской Федерации введены электронные трудовые книжки[339], что в перспективе даёт возможность через информационные ресурсы Пенсионного фонда РФ получать достоверные сведения о трудовой деятельности гражданина.

В соответствии с пп. 4 п. 2 ст. 1 Закона о персональных данных его действие не распространяется на "обработку персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну". Инструкция по допуску данное обстоятельство никак не конкретизирует, поэтому существует правовая неопределённость – относятся ли анкетные данные гражданина, оформляемого на допуск к государственной тайне, к "персональным данным" или нет? С учётом сложившейся практики целесообразно вышеуказанные анкетные данные гражданина отнести к "персональным данным" с внесением соответствующих изменений в Закон о персональных данных.

4) С целью надлежащей идентификации граждан, допускаемых к государственной тайне, внести соответствующее дополнение п. 28.1 в Инструкцию по допуску об обязанности граждан проходить биометрическую идентификацию[340] в ГИС "Единая система идентификации и аутентификации[341]" (ЕСИА).

---

[338] URL: http://neorusedu.ru/events.

[339] URL: http://www.pfrf.ru/etk.

[340] Постановление Правительства РФ от 16.06.2022 № 1089 "Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица" // "Собрание законодательства РФ", 27.06.2022, № 26, ст. 4475.

[341] 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" // "Собрание законодательства РФ", 05.12.2011, № 49 (ч. 5), ст. 7284.

5) С целью ограничения сбора информации о гражданах, допускаемых к государственной тайне, ст. 24 Закона о государственной тайне дополнить ограничение "права на размещение общедоступной информации, а также данных, позволяющих идентифицировать должностное лицо или гражданина, на сайтах и (или) страницах сайтов в информационно-коммуникационной сети "Интернет"".

6) В соответствии с требованиями ст. 22 Закона о государственной тайне и пп. "б" п. 12 Инструкции по допуску гражданин, допускаемый к государственной тайне, обязан предоставлять сведения об отсутствии у него медицинских противопоказаний[342], при этом сведения о проведённом обследовании в медицинскую карту гражданина не заносятся.

В результате чего возникла следующая коллизия. Справка об отсутствии медицинских противопоказаний предоставляется лицом, устраивающимся на работу, работодателю только при оформлении (переоформлении) допуска к государственной тайне. В дальнейшем фактический контроль за наличием (появлением) медицинских противопоказаний у работника со стороны работодателя не осуществляется. Алгоритм прохождения диспансеризации работником по месту своего жительства (пребывания), как правило, наличие медицинских противопоказаний не выявляет (например, имеются скрытые симптомы психических отклонений, "тихий бытовой пьяница" и т.п.).

После публикации[343] автором указанной правовой коллизии Минздравом России был издан приказ[344], в котором указанная коллизия была частично устранена. Так, на работодателей возложена обязанность по периодическому

---

[342] Приказ Минздравсоцразвития РФ от 26.08.2011 № 989н "Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну" // "Российская газета", № 234, 19.10.2011.

[343] Борисов М.А. Правовое регулирование допуска и доступа к информации в условиях цифровой экономики № 20. М.: Ленанд, 2021. 224 с.

[344] Приказ Минздрава РФ от 20.05.2022 № 342н "Об утверждении порядка прохождения обязательного психиатрического освидетельствования работниками, осуществляющими отдельные виды деятельности, его периодичности, а также видов деятельности, при осуществлении которых проводится психиатрическое освидетельствование"; Письмо Минздрава России от 12.08.2022 № 30-7/3105 "Об обязательном психиатрическом освидетельствовании отдельных категорий работников" // URL: http://pravo.gov.ru.

направлению работников на обязательное психиатрическое освидетельствование, однако в указанных нормативных актах отсутствует периодичность такого направления (совмещается ли освидетельствование с каждой диспансеризацией[345] и т.п.). В результате чего, со стороны контролирующих органов поступают различные требования по периодичности психиатрического освидетельствования работников.

Необходимо учесть, что в "Перечне вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные медицинские осмотры при поступлении на работу и периодические медицинские осмотры"[346] отсутствуют должности работников, допущенных к государственной тайне, что не обязывает работников проходить периодические медицинские осмотры в объёме установленного Перечня медицинских противопоказаний. Поэтому целесообразно Перечень работ дополнить пунктом 23 "Работа с государственной и иной охраняемой законом тайной".

В ч. 2 ст. 21, ст. 41 Конституции РФ предусмотрено, что медицинское обследование гражданина может быть осуществлено только с его личного согласия, при этом за гражданином сохраняется право на анонимное лечение[347]. Данная правовая норма позволяет анонимно пройти лечение от алкоголизма (наркомании), при этом на учёте в наркологическом диспансере гражданин состоять не будет, что в дальнейшем позволит получить "Справку об отсутствии медицинских противопоказаний" для работы с государственной тайной.

---

[345] Приказ Минздрава РФ от 28.01.2021 № 29н "Об утверждении Порядка проведения обязательных предварительных и периодических медицинских осмотров работников, предусмотренных частью четвертой статьи 213 Трудового кодекса Российской Федерации, перечня медицинских противопоказаний к осуществлению работ с вредными и (или) опасными производственными факторами, а также работам, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры"; Приказ Минздрава РФ от 27.04.2021 № 404н "Об утверждении Порядка проведения профилактического медицинского осмотра и диспансеризации определённых групп взрослого населения" // URL: http://pravo.gov.ru.

[346] Приказ Минтруда РФ № 988н, Минздрава РФ № 1420н от 31.12.2020 "Об утверждении перечня вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные медицинские осмотры при поступлении на работу и периодические медицинские осмотры" // URL: http://pravo.gov.ru.

[347] Приказ Минздрава РФ от 23.08.1999 № 327 "Об анонимном лечении в наркологических учреждениях (подразделениях)" // URL: http://pravo.gov.ru.

Необходимо отметить, что только менее десяти процентов пациентов полностью избавляются от пагубной привычки[348]. Таким образом, правовые нормы, изложенные в ст. 22 Закона о государственной тайне и пп. "б" п. 12 Инструкции по допуску по своей сути не обеспечивают ограничение допуска к государственной тайне по медицинским противопоказаниям. Необходимо отметить, что вышеуказанная правовая коллизия имеет место и при получении права на использование оружия, управление транспортным средством, летательным аппаратом и т.п. Таким образом, целесообразно такое понятие как "анонимное лечение" исключить.

С развитием "цифровой экономики" в Российской Федерации развёртывается "Единая государственная информационная система в сфере здравоохранения[349]" (ЕГИСЗ), в которой предполагается обрабатывать сведения о лицах, которым оказывается медицинская помощь, проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования, в том числе и выдачу соответствующих направлений.

В рамках функционирования ЕГИСЗ на граждан России заводится "Федеральная интегрированная электронная медицинская карта", поэтому с целью фиксирования медицинских противопоказаний необходимо внести уточнение в п. 21 ст. 94 Закона об охране здоровья граждан[350] в части обязательной регистрации результатов исследований на отсутствие медицинских противопоказаний.

В настоящее время ЕГИСЗ не предполагает специальный сбор информации о наличии медицинских противопоказаний для работы с государственной тайной, поэтому целесообразно внести соответствующие дополнения в п. 4 Положения о ЕГИСЗ, дополнив его пп. "г 1" "федеральный реестр граждан Российской

---

[348] Лыжник О.В. Можно ли излечиться от наркомании // URL: https://kubnews.ru/obshchestvo/2018/10/12/mozhno-li-izlechitsya-ot-narkomanii.

[349] Постановление Правительства РФ от 09.02.2022 № 140 "О единой государственной информационной системе в сфере здравоохранения" (вместе с "Положением о единой государственной информационной системе в сфере здравоохранения") // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1152.

[350] Федеральный закон от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" // "Собрание законодательства РФ", 28.11.2011, № 48, ст. 6724.

Федерации, получивших заключение об отсутствии медицинских противопоказаний на работу с государственной тайной" и пп. "г 2" "федеральный реестр иностранцев и лиц без гражданства, получивших заключение об отсутствии медицинских противопоказаний на работу с государственной тайной".

Необходимо отметить, что ЕГИСЗ не предполагает предоставление информации работодателям и органам безопасности об отсутствии соответствующих медицинских противопоказаний, поэтому целесообразно внести соответствующие дополнения в п. 51 Положения о ЕГИСЗ, дополнив его пп. "б 1" "автоматизированная информационная система Федеральной службы безопасности Российской Федерации".

Внесение вышеуказанных изменений в нормативные правовые акты необходимо, так как в Российской Федерации проводятся работы по созданию возможности для подписания трудового договора в электронной форме. Для этого работодатель проект трудового договора размещает на цифровой платформе "Работа в России"[351]. В трудовой договор из цифровой платформы "Госуслуги"[352] будут подгружаться все необходимые данные (идентифицируется субъект, сведения о рождении, об образовании и т.п.), а также все ограничения на работу (сведения о судимости и т.п.). Таким образом, необходимо, чтобы работодатель обладал сведениями о наличии медицинских противопоказаний.

С целью надлежащей идентификации граждан, допускаемых к государственной тайне, желательно внести соответствующее дополнение в п. 28.1 Инструкции по допуску об обязанности граждан проходить биометрическую идентификацию в ГИС "Единая система идентификации и аутентификации"[353] (ЕСИА).

---

[351] Постановление Правительства РФ от 13.05.2022 № 867 "О единой цифровой платформе в сфере занятости и трудовых отношений "Работа в России" (вместе с "Правилами функционирования единой цифровой платформы в сфере занятости и трудовых отношений "Работа в России") // "Собрание законодательства РФ", 23.05.2022, № 21, ст. 3446.

[352] Федеральный закон от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

[353] П. 19 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3448.

Ввиду глобального противостояния и введения санкций против Российской Федерации в соответствии с Законом об иностранных агентах[354] Министерством юстиции России[355] определён Реестр иностранных агентов[356], поэтому целесообразно, чтобы сведения из указанного реестра были видны в проекте электронного трудового договора.

7) Обеспечить доступ работодателей к информации о работниках, которые допущены к государственной тайне без проведения проверочных мероприятий через ЕПГУ с получением информации от АИС ФСБ России.

8) Обеспечить доступ юридических лиц к информации о лицензиатах на работу с государственной тайной одновременно с получением информации о допуске к государственной тайне их руководителей через ЕПГУ в установленном порядке через АИС ФСБ России.

3.2. Регулирование интеграционных процессов допуска и доступа субъектов к коммерческой и служебной тайне в условиях цифровой экономики

Коммерческая и служебная тайны являются, пожалуй, одними из самых сложных с точки зрения правового регулирования. В Российской Федерации понятия "коммерческая тайна" и "служебная тайна", как вид информации конфиденциального характера, появились только с распадом Советского Союза и перехода экономики на рыночные отношения, когда с января 1995 года вступил в силу Гражданский кодекс РФ (часть первая) и там была введена статья 139 "Служебная и коммерческая тайна" (утратила силу с января 2008 года). Позднее данные виды тайн были закреплены в "Перечне сведений конфиденциального

---

[354] Федеральный закон от 14.07.2022 № 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием" // "Собрание законодательства РФ", 18.07.2022, № 29 (ч. II), ст. 5222.

[355] Приказ Минюста РФ от 29.11.2022 № 307 "Об утверждении Порядка ведения реестра иностранных агентов и размещения содержащихся в нем сведений на официальном сайте Министерства юстиции Российской Федерации в информационно-телекоммуникационной сети "Интернет", Порядка принятия решения об исключении физического лица, впервые включенного в реестр иностранных агентов, из реестра иностранных агентов, формы заявления иностранного агента об исключении из реестра иностранных агентов" // URL: http://pravo.gov.ru.

[356] URL: https://minjust.gov.ru/uploaded/files/reestr-inostrannyih-agentov-01-12-2022.pdf.

характера[357]", где под "служебной тайной" стали пониматься "служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами", а под "коммерческой тайной" – "сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами".

Ранее, в Советском Союзе, вышеуказанные виды тайн были объединены общим понятием "служебная информация ограниченного доступа", с т.н. грифом "Для служебного пользования" (сокращённо – "ДСП"), который являлся низшим грифом секретности[358]. В настоящее время при обращении с информацией, составляющей государственную тайну, в процессе её рассекречивания, изготовления выписок из секретных документов и т.п., активно используется ограничительная пометка "Для служебного пользования"[359].

С ноября 1994 года в Российской Федерации вышеуказанное понятие было модифицировано в понятие "служебная информация ограниченного распространения", которое стало распространяться только на федеральные органы исполнительной власти[360]. Необходимо отметить, что единый Федеральный закон, регулирующий такой вид тайны, как "служебная тайна", в нашей стране, так и не был принят[361].

---

[357] Указ Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера" // "Собрание законодательства РФ", 10.03.1997, № 10, ст. 1127.

[358] Постановление Секретариата ЦК РКП(б) от 30.08.1922 "О порядке хранения и движения секретных документов" // М.: Издание, 1925, а также последующие нормативно-правовые акты Правительства СССР.

[359] Например, "ГКИНП (ОНТА)-14-270-03. Геодезические, картографические инструкции, нормы и правила. Правила контроля отображения границ на картах, предназначенных для открытого опубликования и с пометкой "Для служебного пользования" (утверждены Приказом Роскартографии РФ от 17.07.2003 № 114-пр) // М.: ФГУП "Центральный картографо-геодезический фонд", 2003.

[360] См. Постановление Правительства РФ от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности" // "Собрание законодательства РФ", 25.07.2005, № 30 (ч. II), ст. 3165. (Далее по тексту – Положение).

[361] См. Паспорт проекта Федерального закона № 124871-4 (по состоянию на 01.05.1995 года) "О служебной тайне" // URL: http://sozd.duma.gov.ru.

В качестве разновидности "служебной тайны" Законом об обороне[362] предусмотрена "служебная тайна в области обороны", которым частично регулируются правоотношения, подпадающие под действие "государственной тайны" и частично под "служебную информацию ограниченного распространения". Таким образом, "служебная тайна в области обороны" требует дальнейшего исследования.

Что касается "коммерческой тайны", то порядок её использования регулируется соответствующим федеральным законом[363].

Несмотря на кажущиеся различия "коммерческая" и "служебная" тайны обладают общими требованиями к системам их технической защиты[364], а также к построению систем "допуска" и "доступа".

Правообладателями информации, составляющей "коммерческую" и "служебную" тайны, являются, соответственно, коммерческая организация и орган исполнительной власти, которые и определяют порядок "допуска" и "доступа" субъектов к указанной информации. Также необходимо отметить, что законодатель в указанных нормативно-правовых актах не выделил в качестве самостоятельных определений понятия "допуск" и "доступ", поэтому они приводятся в совокупности.

В Законе о коммерческой тайне можно выделить следующие основания "допуска" к информации, составляющей коммерческую тайну:

- для коммерческой организации – это введение в организации "режима коммерческой тайны"[365] и определение "Перечня информации, составляющей

---

[362] Ст. 3.1 Федерального закона от 31.05.1996 № 61-ФЗ "Об обороне" // "Собрание законодательства РФ", 03.06.1996, № 23, ст. 2750.

[363] Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне" // "Собрание законодательства РФ", 09.08.2004, № 32, ст. 3283. (Далее по тексту – Закон о коммерческой тайне).

[364] См. Руководящий документ ФСТЭК РФ. "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" (утв. Решением Гостехкомиссии РФ от 30.03.1992) и др. // URL: https://fstec.ru/component/attachments/download/297.

[365] См. Постановление Двадцатого арбитражного апелляционного суда от 09.11.2016 № 20АП-6427/2016, Апелляционное определение Санкт-Петербургского городского суда от 27.09.2016 № 33-17808/2016 // URL: http://www.consultant.ru.

коммерческую тайну" (п. 1 ст. 3, п. 1 ч. 1, ч. 2 ст. 10 Закона о коммерческой тайне);

- для федеральных органов исполнительной власти – необходимо направление мотивированного требования[366] обладателю коммерческой тайны (ч. 1 ст. 6 Закона о коммерческой тайне);

- для работников организации – это заключение трудового договора с работодателем, обладателем коммерческой тайны, в котором отдельно прописаны условия о допуске работника к коммерческой тайне, либо предоставления соответствующего согласия, в случае заключения гражданско-правового договора (п. 4 ч. 1 ст. 10 Закона о коммерческой тайне);

- для государственных служащих – основанием для допуска к коммерческой тайне является наличие соответствующих функциональных обязанностей, определённых в служебном контракте руководителем федерального органа исполнительной власти (п. 3 ч. 1 ст. 16, п. 2 ч. 4 ст. 24 Закона о государственной службе[367]). Необходимо отметить, что в соответствии с п. 1.2 Положения государственные служащие, которые допущены к информации ограниченного распространения, автоматически допускаются и к коммерческой тайне, поступившей в федеральные органы исполнительной власти.

Процесс "доступа" к коммерческой тайне предусматривает, что обладатель информации определяет условия, при выполнении которых будет разрешён или запрещён доступ к информации (п. 3 ч. 2 ст. 6.1 Закона о коммерческой тайне). Закон о коммерческой тайне предусматривает следующие условия "доступа" к коммерческой тайне, когда:

- установлен специальный порядок обращения с коммерческой тайной и обеспечен контроль за его соблюдением (п. 2 ч. 1 ст. 10 Закона о коммерческой тайне);

---

[366] Ст. 25 Федерального закона от 26.07.2006 № 135-ФЗ "О защите конкуренции" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3434.

[367] Федеральный закон от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" // "Собрание законодательства РФ", 02.08.2004, № 31, ст. 3215.

- осуществлён учёт лиц, получивших доступ к коммерческой тайне (п. 3 ч. 1 ст. 10 Закона о коммерческой тайне);

- урегулированы правоотношения с работниками на основании трудовых договоров и с контрагентами[368] на основании гражданско-правовых договоров (п. 4 ч. 1 ст. 10 Закона о коммерческой тайне).

Что касается "служебной информации ограниченного распространения", то можно выделить следующие основания "допуска":

- для федеральных органов исполнительной власти – когда руководителем федерального органа исполнительной власти определены категории подчинённых должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, а также порядок её передачи другим субъектам (должностным лицам или федеральным органам исполнительной власти) (п. 1.5, 1.6 Положения);

- для коммерческих организаций – когда федеральный орган исполнительной власти делегирует свои полномочия коммерческой организации в рамках исполнения договора (соглашения и т.п.) (п. 1.5 Положения), т.е. фактически является "заказчиком работ";

- для государственных служащих – основанием для допуска к служебной информации ограниченного распространения является обязательная процедура оформления допуска с обязательным отражением факта допуска в служебном контракте (п. 3 ч. 1 ст. 16, п. 2 ч. 4 ст. 24 Закона о государственной службе[369]). При этом указанная процедура регулируется отдельно в каждом органе исполнительной власти с учётом особенностей, присущих этим органам[370];

---

[368] Постановление Восемнадцатого арбитражного апелляционного суда от 05.08.2014 № 18АП-7541/2014 // URL: http://www.consultant.ru.

[369] Федеральный закон от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" // "Собрание законодательства РФ", 02.08.2004, № 31, ст. 3215.

[370] Приказ Минфина РФ от 19.06.2019 № 98н "Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве финансов Российской Федерации и подведомственных ему организациях и о признании утратившим силу приказа Министерства финансов Российской Федерации от 26 марта 2018 г. № 53н" (вместе с "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения") // URL: http://www.pravo.gov.ru.

- для работников организации – это заключение трудового договора с работодателем (коммерческой организацией), которому федеральный орган исполнительной власти делегировал свои полномочия в рамках исполнения договора (соглашения и т.п.) (п. 1.5 Положения). Необходимо отметить, что в действующем законодательстве данный вопрос специально не урегулирован и осуществляется по аналогии права (по аналогии с коммерческой тайной).

Процесс "доступа" к служебной информации ограниченного распространения законодательно не урегулирован, а отдан на откуп руководителям федеральных органов исполнительной власти. Отсутствие внятной концепции закрытости / транспарентности органов исполнительной власти приводит к отсутствию чётких законодательных положений, касающихся оборота служебной информации ограниченного распространения и, в свою очередь, к противоречиям в её правовом закреплении.

Одним из условий ограничения права на доступ к служебной информации ограниченного распространения указана "служебная необходимость", что предоставляет руководителю федерального органа исполнительной власти широкие дискреционные полномочия по отнесению той или иной информации к "служебной". Необходимо отметить, что в ч. 3 ст. 55 Конституции РФ и в ч. 1 ст. 9 Закона об информации определено: "ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства". Вышеуказанные нормативные акты такой цели ограничения доступа к информации, как "служебная необходимость", не предусматривают.

Если проанализировать нормативные правовые акты ряда федеральных органов исполнительной власти[371], то становится, очевидно, что в них фактически

[371] Приказ Минобрнауки РФ от 22.10.2018 № 51н "Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и его территориальных органах" (вместе с "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения"); Приказ МВД РФ от 09.11.2018 № 755 "О некоторых вопросах обращения со

вопрос доступа к служебной информации ограниченного распространения не урегулирован и всё ограничено общими положениями. Ряд федеральных органов исполнительной власти в своих нормативных документах допускают подмену понятий[372], когда к информации ограниченного распространения не приравнивают, а напрямую относят другие виды тайн (коммерческую тайну, профессиональную тайну, персональные данные). На указанную информацию проставляют ограничительную пометку "Для служебного пользования". Необходимо отметить, что когда в указанных федеральных органах исполнительной власти производится снятие ограничительной пометки "Для служебного пользования", то условия ограничения доступа к другим видам тайн (коммерческой тайне, профессиональной тайне, персональным данным), как правило, не восстанавливаются. Данное обстоятельство ставит под угрозу безопасность информации, переданной в федеральные органы исполнительной власти другими субъектами (коммерческой тайне, профессиональной тайне, персональным данным), и создаёт предпосылки к осуществлению несанкционированного доступа к ней неограниченного круга лиц.

В отдельных случаях, федеральные органы исполнительной власти наоборот часть информации, которая может быть отнесена к "служебной информации ограниченного распространения", относят к другим видам тайн или к информации с неопределённым правовым статусом. Например, Федеральная налоговая служба РФ в своих нормативных документах[373] разделила "налоговую

служебной информацией ограниченного распространения в системе МВД России" (вместе с "Инструкцией по организации деятельности по обращению со служебной информацией ограниченного распространения в системе МВД России"); Приказ МНС РФ от 03.03.2003 № БГ-3-28/96 "Об утверждении Порядка доступа к конфиденциальной информации налоговых органов" // URL: http://www.pravo.gov.ru.

[372] Приказ Минфина РФ от 17.06.2014 № 162 "Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации и организаций, находящихся в его ведении"; Приказ Ространснадзора РФ от 05.02.2016 № СС-94фс "Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Федеральной службы по надзору в сфере транспорта и её территориальных органов" // URL: http://www.pravo.gov.ru.

[373] Приказ ФНС РФ от 31.12.2009 № ММ-7-6/728@ "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в налоговых органах" (утратил силу с 21.04.2021) // URL: http://www.pravo.gov.ru.

тайну"[374] и "служебную информацию ограниченного распространения", однако, по своей правовой природе "налоговая тайна" может быть отнесена к "служебной информации ограниченного распространения". После публикации[375] автором указанной правовой коллизии Федеральной налоговой службой РФ был издан новый приказ[376], в котором указанная коллизия была устранена.

В связи активным внедрением в деятельность федеральных органов исполнительной власти информационных систем и электронного документооборота[377], предоставления государственных и муниципальных услуг в электронной форме происходит поиск наиболее оптимальных путей и форм управления обществом и государством, что является главной проблемой развития Российской Федерации[378]. Внешне это выражается в реорганизации системы государственных органов, активном внедрении электронных форм взаимодействия и управления, повышении их открытости и прозрачности.

Необходимость правового регулирования института служебной тайны в условиях "цифровой экономики" обусловлено целым рядом факторов, среди которых:

- отсутствие в современном законодательстве единого подхода к "служебной информации ограниченного распространения" приводит к тому, что в

---

[374] Ст. 102 "Налогового кодекса Российской Федерации (часть первая)" от 31.07.1998 № 146-ФЗ // "Собрание законодательства РФ", № 31, 03.08.1998, ст. 3824.

[375] Борисов М.А., Северин В.А. Проблемы допуска и доступа субъектов к коммерческой и служебной тайне в условиях цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2019, № 6. С. 238-241.

[376] Приказ ФНС РФ от 21.04.2021 № ЕД-7-24/391@ "О работе с несекретной информацией, доступ к которой ограничен федеральным законодательством, а также служебной информацией, ограничение на распространение которой диктуется служебной необходимостью" (вместе с "Порядком организации защиты служебной информации ограниченного распространения в налоговых органах", "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей служебной информации ограниченного распространения") // URL: http://www.pravo.gov.ru.

[377] Федеральный закон от 24.04.2020 № 122-ФЗ "О проведении эксперимента по использованию электронных документов, связанных с работой" // "Собрание законодательства РФ", 27.04.2020, № 17, ст. 2700; "Концепция развития электронного документооборота в хозяйственной деятельности", утверждена решением президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 25.12.2020 № 34) // URL: https://www.nalog.ru/html/sites/www.new.nalog.ru/docs/edo/edo_concept.pdf.

[378] "Основное препятствие: "Греф назвал главную проблему России". "Бизнес", 14.03.2019 // URL: https://www.gazeta.ru/business/2019/03/14/12242413.shtml.

процессе межведомственного информационного обмена в информационных системах циркулирует информация, обладающая разным уровнем важности (ценности), в результате чего возникают предпосылки к её неограниченному доступу, или накоплению, что в совокупности может относиться к "государственной тайне";

- возможность ограничения распространения (доступа) служебной информации по усмотрению руководителя федерального органа исполнительной власти (органа местного самоуправления), также не способствует её защищённости;

- отсутствие целостного государственного механизма защиты "служебной информации ограниченного доступа", поступающей в федеральные органы исполнительной власти (органы местного самоуправления) и накапливаемой ими провоцирует злоупотребления со стороны должностных лиц федеральных органов исполнительной власти при обращении с данной информацией, а также возникновению "коррупционной составляющей".

Данные настоящего исследования подтверждают вывод о том, что унификация правил введения, сохранения и прекращения конфиденциальности "служебной тайны" в федеральных органах исполнительной власти (в органах местного самоуправления) будет способствовать:

- единому пониманию "служебной тайны" со стороны должностных лиц федеральных органов исполнительной власти, а также других участников (субъектов) цифровой экономики;

- минимизации затрат на построение системы защиты "служебной тайны";

- формированию позитивного имиджа федеральных органов исполнительной власти, органов местного самоуправления, а также российского государственного аппарата в целом;

- сокращению случаев незаконного распространения и неправомерного использования "служебной информации ограниченного распространения" федеральных органов исполнительной власти (органов местного самоуправления);

- устранению "коррупционной составляющей" и возникновении потребности борьбы с ней и др.

В условиях "цифровой экономики" доля государственных информационных систем в обработке информации будет постоянно возрастать, где в общем массиве будет одновременно обрабатываться информация, составляющая служебную тайну, коммерческую тайну и персональные данные, при этом отделить данные виды тайн и обеспечить их самостоятельную защиту не представляется возможным. Ранее отмечалось (см. раздел 1.4 настоящей диссертации), что в ряде государств сложилась практика объединения разнородной информации и присвоение ей отдельного наименования (например, "официальная" и т.п.). В Российской Федерации сложилась несколько иная практика, когда информации, обрабатываемой федеральными органами исполнительной власти, присваивалась ограничительная пометка "Для служебного пользования". Учитывая сложившуюся международную практику и отечественный опыт, целесообразно всю информацию, которая обрабатывается в государственных информационных системах, отнести к "служебной тайне". Что касается "коммерческой тайны", то данная правовая норма будет сохранена, если информация будет обрабатываться только в информационной системе коммерческой организации.

Существующий пробел целесообразно восполнить путём принятия Федерального закона, в котором будет закреплено понятие "служебной тайны" и определено её место в общей системе тайн, а также установлен единый порядок обращения со "служебной тайной" в федеральных органах исполнительной власти и органах местного самоуправления. Важным является определение полномочий (пределы правоприменения) федеральных органов исполнительной власти и органов местного самоуправления по распоряжению "служебной тайной" с учётом баланса их интересов, в том числе при использовании информационных систем.

3.3. Оптимизация регулирования допуска и доступа субъектов к персональным данным в условиях цифровой экономики

Персональные данные являются одними из самых противоречивых и динамичных разновидностей информации, правовое регулирование которых претерпевает серьёзные изменения. Первое упоминание о "персональных данных" относится к периоду бурного развития вычислительных сетей и появлению такого понятия, как "база данных", когда в 1970 году в Германии (в ФРГ) в земле Гессен впервые был принят "Закон о персональных данных". После этого аналогичные законы были приняты в Швеции (в 1973 году[379]), в Соединённых Штатах (в 1974 году[380]), в Германии (в 1977 году[381]) и во Франции (в 1978 году[382]).

На международном уровне впервые регламентация персональных данных была осуществлена в 1980 году, когда были приняты "Основные положения о защите неприкосновенности частной жизни и международных обменов персональными данными[383]", в которых были зафиксированы основные принципы работы с ними. Позже на основе вышеуказанного нормативного акта были разработаны Конвенция Совета Европы "О защите прав личности в связи с

---

[379] В настоящее время действует "Федеральный акт о защите персональных данных" (Datenschutzgesetz 2000 – DSG 2000) // URL: https://wipolex.wipo.int/ru/legislation/profile/SE, а также законодательство Евросоюза (ЕС).

[380] В настоящее время законодательство о защите персональных данных в США представляет собой разрозненный набор действующих локальных нормативных актов и узкоспециализированных федеральных законов: регулирующих банковские организации (FCRA, 1970 и GLB, 1999), медицинские учреждения (HIPAA, 1996) и телекоммуникации (ECPA, 1986), также законы штатов. Например, в штате Калифорния действует более 25 законов штата о конфиденциальности и безопасности данных, в том числе и принятый "Калифорнийский закон о защите прав потребителей 2018 года" (CCPA), вступающий в силу 01.01.2020 года // URL: https://www.dlapiperdataprotection.com /?t=law&c=US.

[381] В настоящее время Германия привела немецкую правовую базу в соответствие с GDPR, приняв новый "Федеральный закон о защите данных Германии" (Bundesdatenschutzgesetz - BDSG) от 05.07.2017 года, который вступил в силу вместе с GDPR 25.05.2018 года // URL: https://www.dlapiperdataprotection.com/?t=law&c=DE.

[382] В настоящее время Франция адаптировала своё законодательство в соответствие с требованиями GDPR, внеся соответствующие изменения в "Law No. 78-17 of January 6, 1978 "On information technology, data files and civil liberties, the principal law regulating data protection in France", вступившие в силу с 01.07.2019 года // URL: https://www.dlapiperdataprotection.com/?t=law&c=FR.

[383] Защита персональных данных. Опыт правового регулирования / Сост. Е.К.Волчинская / Предисл. А.К.Симонов. М.: Галерея, 2001. 173 с. (С. 12-32).

автоматической обработкой персональных данных"(ETS № 108, г. Страсбург, 28.01.1981)[384] и Руководящие принципы Организации Экономического Сотрудничества и Развития (ОСЭР) "О защите приватности в связи с трансграничной передачей персональных данных[385]", которые существенно повлияли на дальнейшее развитие законодательства о персональных данных во всём мире[386].

В Российской Федерации правоотношения в области персональных данных регулируют Федеральный закон "О персональных данных"[387] (далее по тексту – Закон о персональных данных) и Закон об информации. В связи со стремительным развитием "цифровой экономики" и дальнейшим формированием международной нормативной базы вышеуказанные федеральные законы постоянно подвергаются существенной доработке. Следует подчеркнуть, что по состоянию на апрель 2023 года Закон об информации претерпел пятьдесят восемь редакций, а Закон о персональных данных – двадцать девять. Кроме того, издано более тридцати подзаконных актов, регламентирующих деятельность в области сбора, хранения, уничтожения и обращения с персональными данными граждан Российской Федерации.

Мировое нормотворчество в области обработки персональных данных адаптируется с учётом требований изложенных в "Генеральном регламенте о защите персональных данных[388]" (англ. General Data Protection Regulation, GDPR) (далее по тексту – Генеральный регламент), введённом в действие Постановлением Европейского Союза № 2016/679 от 27.04.2016 года.

---

[384] Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью / Сост.: Ю.Н.Жданов, В.П.Зимин, Т.Н.Москалькова, В.С.Овчинский, Н.Б.Слюсарь, В.В.Черников. М.: СПАРК, 1998. 388 с. (С. 106-114).

[385] Материал с официального сайта ОСЭР // URL: http://oecdru.org/oecd_rf.html.

[386] Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. № 8. Изд. 3. М.: Ленанд, 2020. 224 с.

[387] Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3451.

[388] Регламент № 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий Регламент о защите персональных данных)" (Принят в гор. Брюсселе 27.04.2016) // URL: http://eur-lex.europa.eu.

Вступивший в силу с 25.05.2018 года Генеральный регламент расширил сферу действия европейского законодательства, детализировал права субъектов персональных данных и ужесточил обязанности операторов при обработке и защите персональных данных с учётом современных технологий. Обязательства по соблюдению Генерального регламента распространяются не только на юридических лиц, ведущих деятельность на территории двадцати восьми стран Европейского Союза, но и на любые юридические лица вне зависимости от их местонахождения, при условии, что они обрабатывают персональные данные граждан Европейского Союза.

Необходимо отметить, что Генеральный регламент позаимствовал много положений из российского законодательства в области защиты персональных данных, однако, соответствие отечественному законодательству не обеспечивает автоматическое соблюдение Генерального регламента, так как ряд процессов и требований введены Генеральным регламентом впервые.

В соответствии с Законом о персональных данных под "персональными данными" понимается "любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)"[389], а под "обработкой персональных данных" понимается "любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных[390]". Также к вопросам обработки персональных данных относится и обеспечение "допуска" и "доступа" субъектов к персональным данным. В Законе о персональных данных не выделено самостоятельного понятия "допуск" и закон оперирует только понятием "доступ". Необходимо отметить, что понятие "персональные данные"

[389] П. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3451.

[390] П. 3 ст. 3 Там же.

изначально вводилось исключительно для обозначения цели систематизации информации, обрабатываемой в электронном виде в информационных системах.

Законодательство о персональных данных выделяет трёх субъектов персональных данных, которым необходим "допуск" и "доступ" к обрабатываемым персональным данным:

- физическое лицо, персональные данные которого подлежат обработке (ст. 9, 14 Закона о персональных данных);

- юридическое лицо (оператор[391]), который обрабатывает персональные данные и к которому относятся:

а) оператор персональных данных, находящийся на территории Российской Федерации (ст. 18 Закона о персональных данных);

б) оператор персональных данных, находящийся за пределами территории Российской Федерации (ст. 12 Закона о персональных данных);

в) федеральный орган исполнительной власти – оператор персональных данных (ст. 13 Закона о персональных данных);

- иное лицо – юридическое лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных.

Необходимо отметить, что российское и международное законодательство[392] имеет схожее понятие "оператор персональных данных".

В отношении субъектов, чья обработка персональных данных осуществляется, ч. 3 ст. 14 Закона о персональных данных предусматривает право субъекта на получение информации от оператора о характере обрабатываемых его персональных данных. Указанные права субъект персональных данных может реализовать через своего доверителя[393].

---

[391] Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 Закона о персональных данных).

[392] Opinion 1/2010 On the concepts of "controller" and "processor". Article 29 Data Protection Working Party. 16 February.

[393] Ст. 185 "Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

С целью своей идентификации (фактически получения "допуска" к своим персональным данным) субъект персональных данных в адрес оператора персональных данных направляет запрос, который содержит:

- сведения о документе, удостоверяющем личность[394];

- подтверждение участия субъекта в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

- подпись субъекта персональных данных. Субъект может выразить своё согласие в виде графической подписи, электронной подписи (как квалифицированной, так и простой), в устной форме с применением биометрического подтверждения голоса[395] и аудиозаписи заявления. С развитием искусственного интеллекта и технологии "NuDetect[396]" получит своё развитие конклюдентная форма подтверждения согласия субъекта.

В современный период активно развиваются системы геномной идентификации[397] субъектов персональных данных, которые являются составной

---

[394] Указ Президента РФ от 13.03.1997 № 232 "Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации" // "Собрание законодательства РФ", 17.03.1997, № 11, ст. 1301; Постановление Правительства РФ от 08.07.1997 № 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" // "Собрание законодательства РФ", 14.07.1997, № 28, ст. 3444.

[395] Например, Национальный стандарт РФ. "ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018). Информационные технологии. Биометрия. Общие положения и примеры применения" (утв. Приказом Росстандарта РФ от 19.11.2019 № 1184-ст) // М.: Стандартинформ, 2019.

[396] Технология "NuDetect" в настоящее время активно развивается в банковской деятельности и помогает идентифицировать личность клиентов, используя их естественное поведение при удалённой работе с банковским приложением (см. URL: https://developer.mastercard.com/product/nudetect).

[397] Федеральный закон от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740; Постановление Правительства РФ от 11.10.2011 № 828 "Об утверждении Положения о порядке проведения обязательной государственной геномной регистрации лиц, осуждённых и отбывающих наказание в виде лишения свободы" // "Собрание законодательства РФ", 17.10.2011, № 42, ст. 5926; Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19794-14-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК" (утв. Приказом Росстандарта РФ от 09.06.2017 № 528-ст) // М.: Стандартинформ, 2018.

частью общей системы развития генетических технологий в Российской Федерации[398], что соответствует международной тенденции[399].

В совокупности с положениями Генерального регламента зарубежными специалистами предлагается, в частности выработать систему инструментов информационного права, когда геномный образ человека будет отнесён к персональным данным[400]. В том же направлении движется и российское законодательство в области персональных данных[401], предполагающее на первом этапе провести генетическую паспортизацию граждан Российской Федерации.

Решение данного вопроса имеет важное значение для обеспечения безопасности страны. Сбор геномных персональных данных граждан Российской Федерации будет способствовать повышению эффективности борьбы с преступностью, в том числе с терроризмом и экстремизмом, а также будет иметь профилактическое значение и окажет позитивное влияние на криминогенную ситуацию в стране. Создание "Федеральной базы данных геномной информации[402]" (ФБДГИ) граждан Российской Федерации позволит оперативно выявлять и устранять наследственные патологические заболевания, предсказывать эффективность или аллергенность некоторых лекарственных средств, что позволит разрабатывать индивидуальные лекарственные средства, средства против биологического оружия, оперативно локализовывать эпидемии и повышать уровень биологической безопасности России.

---

[398] Указ Президента РФ от 28.11.2018 № 680 "О развитии генетических технологий в Российской Федерации" (вместе с "Положением о совете по реализации Федеральной научно-технической программы развития генетических технологий на 2019 - 2027 годы") // "Собрание законодательства РФ", 03.12.2018, № 49 (ч. VI), ст. 7586.

[399] "Концепция ответственного обмена геномными данными и данными, связанными со здоровьем человека" // https://www.ga4gh.org/wp-content/uploads/Framework-Russian-translation.pdf.

[400] Бикбулатова Ю.С., Дупан А.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт // "Российская юстиция", 2019, № 9.

[401] Указ Президента РФ от 11.03.2019 № 97 "Об Основах государственной политики Российской Федерации в области обеспечения химической и биологической безопасности на период до 2025 года и дальнейшую перспективу" // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1106; Паспорт проекта Федерального закона № 744029-7 "О внесении изменений в статью 11 Федерального закона "О персональных данных" в части обработки биометрических персональных данных" // URL: http://www.consultant.ru.

[402] См. п. 5 ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740.

ФБДГИ создавалась в соответствии с принятой во многих странах мира аналогичной системой Combined DNA Index System (CODIS), что гарантирует сопоставимость данных, как в России, так и за рубежом в рамках межгосударственного сотрудничества, в том числе по линии Интерпола.

Вместе с тем, как показывает исследование, сбор геномной информации порождает целый ряд морально-этических и других проблем. Так, наличие тех или иных геномных отклонений субъекта может привести к его дискриминации по геномному признаку. Например, запрет на рождение детей некоторыми парами, обязательный отбор и отбраковка предимплантационных эмбрионов и даже аборты по таким медицинским показаниям, работодатели будут отказывать в приёме на работу лицам с сердечно-сосудистыми и другими заболеваниями, будут отбраковывать спортсменов без потенциальных задатков в повышенной выносливости, силы и т.п.

Неправомерное использование геномной информации может спровоцировать повышение доли преступлений в отношении граждан Российской Федерации. Так, утечка информации из ФБДГИ позволит "чёрным трансплантологам" получить информацию о потенциальном доноре-жертве, что может привести к его преждевременной гибели. Хищение геномной информации иностранными спецслужбами позволит создать "генетическое оружие" в отношении многонационального состава граждан Российской Федерации.

В 2009 году в Израиле был проведён эксперимент, когда были сфабрикованы геномные доказательства (кровь и слюна) человека, который на "месте преступления" не был, однако "преступникам" заранее был известен ДНК-профиль данного человека[403]. Следует отметить, что подобная ситуация создает огромные возможности для злоупотребления генетической информацией субъекта, в т.ч. кражу его генетической идентичности.

[403] Богданова Е.Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация // "Lex russica", 2019, № 6.

Анализ публикаций показывает, что геномная информация[404] является необычной категорией персональных данных, требующей усиленной защиты. Ряд правоведов справедливо предлагает[405] обособить геномные данные в Законе о персональных данных, Законе об информации и в законодательстве об охране здоровья граждан, отдельно оговорив условия предоставления геномной информации членам семьи субъекта персональных данных, а также условия формирования биобанков и системы RWD[406] (англ. "real world data").

Представляется, что при отнесении геномной информации к персональным данным необходимо учитывать следующие особенности:

а) одним из условий законности обработки собираемой генетической информации является её целевое ограничение, которое ограничивает свободу исследователя идти на новые открытия и инновации в этой области. Развитие технического прогресса с течением времени будет открывать новые условия и цели обработки геномной информации. Таким образом, принцип "целевого ограничения" геномных персональных данных в данном случае неприменим;

б) по мере развития "цифровой экономики" значение ФБДГИ будет возрастать соответственно, можно ожидать увеличения объёмов и качества собираемой генетической информации. Это, в свою очередь, будет способствовать повышенному интересу разведок иностранных государств и криминальных структур к обрабатываемой в ФБДГИ генетической информации. Степень ущерба, который может быть нанесён Российской Федерации в случае утраты / хищения генетической информации, значителен. Отсюда следует необходимость повышения требований к защите генетической информации, обрабатываемой в ФБДГИ на уровне государства. Существующие сегодня

---

[404] См. п. 3 ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740.

[405] Комментарий к Федеральному закону от 3 декабря 2008 г. № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" (постатейный) / отв. ред. Е.Н. Холопова // СПС КонсультантПлюс, 2016; Бикбулатова Ю.С., Дупан А.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт М.: "Российская юстиция", 2019, № 9.

[406] Данные реального мира (RWD) в медицине – это данные, которые получены из ряда не связанных между собой источников: электронных медицинских карт, опросов пациентов, клинических испытаний и наблюдательных (когортных), контролируемых (рандомизированных) исследований и др.

требования к защите персональных данных не обеспечивают адекватных мер защиты, поэтому целесообразно генетическую информацию, содержащуюся в ФБДГИ, отнести к государственной тайне. Причём мероприятия по допуску к государственной тайне, нужно проводить и в отношении должностных лиц, осуществляющих обработку генетической информации в ФБДГИ.

Следующий важный вопрос – это обработка персональных данных. Закон о персональных данных предусматривает два основных условия обработки персональных данных, которые оператор получил от субъекта:

- с письменного согласия[407] субъекта персональных данных (ст. 6, ст. 9 Закона о персональных данных), что фактически является оформленным "допуском";

- без письменного согласия субъекта персональных данных (в рамках исполнения закона / государственных интересов[408]) (ст. 6, ч. 8 ст. 14 Закона о персональных данных).

Оператор обязан уведомить уполномоченный орган[409] об обработке персональных данных, за исключением случаев, когда обработка персональных данных осуществляется в рамках трудовых и гражданско-правовых отношений, обработки общедоступной информации, информации, включённой в государственные информационные системы, при обеспечении безопасности и т.п. (ч. 2 ст. 22 Закона о персональных данных). При этом уполномоченный орган

---

[407] Ст. 65 "Трудового кодекса Российской Федерации" от 30.12.2001 № 197-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 3; Ч. 4 ст. 8 Федерального закона от 28.03.1998 № 53-ФЗ "О воинской обязанности и военной службе" // "Собрание законодательства РФ", 30.03.1998, № 13, ст. 1475.

[408] Федеральный закон от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" // "Собрание законодательства РФ", 13.08.2001, № 33 (ч. I), ст. 3418.

[409] 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") // "Собрание законодательства РФ", 23.03.2009, № 12, ст. 1431; Приказ Роскомнадзора РФ от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения" // URL: http://www.pravo.gov.ru.

обязан проводить периодический государственный контроль и надзор за обработкой персональных данных[410] в случае, если оператор осуществляет:

- обработку персональных данных в государственных информационных системах[411] (ст. 13 Закона о персональных данных);

- сбор биометрических и специальных категорий персональных данных[412] (ст. 10, ст. 11 Закона о персональных данных);

- трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных (ст. 12 Закона о персональных данных) или обработку персональных данных по поручению иностранного государственного органа (юридического лица, физического лица), который не зарегистрирован в установленном порядке на территории Российской Федерации[413].

При обработке персональных данных субъектов оператор решает две основные задачи:

- обеспечение "допуска" и доступа" к персональным данным работников оператора (ст. 18.1 Закона о персональных данных);

---

[410] Постановление Правительства РФ от 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных" (вместе с "Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных") // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. III), ст. 5424.

[411] Постановление Правительства РФ от 15.10.2021 № 1753 "Об утверждении требований к организационным и техническим условиям осуществления многофункциональными центрами предоставления государственных и муниципальных услуг размещения или обновления в единой системе идентификации и аутентификации сведений, необходимых для регистрации физических лиц в данной системе, размещения биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, с использованием программно-технических комплексов" // "Собрание законодательства РФ", 25.10.2021, № 43, ст. 7251.

[412] Постановление Правительства РФ от 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" // "Собрание законодательства РФ", 09.07.2018, № 28, ст. 4234.

[413] Федеральный закон от 01.07.2021 № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. I), ст. 5064.

- обеспечение к "допуска" и "доступа" к персональным данным субъектов персональных данных в соответствии с целями обработки персональных данных (п. 2, 4, 5 ст. 5 Закона о персональных данных).

Механизм обеспечения "допуска" и доступа" к персональным данным работников оператора Законом о персональных данных не урегулирован и фактически отдан на откуп оператору. Так, в ряде локальных нормативных актах[414] под "допуском к обработке персональных данных операторов" понимается "процедура оформления права на доступ к персональным данным", оформляется "допуск" путём "издания приказа о назначении работника на должность, должностной инструкции, предусматривающей обработку персональных данных, заключением обязательства о неразглашении персональных данных[415]". В свою очередь, под "доступом" понимается "возможность обработки персональных данных[416]", при этом "представители сторонних организаций допускаются на основании заключённых договоров, который должен содержать перечень действий (операций) с персональными данными, цели обработки, обязанность лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также перечень требований по защите обрабатываемых персональных данных[417]".

Изучение показывает, что с каждым годом объёмы обработки информации постоянно увеличиваются, в том числе растёт объём обработки и персональных данных. Поэтому всё чаще операторы поручают обработку персональных данных третьим лицам, к которым, как правило, относятся различные аутсорсинговые организации (например, ведение бухгалтерии, предоставление вычислительных мощностей и т.п.). В ч. 3 ст. 6 Закона о персональных данных под иными лицами

---

[414] Например, в пп. 1 п. 3 "Порядка обработки и обеспечения режима защиты персональных данных работников ОАО "РЖД"", утверждённого Приказом ОАО "РЖД" от 20.07.2016 № 60 "Об обеспечении защиты персональных данных в ОАО "РЖД" // URL: http://www.consultant.ru.

[415] См. п. 4 Там же.

[416] См. пп. 2 п. 3 Там же.

[417] См. п. 8, 21 Там же.

понимается "лицо, осуществляющее обработку персональных данных по поручению оператора". Ключевыми характеристиками такого лица являются:

- наличие самостоятельной правосубъектности (лицо юридически самостоятельное по отношению к оператору);

- обработка данных осуществляется таким лицом в интересах оператора.

В европейском законодательстве связка "оператор" – "иное лицо" рассматривается как "оператор" (англ. "data controller") – "обработчик" (англ. "data processor")[418].

Главным отличием оператора от иного лица является распределение ответственности между ними. Так иное лицо не обязано получать согласие субъекта персональных данных на их обработку. В соответствии с ч. 4, 5 ст. 6 Закона о персональных данных оператор несёт ответственность[419] перед субъектом персональных данных за действия иного лица, а иное лицо, в свою очередь, – перед оператором. Таким образом, субъект персональных данных в силу закона не может предъявить свои требования напрямую иному лицу, такие требования должны быть предъявлены непосредственно оператору.

В данном случае необходимо отметить, что иное лицо по отношению к различным персональным данным может выступать и в роли оператора (например, в отношении своих работников и т.п.). Допуск к обработке персональных данных в интересах оператора "иное лицо" получает в соответствии с поручением оператора. Закон о персональных данных не предусматривает формы и характер такого поручения, которое может представлять собой отдельный договор или отдельные условия в ином договоре. Как правило, заключается агентский договор, договор возмездного оказания услуг и т.п.

В ситуации, когда иное лицо может находиться на территории иностранного государства, законодатель предусмотрел допуск такого лица к персональным данным путём реализации "трансграничной передачи персональных данных". Под

---

[418] Opinion 1/2010 On the concepts of "controller" and "processor". Article 29 Data Protection Working Party. 16 February 2010.

[419] См. ст. 13.11, 13.14, 13.14.1 "Кодекса Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 1.

"трансграничной передачей персональных данных" понимается отдельный вид обработки таких данных, который заключается в передаче их "на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу" (п. 11 ст. 3 Закона о персональных данных). Таким образом, персональные данные выходят из-под юрисдикции Российской Федерации и попадают под юрисдикцию другого государства.

В практике различают следующие особенности трансграничной передачи персональных данных, которые нужно учитывать субъектам:

- трансграничная передача персональных данных на территорию иностранных государств, являющихся сторонами "Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[420]", а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных[421]. (ч. 1, 2 ст. 12 Закона о персональных данных);

- трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (ч. 4 ст. 12 Закона о персональных данных).

Закон о персональных данных не вводит специальных ограничений на трансграничную передачу персональных данных, однако необходимо выполнить ряд условий:

- собираемые оператором персональные данные российских пользователей в обязательном порядке должны сначала "осесть" (локализоваться, зафиксироваться) на территории Российской Федерации, и лишь после этого они

---

[420] "Конвенция о защите физических лиц при автоматизированной обработке персональных данных" (заключена в гор. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 419.

[421] Приказ Роскомнадзора РФ от 05.08.2022 № 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" // URL: http://pravo.gov.ru; Письмо Минкомсвязи РФ от 13.05.2009 № ДС-П11-2502 "Об осуществлении трансграничной передачи персональных данных" // URL: http://www.consultant.ru.

могут быть переданы иностранному лицу (оператору, обработчику) с соблюдением положений ст. 12 Закона о персональных данных (ч. 5 ст. 18 Закона о персональных данных);

- решением федерального органа исполнительной власти[422] может быть запрещена[423] трансграничная передача персональных данных иностранным лицам[424], в целях защиты нравственности, здоровья, прав и законных интересов граждан[425];

- такое освобождение происходит, если обработка персональных данных осуществляется:

а) для достижения целей, предусмотренных международным договором РФ или законом, для выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей[426];

б) в целях отправления правосудия, исполнения судебного акта;

в) для исполнения полномочий государственными и муниципальными органами;

---

[422] 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") // "Собрание законодательства РФ", 23.03.2009, № 12, ст. 1431.

[423] Постановление Правительства РФ от 10.01.2023 № 6 "Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении" // URL: http://pravo.gov.ru.

[424] Ст. 16 Федерального закона от 01.07.2021 № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. I), ст. 5064.

[425] Постановление Правительства РФ от 16.01.2023 № 24 "Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан" // URL: http://pravo.gov.ru.

[426] Постановление Правительства РФ от 29.12.2022 № 2526 "Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3-6, 8-11 статьи 12 Федерального закона "О персональных данных" // "Собрание законодательства РФ", 02.01.2023, № 1 (ч. II), ст. 326.

г) в целях ведения профессиональной деятельности журналиста и / или законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности.

Законом о персональных данных также предусмотрена возможность субъекту относить свои персональные данные к категории общедоступных (ст. 8 Закона о персональных данных). При этом оператор имеет право обрабатывать персональные данные только с письменного согласия субъекта, что является "допуском". Закон о персональных данных не содержит определения "общедоступные категории персональных данных". К источникам образования общедоступных персональных данных относятся различные справочники (телефонные, Интернет-адресов и т.п.), Интернет-площадки для публикаций информации, порталы "открытых данных" и т.п., которые не предполагают какого-либо ограничения к информации[427]. При этом под общедоступными источниками персональных данных понимаются лишь те, которые создаются по инициативе оператора. К данной категории не относятся информационные системы оператора, которые собирают персональные данные в целях исполнения требований законодательства о раскрытии или опубликовании определённой информации[428] (п. 11 ч. 1 ст. 6 Закона о персональных данных).

На основе вышеизложенного, можно выделить несколько проблем с обеспечением "допуска" и "доступа" субъектов к персональным данным:

1) Характер обрабатываемых персональных данных является весьма разнородным: от "общедоступных" до "генетических", которые по своему характеру наносят различный ущерб[429] в случае их утраты / хищения разведками

---

[427] "Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе" (утв. ФССП РФ 30.11.2010 № 02-7) // "Бюллетень Федеральной службы судебных приставов", № 1, 2011.

[428] Например, не относятся сведения о ЕГРЮЛ (см. Постановление Президиума Нижегородского областного суда от 06.07.2016 по делу № 44г-49/2016 // URL: http://www.consultant.ru).

[429] Приказ Минцифры РФ от 25.05.2021 № 494 "Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного

иностранных государств и криминальными структурами. В соответствии с п. 5 ч. 1 ст. 18.1 Закона о персональных данных оценка ущерба отнесена в ведение оператора, в результате чего разрабатываемые на местах методики оценки[430] носят формальный характер и не отражают прогноз ущерба, который реально может возникнуть. Если для общедоступных персональных данных это не является критичным, то для информации, обрабатываемой в государственных информационных системах, это может привести к значительному ущербу Российской Федерации.

2) Действующее законодательство в области персональных данных урегулирует только вопросы, связанные с технической защитой персональных данных в информационных системах[431], при этом механизм "допуска" работников (в плане их проверки на предмет действий оформляемого лица, создающих угрозу безопасности Российской Федерации), по аналогии с механизмом допуска к государственной тайне не предусмотрен.

3) Действующее законодательство в области персональных данных не урегулирует механизм "допуска" и "доступа" работников оператора к персональным данным субъекта персональных данных, предъявляя лишь

самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учётом оценки возможного вреда, проведённой в соответствии с законодательством Российской Федерации о персональных данных" // URL: http://pravo.gov.ru.

[430] Постановление Администрации Тамбовской области от 26.06.2018 № 626 "Об утверждении правил оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации области" // URL: http://docs.cntd.ru/document/550130088.

[431] Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // "Собрание законодательства РФ", 05.11.2012, № 45, ст. 6257; Приказ ФСТЭК РФ от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" // "Российская газета", № 107, 22.05.2013; Приказ ФСБ РФ от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости" // "Российская газета", № 211, 17.09.2014.

требование к деловой репутации оператора[432]. Порядок "допуска" и "доступа" работников отдан на откуп оператору персональных данных.

4) Развитие "цифровой экономики" Российской Федерации стимулирует развитие различных информационных систем, в том числе и государственных информационных систем, в которых накапливаются и обрабатываются персональные данные[433], так с 30.12.2021 года в России создана "единая информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица".

5) В государственных информационных системах обрабатываются персональные данные, объём и важность которых может нанести значительный ущерб безопасности Российской Федерации в случае их утраты / хищения разведками иностранных государств и криминальными структурами[434].

Существующий пробел целесообразно восполнить путём внесения изменений в следующие нормативные правовые акты (см. приложение 2):

1) Необходимо отнести государственные информационные системы, в т.ч. и ФБДГИ, в которых обрабатывается информация обо всех гражданах Российской Федерации (лицах без гражданства / иностранных гражданах) к объектам критической информационной инфраструктуры. Для этого п. 8 ст. 2 Федерального

---

[432] Приказ Минцифры РФ от 27.08.2021 № 896 "Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающей услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц" // URL: http://pravo.gov.ru.

[433] 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.

[434] URL: https://ics-cert.kaspersky.ru/media/Threats_to_Biometrics_FINAL-RU.pdf.

закона "О безопасности критической информационной инфраструктуры Российской Федерации"[435] необходимо изложить в следующей редакции:

"8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, обработки биометрической и геномной информации, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей, а также государственные информационные системы, в которых централизованно обрабатываются персональные данные всех граждан Российской Федерации".

Это позволит существенно повысить защищённость биометрической и геномной информации, а также персональных данных обрабатываемых в соответствующих государственных информационных системах.

2) Необходимо внести следующие дополнения в ст. 5 Закона о государственной тайне:

"2) сведения в области экономики, науки и техники:

об информации, содержащейся в "Единой информационной системе персональных данных Российской Федерации"[436];

---

[435] Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // "Собрание законодательства РФ", 31.07.2017, № 31 (ч. I), ст. 4736.

[436] Постановление Правительства РФ от 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" // "Собрание законодательства РФ", 09.07.2018, № 28, ст. 4234.

об информации, содержащейся в "Федеральной базе данных геномной информации[437]"".

Отнесение вышеуказанной информации к государственной тайне будет способствовать тому, что должностные лица, которые будут участвовать обработке указанной информации, будут допускаться к ней по правилам, предусмотренным к государственной тайне[438].

Внесение данных правовых норм позволит существенно снизить коррупционную составляющую со стороны должностных лиц, осуществляющих работу с массивами персональных данных граждан Российской Федерации, так как на них будет распространяться соответствующая уголовная[439] и административная[440] ответственность.

---

[437] П. 5 ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740.

[438] Постановление Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

[439] Ст. 275, 275.1, 276, 283, 283.1, 284 "Уголовного кодекса Российской Федерации" от 13.06.1996 № 63-ФЗ // "Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954.

[440] Ч. 7 ст. 13.12, ч. 7 ст. 13.15 "Кодекса Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 1.

ЗАКЛЮЧЕНИЕ

Результаты проведённого исследования правового регулирования допуска и доступа субъектов к информации в условиях цифровой экономики позволяют сделать следующие выводы и представить следующие предложения по повышению эффективности нормативно-правового регулирования, совершенствованию нормативно-правовой базы и организационной структуры государственного управления информацией в условиях цифровой экономики.

В ходе анализа понятий "информация", а также "допуск" и "доступ" была установлена необходимость в совершенствовании терминологического аппарата и унификации указанных терминов и определений с учётом развития "цифровой экономики", в процессе развития которой существенно меняются функции указанных понятий. Так информация, обрабатываемая вне информационной системы, оценивается как нечто неопределённое, не подлежащее систематизации, то информация, обрабатываемая в информационной системе, – это товар, продукция, предмет труда и объект услуг, которое подлежит систематизации и классификации. Аналогичная проблема имеет место и в отношении понятий "допуск" и "доступ", когда для информационных систем целесообразно использовать терминологию, применяемую в области информационных технологий: "идентификация" и "аутентификация". Выполнение указанных предложений позволит прийти к единому пониманию понятий "допуск" и "доступ", что позволит исключить двоякое толкование в нормативных правовых актах, и будет препятствовать выработке псевдо-правовых норм и проявлению "коррупционной" составляющей.

Результаты проведённого исследования позволяют предложить необходимость чёткой систематизации и унификации общедоступной информации и информации ограниченного доступа, так как имеющаяся в Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" классификация информации неприменима в "цифровой экономике".

Исследование порядка допуска и доступа к государственной тайне выявило серьёзные проблемы в порядке их осуществления, которые создают предпосылки для злоупотребления правом и "коррупционной составляющей" со стороны соответствующих должностных лиц, а также неготовность системы к работе в условиях "цифровой экономики". Внесённые предложения, в том числе и по интеграции системы допуска в государственные информационные системы, как представляется, позволят на практике нивелировать возникшие проблемы.

Анализ системы допуска и доступа субъектов к коммерческой и служебной тайне позволил сделать вывод о необходимости повышения роли служебной тайны в обороте информации в условиях "цифровой экономики", о необходимости издания соответствующего федерального закона и необходимости отнесения информации ограниченного доступа, обрабатываемой в государственных информационных системах, в т.ч. относящихся к коммерческой тайне, к служебной тайне в области обороны, к персональным данным, к единому институту служебной тайны.

Изучение практики применения законодательства в области допуска и доступа субъектов к персональным данным позволило сделать вывод о необходимости отнесения персональных данных всех граждан Российской Федерации, которые централизованно обрабатываются в государственных информационных системах, к институту государственной тайны, в особенности это касается биометрических и геномных персональных данных.

Материалы проведённого исследования показывают, что существующая система допуска и доступа субъектов к информации, разработанная ещё в советское время, в настоящее время уже не отвечает новым требованиям, которые определяются условиями формирования в России "цифровой экономики", а также в условиях глобального мирового противостояния. Нужны существенные изменения на концептуальном уровне понимания "допуск" и "доступ" субъектов к информации, что обусловливает необходимость дальнейшего развития данного направления.

Также видится целесообразным в отдельном изучении рассмотренного вопроса при подготовке студентов-юристов в рамках учебной дисциплины "Информационное право".

Как показывает судебная практика[441], неправильное правоприменение в области допуска и доступа к информации влечёт за собой ущемление прав и свобод граждан, создаёт предпосылки к возникновению "коррупционной составляющей", что, в свою очередь, подрывает авторитет органов государственной власти.

[441] См. Определения Конституционного Суда РФ от 23.06.2015 № 1538-О, от 29.09.2016 № 1863-О, от 28.11.2019 № 3012-О; Определения Верховного Суда РФ от 12.10.2000 № 4-Г00-18, от 13.01.2004 № 66-г03-19, от 12.04.2011 № 206-Г11-2, от 23.03.2020 № 4-КГ20-8 // URL: http://www.consultant.ru.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ И НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Нормативные правовые акты Российской Федерации (действующие)

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // "Собрание законодательства РФ", 04.08.2014, № 31, ст. 4398.

2. Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1 "О Декларации прав и свобод человека и гражданина" // "Ведомости СНД РСФСР и ВС РСФСР", 1991, № 52, ст. 1865.

3. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ // "Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

4. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ // "Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954.

5. "Налоговый кодекс Российской Федерации" (часть первая) от 31.07.1998 № 146-ФЗ // "Собрание законодательства РФ", 03.08.1998, № 31, ст. 3824.

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

7. "Трудовой кодекс Российской Федерации" от 30.12.2001 № 197-ФЗ // "Собрание законодательства РФ", 07.01.2002, № 1 (ч. 1), ст. 3.

8. "Арбитражный процессуальный кодекс Российской Федерации" от 24.07.2002 № 95-ФЗ // "Собрание законодательства РФ", 29.07.2002, № 30, ст. 3012.

9. "Гражданский процессуальный кодекс Российской Федерации" от 14.11.2002 № 138-ФЗ // "Собрание законодательства РФ", 18.11.2002, № 46, ст. 4532.

10. "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 № 230-ФЗ // "Собрание законодательства РФ", 25.12.2006, № 52 (ч. 1), ст. 5496.

11. Закон Российской Федерации от 27.12.1991 № 2124-1 "О средствах массовой информации" // "Ведомости СНД и ВС РФ", 13.02.1992, № 7, ст. 300.

12. Закон Российской Федерации от 11.03.1992 № 2487-1 "О частной детективной и охранной деятельности в Российской Федерации" // "Ведомости СНД РФ и ВС РФ", 23.04.1992, № 17, ст. 888.

13. Закон Российской Федерации от 21.07.1993 № 5485-1 "О государственной тайне" // "Собрание законодательства РФ", 13.10.1997, № 41, ст. 8220-8235.

14. Федеральный закон от 29.12.1994 № 77-ФЗ "Об обязательном экземпляре документов" // "Собрание законодательства РФ", 02.01.1995, № 1, ст. 1.

15. Федеральный закон от 12.08.1995 № 144-ФЗ "Об оперативно-розыскной деятельности" // "Собрание законодательства РФ", 14.08.1995, № 33, ст. 3349.

16. Федеральный закон от 01.04.1996 № 27-ФЗ "Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования" // "Собрание законодательства РФ", 01.04.1996, № 14, ст. 1401.

17. Федеральный закон от 31.05.1996 № 61-ФЗ "Об обороне" // "Собрание законодательства РФ", 03.06.1996, № 23, ст. 2750.

18. Федеральный закон от 26.02.1997 № 31-ФЗ "О мобилизационной подготовке и мобилизации в Российской Федерации" // "Собрание законодательства РФ", 03.03.1997, № 9, ст. 1014.

19. Федеральный закон от 28.03.1998 № 53-ФЗ "О воинской обязанности и военной службе" // "Собрание законодательства РФ", 30.03.1998, № 13, ст. 1475.

20. Федеральный закон от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" // "Собрание законодательства РФ", 13.08.2001, № 33 (ч. I), ст. 3418.

21. Федеральный закон от 31.05.2002 № 62-ФЗ "О гражданстве Российской Федерации" // "Собрание законодательства РФ", 03.06.2002, № 22, ст. 2031.

22. Федеральный закон от 31.05.2002 № 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" // "Собрание законодательства РФ", 10.06.2002, № 23, ст. 2102.

23. Федеральный закон от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности" // "Собрание законодательства РФ", 29.07.2002, № 30, ст. 3031.

24. Федеральный закон от 07.07.2003 № 126-ФЗ "О связи" // "Собрание законодательства РФ", 14.07.2003, № 28, ст. 2895.

25. Федеральный закон от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" // "Собрание законодательства РФ", 02.08.2004, № 31, ст. 3215.

26. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне" // "Собрание законодательства РФ", 09.08.2004, № 32, ст. 3283.

27. Федеральный закон от 22.10.2004 № 125-ФЗ "Об архивном деле в Российской Федерации" // "Собрание законодательства РФ", 25.10.2004, № 43, ст. 4169.

28. Федеральный закон от 26.07.2006 № 135-ФЗ "О защите конкуренции" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3434.

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

30. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (ч. 1), ст. 3451.

31. Федерального закона от 29.11.2007 № 282-ФЗ "Об официальном статистическом учёте и системе государственной статистики в Российской Федерации" // "Собрание законодательства РФ", 03.12.2007, № 49, ст. 6043.

32. Федеральный закон от 03.12.2008 № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" // "Собрание законодательства РФ", 08.12.2008, № 49, ст. 5740.

33. Федеральный закон от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" // "Собрание законодательства РФ", 02.08.2010, № 31, ст. 4179.

34. Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" // "Собрание законодательства РФ", 03.01.2011, № 1, ст. 48.

35. Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи" // "Собрание законодательства РФ", 11.04.2011, № 15, ст. 2036.

36. Федеральный закон от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" // "Собрание законодательства РФ", 28.11.2011, № 48, ст. 6724.

37. Федеральный закон от 05.04.2013 № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" // "Собрание законодательства РФ", 08.04.2013, № 14, ст. 1652.

38. Федеральный конституционный закон от 21.03.2014 № 6-ФКЗ "О принятии в Российскую Федерацию Республики Крым и образовании в составе Российской Федерации новых субъектов - Республики Крым и города федерального значения Севастополя" // "Собрание законодательства РФ", 24.03.2014, № 12, ст. 1201.

39. Федеральный закон от 03.07.2016 № 238-ФЗ "О независимой оценке квалификации" // "Собрание законодательства РФ", 04.07.2016, № 27 (ч. I), ст. 4171.

40. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // "Собрание законодательства РФ", 31.07.2017, № 31 (ч. I), ст. 4736.

41. Федеральный закон от 02.08.2019 № 259-ФЗ "О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 05.08.2019, № 31, ст. 4418.

42. Федеральный закон от 24.04.2020 № 122-ФЗ "О проведении эксперимента по использованию электронных документов, связанных с работой" // "Собрание законодательства РФ", 27.04.2020, № 17, ст. 2700.

43. Федеральный закон от 31.07.2020 № 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации" // "Собрание законодательства РФ", 03.08.2020, № 31 (ч. I), ст. 5007.

44. Федеральный закон от 29.12.2020 № 479-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", "Собрание законодательства РФ", 04.01.2021, № 1 (ч. 1), ст. 18.

45. Федеральный закон от 01.07.2021 № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. I), ст. 5064.

46. Федеральный закон от 08.03.2022 № 46-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 14.03.2022, № 11, ст. 1596.

47. Федеральный закон от 14.07.2022 № 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием" // "Собрание законодательства РФ", 18.07.2022, № 29 (ч. II), ст. 5222.

48. Федеральный конституционный закон от 04.10.2022 № 5-ФКЗ "О принятии в Российскую Федерацию Донецкой Народной Республики и образовании в составе Российской Федерации нового субъекта - Донецкой Народной Республики" // "Собрание законодательства РФ", 10.10.2022, № 41, ст. 6930.

49. Федеральный конституционный закон от 04.10.2022 № 6-ФКЗ "О принятии в Российскую Федерацию Луганской Народной Республики и образовании в составе Российской Федерации нового субъекта - Луганской Народной Республики" // "Собрание законодательства РФ", 10.10.2022, № 41, ст. 6931.

50. Федеральный конституционный закон от 04.10.2022 № 7-ФКЗ "О принятии в Российскую Федерацию Запорожской области и образовании в составе Российской Федерации нового субъекта - Запорожской области" // "Собрание законодательства РФ", 10.10.2022, № 41, ст. 6932.

51. Федеральный конституционный закон от 04.10.2022 № 8-ФКЗ "О принятии в Российскую Федерацию Херсонской области и образовании в составе Российской Федерации нового субъекта - Херсонской области" // "Собрание законодательства РФ", 10.10.2022, № 41, ст. 6933.

52. 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 утратившими силу отдельных положений законодательных актов Российской Федерации" // "Собрание законодательства РФ", 02.01.2023, № 1 (ч. I), ст. 19.

53. Федеральный закон от 18.03.2023 № 62-ФЗ "Об особенностях правового положения граждан Российской Федерации, имеющих гражданство Украины" // "Собрание законодательства РФ", 20.03.2023, № 12, ст. 1875.

54. Указ Президента РФ от 28.06.1993 № 966 "О Концепции правовой информатизации России" // "Собрание актов Президента и Правительства РФ", 05.07.1993, № 27, ст. 2521.

55. Указ Президента РФ от 31.12.1993 № 2334 "О дополнительных гарантиях прав граждан на информацию" // "Собрание актов Президента и Правительства РФ", 10.01.1994, № 2, ст. 74.

56. Указ Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера" // "Собрание законодательства РФ", 10.03.1997, № 10, ст. 1127.

57. Указ Президента РФ от 13.03.1997 № 232 "Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации" // "Собрание законодательства РФ", 17.03.1997, № 11, ст. 1301.

58. Указ Президента РФ от 07.05.2012 № 601 "Об основных направлениях совершенствования системы государственного управления" // "Собрание законодательства РФ", 07.05.2012, № 19, ст. 2338.

59. Указ Президента РФ от 29.12.2012 № 1709 "О паспорте гражданина Российской Федерации, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем на электронном носителе

информации дополнительные биометрические персональные данные его владельца" // "Собрание законодательства РФ", 31.12.2012, № 53 (ч. 2), ст. 7861.

60. Указ Президента РФ от 08.07.2013 № 613 "Вопросы противодействия коррупции" (вместе с "Порядком размещения сведений о доходах, расходах, об имуществе и обязательствах имущественного характера отдельных категорий лиц и членов их семей на официальных сайтах федеральных государственных органов, органов государственной власти субъектов Российской Федерации и организаций и предоставления этих сведений общероссийским средствам массовой информации для опубликования") // "Собрание законодательства РФ", 15.07.2013, № 28, ст. 3813.

61. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.

62. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы" // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901.

63. Указ Президента РФ от 07.05.2018 № 204 "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" // "Собрание законодательства РФ", 14.05.2018, № 20, ст. 2817.

64. Указ Президента РФ от 28.11.2018 № 680 "О развитии генетических технологий в Российской Федерации" (вместе с "Положением о совете по реализации Федеральной научно-технической программы развития генетических технологий на 2019 - 2027 годы") // "Собрание законодательства РФ", 03.12.2018, № 49 (ч. VI), ст. 7586.

65. Указ Президента РФ от 11.03.2019 № 97 "Об Основах государственной политики Российской Федерации в области обеспечения химической и биологической безопасности на период до 2025 года и дальнейшую перспективу" // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1106.

66. Указ Президента РФ от 24.04.2019 № 183 "Об определении в гуманитарных целях категорий лиц, имеющих право обратиться с заявлениями о приёме в гражданство Российской Федерации в упрощённом порядке" // "Собрание законодательства РФ", 29.04.2019, № 17, ст. 2071.

67. Указ Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // "Собрание законодательства РФ", 14.10.2019, № 41, ст. 5700.

68. Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. II), ст. 5351.

69. Распоряжение Президента РФ от 16.04.2005 № 151-рп "О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне" // "Собрание законодательства РФ", 25.04.2005, № 17, ст. 1547.

70. Постановление Правительства РФ от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности" // "Собрание законодательства РФ", 25.07.2005, № 30 (ч. II), ст. 3165.

71. Постановление Правительства РФ от 15.04.1995 № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" // "Собрание законодательства РФ", 24.04.1995, № 17, ст. 1540.

72. Постановление Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации" // "Собрание законодательства РФ", 03.07.1995, № 27, ст. 257.

73. Постановление Правительства РФ от 08.07.1997 № 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" // "Собрание законодательства РФ", 14.07.1997, № 28, ст. 3444.

74. Постановление Правительства РФ от 02.08.1997 № 973 "Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или Международным организациям" // "Собрание законодательства РФ", 11.08.1997, № 32, ст. 3786.

75. Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // "Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407.

76. Постановление Правительства РФ от 05.01.2004 № 3-1 "Об утверждении Инструкции по обеспечению режима секретности в Российской Федерации" // М.: Издание, 2011.

77. Постановление Правительства РФ от 24.12.2007 № 928 "О порядке проведения проверки наличия в заявках на выдачу патента на изобретение, полезную модель или промышленный образец, созданные в Российской Федерации, сведений, составляющих государственную тайну" // "Собрание законодательства РФ", 31.12.2007, № 53, ст. 6624.

78. 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") // "Собрание законодательства РФ", 23.03.2009, № 12, ст. 1431.

79. Постановление Правительства РФ от 22.09.2009 № 754 "Об утверждении Положения о системе межведомственного электронного документооборота" // "Собрание законодательства РФ", 28.09.2009, № 39, ст. 4614.

80. Постановление Правительства РФ от 25.12.2009 № 1088 "О государственной автоматизированной информационной системе "Управление" (вместе с "Положением о государственной автоматизированной информационной системе "Управление") // "Собрание законодательства РФ", 04.01.2010, № 1, ст. 101.

81. Постановление Правительства РФ от 06.02.2010 № 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" // "Собрание законодательства РФ", 15.02.2010, № 7, ст. 762.

82. Постановление Правительства РФ от 04.03.2010 № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию" // "Собрание законодательства РФ", 08.03.2010, № 10, ст. 1103.

83. 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.

84. Постановление Правительства РФ от 11.10.2011 № 828 "Об утверждении Положения о порядке проведения обязательной государственной геномной регистрации лиц, осуждённых и отбывающих наказание в виде лишения свободы" // "Собрание законодательства РФ", 17.10.2011, № 42, ст. 5926.

85. Постановление Правительства РФ от 24.10.2011 № 861 "О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)" // "Собрание законодательства РФ", 31.10.2011, № 44, ст. 6274.

86. 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" // "Собрание законодательства РФ", 05.12.2011, № 49 (ч. 5), ст. 7284.

87. Постановление Правительства РФ от 21.03.2012 № 218 "О Федеральной службе по интеллектуальной собственности" // "Собрание законодательства РФ", 02.04.2012, № 14, ст. 1627.

88. Постановление Правительства РФ от 26.10.2012 № 1101 "О единой автоматизированной информационной системе Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено" // "Собрание законодательства РФ", 29.10.2012, № 44, ст. 6044.

89. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // "Собрание законодательства РФ", 05.11.2012, № 45, ст. 6257.

90. Постановление Правительства РФ от 10.07.2013 № 583 "Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети Интернет в форме открытых данных" // "Собрание законодательства РФ", 29.07.2013, № 30 (ч. II), ст. 4107.

91. Постановление Правительства РФ от 15.04.2014 № 313 "Об утверждении государственной программы Российской Федерации "Информационное общество" // "Собрание законодательства РФ", 05.05.2014, № 18 (ч. II), ст. 2159.

92. Постановление Правительства РФ от 16.11.2015 № 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд" (вместе с "Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации", "Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включённого в единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации), для целей осуществления закупок для обеспечения государственных и муниципальных нужд") // "Собрание законодательства РФ", 23.11.2015, № 47, ст. 6600.

93. Постановление Правительства РФ от 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" // "Собрание законодательства РФ", 09.07.2018, № 28, ст. 4234.

94. Постановление Правительства РФ от 02.03.2019 № 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации") // "Собрание законодательства РФ", 18.03.2019, № 11, ст. 1119.

95. Постановление Правительства РФ от 26.04.2019 № 515 "О системе маркировки товаров средствами идентификации и прослеживаемости движения товаров" (вместе с "Правилами маркировки товаров, подлежащих обязательной маркировке средствами идентификации", "Положением о государственной информационной системе

мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации") // "Собрание законодательства РФ", 13.05.2019, № 19, ст. 2279.

96. Постановление Правительства РФ от 30.07.2019 № 984 "Об утверждении Правил информационного взаимодействия единой автоматизированной системы страхования жилых помещений с информационными ресурсами федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и Центрального банка Российской Федерации" // "Собрание законодательства РФ", 05.08.2019, № 31, ст. 4649.

97. Постановление Правительства РФ от 26.09.2019 № 1251 "О проведении эксперимента по маркировке средствами идентификации и мониторингу оборота отдельных видов табачной продукции, подлежащих обязательной маркировке с 1 июля 2020 г." (вместе с "Положением о проведении эксперимента по маркировке средствами идентификации и мониторингу оборота отдельных видов табачной продукции, подлежащих обязательной маркировке с 1 июля 2020 г.") // "Собрание законодательства РФ", 07.10.2019, № 40, ст. 5553.

98. Постановление Правительства РФ от 23.09.2020 № 1526 "О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети "Интернет" информации о фактах приёма, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети "Интернет" и информации об этих пользователях и предоставления её уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации" // "Собрание законодательства РФ", 05.10.2020, № 40, ст. 6258.

99. Постановление Правительства РФ от 22.06.2021 № 956 "О государственной информационной системе "Цифровая аналитическая платформа предоставления статистических данных" (вместе с "Положением о государственной информационной системе "Цифровая аналитическая платформа предоставления статистических данных") // "Собрание законодательства РФ", 28.06.2021, № 26, ст. 4979.

100. Постановление Правительства РФ от 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных" (вместе с "Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных") // "Собрание законодательства РФ", 05.07.2021, № 27 (ч. III), ст. 5424.

101. Постановление Правительства РФ от 07.10.2021 № 1705 "О едином реестре результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального или двойного назначения и признании утратившими силу некоторых актов Правительства Российской Федерации и отдельного положения акта Правительства Российской Федерации" (вместе с "Правилами формирования и ведения единого реестра результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального или двойного назначения") // "Собрание законодательства РФ", 18.10.2021, № 42, ст. 7118.

102. Постановление Правительства РФ от 15.10.2021 № 1753 "Об утверждении требований к организационным и техническим условиям осуществления многофункциональными центрами предоставления государственных и муниципальных услуг размещения или обновления в единой системе идентификации и аутентификации сведений, необходимых для регистрации физических лиц в данной системе, размещения биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, с использованием программно-технических комплексов" // "Собрание законодательства РФ", 25.10.2021, № 43, ст. 7251.

103. Постановление Правительства РФ от 20.10.2021 № 1801 "Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети "Интернет" организатором сервиса обмена мгновенными сообщениями" // "Собрание законодательства РФ", 25.10.2021, № 43, ст. 7291.

104. Постановление Правительства РФ от 26.11.2021 № 2052 "Об утверждении Правил обращения со сведениями, составляющими служебную тайну в области обороны" // "Собрание законодательства РФ", 06.12.2021, № 49 (ч. I), ст. 8241.

105. Постановление Правительства РФ от 27.01.2022 № 60 "О мерах по информационному обеспечению контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, по организации в ней документооборота, о внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившими силу актов и отдельных положений актов Правительства Российской Федерации" // "Собрание законодательства РФ", 07.02.2022, № 6, ст. 872.

106. Постановление Правительства РФ от 05.02.2022 № 116 "Об утверждении Правил ведения Федерального реестра медицинских документов о рождении" // "Собрание законодательства РФ", 14.02.2022, № 7, ст. 974.

107. Постановление Правительства РФ от 09.02.2022 № 140 "О единой государственной информационной системе в сфере здравоохранения" (вместе с "Положением о единой государственной информационной системе в сфере здравоохранения") // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1152.

108. Постановление Правительства РФ от 15.02.2022 № 172 "О государственной информационной системе "Типовое облачное решение системы электронного документооборота" (вместе с "Положением о государственной информационной системе "Типовое облачное решение системы электронного документооборота") // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1178.

109. Постановление Правительства РФ от 02.03.2022 № 279 "О государственной информационной системе "Платформа "Центр хранения электронных документов" // "Собрание законодательства РФ", 07.03.2022, № 10, ст. 1532.

110. Постановление Правительства РФ от 12.03.2022 № 351 "Об особенностях раскрытия и предоставления информации, подлежащей раскрытию и предоставлению в соответствии с требованиями Федерального закона "Об акционерных обществах" и Федерального закона "О рынке ценных бумаг", и особенностях раскрытия инсайдерской информации в соответствии с требованиями Федерального закона "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" // "Собрание законодательства РФ", 21.03.2022, № 12, ст. 1837.

111. Постановление Правительства РФ от 18.03.2022 № 395 "Об особенностях доступа к информации, содержащейся в государственном информационном ресурсе бухгалтерской (финансовой) отчётности, и раскрытия консолидированной финансовой отчётности в 2022 году" // "Собрание законодательства РФ", 21.03.2022, № 12, ст. 1877.

112. Постановление Правительства РФ от 19.03.2022 № 414 "О некоторых вопросах применения требований и целевых значений показателей, связанных с публикационной активностью" // "Собрание законодательства РФ", 28.03.2022, № 13, ст. 2076.

113. Постановление Правительства РФ от 28.03.2022 № 493 "Об утверждении Правил взаимодействия Федеральной государственной информационной системы прослеживаемости пестицидов и агрохимикатов и иных государственных информационных систем" // "Собрание законодательства РФ", 04.04.2022, № 14, ст. 2274.

114. Постановление Правительства РФ от 13.05.2022 № 867 "О единой цифровой платформе в сфере занятости и трудовых отношений "Работа в России" (вместе с "Правилами функционирования единой цифровой платформы в сфере занятости и трудовых отношений "Работа в России") // "Собрание законодательства РФ", 23.05.2022, № 21, ст. 3446.

115. Постановление Правительства РФ от 16.06.2022 № 1089 "Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица"// "Собрание законодательства РФ", 27.06.2022, № 26, ст. 4475.

116. Постановление Правительства РФ от 22.07.2022 № 1313 "Об утверждении Правил представления операторами подвижной радиотелефонной связи информации, необходимой для осуществления мониторинга соблюдения операторами связи обязанности по проверке достоверности сведений об абонентах и сведений о пользователях услугами связи абонентов - юридических лиц либо индивидуальных предпринимателей" // "Собрание законодательства РФ", 01.08.2022, № 31, ст. 5707.

117. Постановление Правительства РФ от 29.12.2022 № 2526 "Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3-6, 8-11 статьи 12 Федерального закона "О персональных данных" // "Собрание законодательства РФ", 02.01.2023, № 1 (ч. II), ст. 326.

118. Постановление Правительства РФ от 31.12.2022 № 2560 "Об утверждении Правил размещения государственными органами, органами местного самоуправления и подведомственными организациями информации на своих официальных страницах, получения доступа к информации, размещаемой на официальных страницах, и осуществления взаимодействия с пользователями информацией на официальных страницах с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, предусмотренной Федеральным законом "Об организации предоставления государственных и муниципальных услуг", и Правил взаимодействия официальных сайтов и официальных страниц с федеральной

государственной информационной системой "Единый портал государственных и муниципальных услуг (функций)", включая требования, предъявляемые к такому взаимодействию" // "Собрание законодательства РФ", 09.01.2023, № 2, ст. 518.

119. Постановление Правительства РФ от 10.01.2023 № 6 "Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении" // URL: http://pravo.gov.ru.

120. Постановление Правительства РФ от 16.01.2023 № 24 "Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан" // URL: http://pravo.gov.ru.

121. Распоряжение Правительства РФ от 05.09.2002 № 1227-р "О создании федерального государственного унитарного предприятия Почта России" // "Собрание законодательства РФ", 09.09.2002, № 36, ст. 3511.

122. Распоряжение Правительства РФ от 10.07.2013 № 1187-р "О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети Интернет в форме открытых данных" // "Собрание законодательства РФ", 29.07.2013, № 30 (ч. II), ст. 4128.

123. Распоряжение Правительства РФ от 30.01.2014 № 93-р "Об утверждении "Концепции открытости федеральных органов исполнительной власти" // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 547.

124. Распоряжение Правительства РФ от 28.04.2018 № 792-р "Об утверждении перечня отдельных товаров, подлежащих обязательной маркировке средствами идентификации" // "Собрание законодательства РФ", 07.05.2018, № 19, ст. 2773.

(недействующие)

125. Указ Петра I от 16.01.1724 "О поручении секретных дел в Сенате благонадёжным людям" // Полное собрание законов Российской империи. Т. 7 (1723–1727). Печат. в Типографии 2-го отд. Собственной Его Императорского Величества Канцелярии. 1830. Ст. 4409.

126. Постановление Секретариата ЦК РКП(б) от 30.08.1922 "О порядке хранения и движения секретных документов" // М.: Издание, 1925.

127. Постановление Секретариата ЦК КПСС и Совета Министров СССР от 04.12.1976 "Об обеспечении безопасности в автоматизированных системах управления войсками и вычислительной техники общего применения от утечки информации за счёт побочных электромагнитных излучений и наводок и несанкционированного доступа", М.: Издание, 1977.

128. Закон Российской Федерации от 28.11.1991 № 1948-1 "О гражданстве Российской Федерации" // "Ведомости СНД и ВС РФ", 06.02.1992, № 6, ст. 243 (не применяется).

129. Федеральный закон от 20.02.1995 № 24-ФЗ "Об информации, информатизации и защите информации" // "Собрание законодательства РФ", 20.02.1995, № 8, ст. 609.

130. Паспорт проекта Федерального закона № 124871-4 (по состоянию на 01.05.1995 года) "О служебной тайне" // URL: http://sozd.duma.gov.ru.

131. Проект Федерального закона (по состоянию на 15.05.2001) "О праве на информацию в Российской Федерации" // URL: http://docs.cntd.ru/document/ 901799770.

132. Приказ ФНС России от 31.12.2009 № ММ-7-6/728@ "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в налоговых органах" // URL: http://www.pravo.gov.ru.

133. Проект Федерального закона № 744029-7 "О внесении изменений в статью 11 Федерального закона "О персональных данных" в части обработки биометрических персональных данных" // URL: http://www.consultant.ru.

Нормативные акты федеральных органов исполнительной власти

134. Руководящий документ ФСТЭК России. "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" (утверждены решением Гостехкомиссии России от 30.03.1992) // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty.

135. Руководящий документ ФСТЭК России. "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (утверждены решением Гостехкомиссии России от 30.03.1992) // URL: https://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty.

136. Руководящий документ ФСТЭК России. "Защита от несанкционированного доступа к информации. Термины и определения" (утв. решением Гостехкомиссии РФ от 30.03.1992) // URL: https://fstec.ru/component/ attachments/download/298.

137. Приказ Минсвязи РФ от 29.06.1995 № 79 "О сертификации оборудования сотовой связи с учётом временных технических решений" // URL: http://www.consultant.ru.

138. Приказ Минздрава РФ от 23.08.1999 № 327 "Об анонимном лечении в наркологических учреждениях (подразделениях)" // URL: http://pravo.gov.ru.

139. Приказ ФСБ России от 13.11.1999 № 564 "Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о её знаках соответствия" // "Бюллетень нормативных актов федеральных органов исполнительной власти", № 3, 17.01.2000.

140. Приказ МНС России от 03.03.2003 № БГ-3-28/96 "Об утверждении Порядка доступа к конфиденциальной информации налоговых органов" // URL: http://www.pravo.gov.ru.

141. Руководящий документ Роскартографии России. "ГКИНП (ОНТА)-14-270-03. Геодезические, картографические инструкции, нормы и правила. Правила контроля отображения границ на картах, предназначенных для открытого опубликования и с пометкой "Для служебного пользования" (утверждены Приказом Роскартографии России от 17.07.2003 № 114-пр) // М.: ФГУП "Центральный картографо-геодезический фонд", 2003.

142. Письмо Минкомсвязи России от 13.05.2009 № ДС-П11-2502 "Об осуществлении трансграничной передачи персональных данных" // URL: http://www.consultant.ru.

143. "Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе" (утв. ФССП РФ 30.11.2010 № 02-7) // "Бюллетень Федеральной службы судебных приставов", № 1, 2011.

144. Приказ Минздравсоцразвития РФ от 26.08.2011 № 989н "Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну" // "Российская газета", № 234, 19.10.2011.

145. Решение Координационного центра национального домена сети "Интернет" от 05.10.2011 № 2011-18/81 "Правила регистрации доменных имён в доменах .RU и .РФ" (ред. от 06.09.2018 № 2018-06/26) // URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf.

146. "Рекомендации по применению Федерального закона от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

в отношении печатной (книжной) продукции" (утверждено Минкомсвязи России от 22.01.2013 № АВ-П17-531) // URL: http://www.consultant.ru.

147. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" // "Российская газета", № 107, 22.05.2013.

148. "Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных. Версия 3.0" (утверждены протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 № 4) // URL: http://data.gov.ru.

149. Приказ Минфина России от 17.06.2014 № 162 "Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации и организаций, находящихся в его ведении" // URL: http://www.pravo.gov.ru.

150. Приказ ФСБ России от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости" // "Российская газета", № 211, 17.09.2014.

151. Приказ Ространснадзора России от 05.02.2016 № СС-94фс "Об утверждении Перечня сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Федеральной службы по надзору в сфере транспорта и её территориальных органов" // URL: http://www.pravo.gov.ru.

152. Приказ ОАО "РЖД" от 20.07.2016 № 60 "Об обеспечении защиты персональных данных в ОАО "РЖД" (вместе с "Положением об обработке и защите персональных данных работников ОАО "РЖД", "Порядком обработки и обеспечения режима защиты персональных данных работников ОАО "РЖД") // URL: http://www.consultant.ru.

153. Приказ Роскомнадзора России от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале

обработки персональных данных и о внесении изменений в ранее представленные сведения" // URL: http://www.pravo.gov.ru.

154. Приказ Минпромторга России от 20.06.2017 № 1907 "Об утверждении Рекомендаций по применению принципов бережливого производства в различных отраслях промышленности" // URL: http://www.consultant.ru.

155. Письмо Минтруда РФ от 18.08.2017 № 14-2/В-761 // "Нормативные акты для бухгалтера", 2017, № 20.

156. Приказ ФСТЭК России от 06.12.2017 № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации" // URL: http://www.pravo.gov.ru.

157. Приказ Роскомнадзора России от 14.12.2017 № 249 "Об утверждении требований к способам (методам) ограничения доступа к информационным ресурсам, а также требований к размещаемой информации об ограничении доступа к информационным ресурсам" // URL: http://www.pravo.gov.ru.

158. Приказ ФСТЭК России от 03.04.2018 № 55 "Об утверждении Положения о системе сертификации средств защиты информации" // URL: http://www.pravo.gov.ru.

159. Постановление Администрации Тамбовской области от 26.06.2018 № 626 "Об утверждении правил оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации области" // URL: http://docs.cntd.ru/document/550130088.

160. Приказ Минобрнауки России от 22.10.2018 № 51н "Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и его территориальных органах" (вместе с "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения") // URL: http://www.pravo.gov.ru.

161. Приказ МВД России от 09.11.2018 № 755 "О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России" (вместе с "Инструкцией по организации деятельности по обращению со служебной информацией ограниченного распространения в системе МВД России") // URL: http://www.pravo.gov.ru.

162. Приказ Роскомнадзора России от 11.02.2019 № 21 "Об утверждении Порядка идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам" // URL: http://www.pravo.gov.ru.

163. Приказ Минфина России от 19.06.2019 № 98н "Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве финансов Российской Федерации и подведомственных ему организациях и о признании утратившим силу приказа Министерства финансов Российской Федерации от 26 марта 2018 г. № 53н" (вместе с "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения") // URL: http://www.pravo.gov.ru.

164. Положение Банка России от 18.08.2019 № 690-П "О порядке передачи банками в таможенные органы, а также таможенными органами в банки электронных документов, подписанных усиленной квалифицированной электронной подписью, и информации в электронном виде, предусмотренных статьёй 61 Федерального закона от 3 августа 2018 года № 289-ФЗ "О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации" (вместе с "Графиком обмена архивными файлами и сообщениями") // "Вестник Банка России", № 66, 03.10.2019.

165. "Концепция развития электронного документооборота в хозяйственной деятельности", утверждена решением президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 25.12.2020 № 34) // URL: https://www.new.nalog.ru/docs/edo/edo_concept.pdf.

166. Приказ Минтруда России № 988н, Минздрава России № 1420н от 31.12.2020 "Об утверждении перечня вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные медицинские осмотры при поступлении на работу и периодические медицинские осмотры" // URL: http://www.pravo.gov.ru.

167. Приказ Минздрава России от 28.01.2021 № 29н "Об утверждении Порядка проведения обязательных предварительных и периодических медицинских осмотров работников, предусмотренных частью четвертой статьи 213 Трудового кодекса Российской Федерации, перечня медицинских противопоказаний к осуществлению работ с вредными и (или) опасными производственными факторами, а также работам, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры" // URL: http://www.pravo.gov.ru.

168. Приказ ФНС России от 21.04.2021 № ЕД-7-24/391@ "О работе с несекретной информацией, доступ к которой ограничен федеральным законодательством, а также служебной информацией, ограничение на распространение которой диктуется служебной необходимостью" (вместе с "Порядком организации защиты служебной информации ограниченного распространения в налоговых органах", "Порядком передачи служебной информации ограниченного распространения другим органам и организациям", "Порядком снятия пометки "Для служебного пользования" с носителей служебной информации ограниченного распространения") // URL: http://www.pravo.gov.ru.

169. Приказ Минздрава России от 27.04.2021 № 404н "Об утверждении Порядка проведения профилактического медицинского осмотра и диспансеризации определённых групп взрослого населения" // URL: http://pravo.gov.ru.

170. Приказ Минцифры России от 25.05.2021 № 494 "Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учётом оценки возможного вреда, проведённой в соответствии с законодательством Российской Федерации о персональных данных" // URL: http://pravo.gov.ru.

171. Приказ Минцифры России от 27.08.2021 № 896 "Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающей услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц" // URL: http://pravo.gov.ru.

172. Приказ Минцифры России от 10.09.2021 № 930 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных

данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации" // URL: http://www.pravo.gov.ru.

173. Приказ Минсельхоза России от 01.10.2021 № 687 "Об утверждении порядка и формата представления в форме электронного документа деклараций об объёме винограда, использованного для производства винодельческой продукции, в том числе российской винодельческой продукции защищённых наименований, и полного цикла производства дистиллятов, формы и порядка заполнения таких деклараций" // URL: http://www.pravo.gov.ru.

174. Приказ Росгвардии России от 27.12.2021 № 480 "Об утверждении Перечня сведений Федеральной службы войск национальной гвардии Российской Федерации, подлежащих отнесению к служебной тайне в области обороны" // URL: http://pravo.gov.ru.

175. Приказ МЧС России от 29.12.2021 № 940 "Об утверждении Перечня сведений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, подлежащих отнесению к служебной тайне в области обороны" // URL: http://pravo.gov.ru.

176. Приказ Министра обороны России от 17.01.2022 № 22 "Об утверждении Перечня сведений Вооружённых Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны" // URL: http://pravo.gov.ru.

177. Решение Совета директоров Банка России от 14.04.2022 "О перечне информации кредитных организаций (головных кредитных организаций банковских групп), которую они временно не должны раскрывать" // URL: http://www.cbr.ru.

178. Приказ Минздрава России от 20.05.2022 № 342н "Об утверждении порядка прохождения обязательного психиатрического освидетельствования работниками, осуществляющими отдельные виды деятельности, его периодичности, а также видов деятельности, при осуществлении которых проводится психиатрическое освидетельствование" // URL: http://pravo.gov.ru.

179. Приказ Роскомнадзора России от 05.08.2022 № 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" // URL: http://pravo.gov.ru.

180. Письмо Минздрава России от 12.08.2022 № 30-7/3105 "Об обязательном психиатрическом освидетельствовании отдельных категорий работников" // URL: http://pravo.gov.ru.

181. Приказ ФСБ России от 04.11.2022 № 547 "Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации,

которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации" // URL: http://pravo.gov.ru.

182. Приказ Минюста России от 29.11.2022 № 307 "Об утверждении Порядка ведения реестра иностранных агентов и размещения содержащихся в нем сведений на официальном сайте Министерства юстиции Российской Федерации в информационно-телекоммуникационной сети "Интернет", Порядка принятия решения об исключении физического лица, впервые включённого в реестр иностранных агентов, из реестра иностранных агентов, формы заявления иностранного агента об исключении из реестра иностранных агентов" // URL: http://pravo.gov.ru.

183. Приказ ФНС России от 30.11.2022 № ЕД-7-8/1133@ "Об утверждении форм и форматов представления документов, используемых налоговыми органами и налогоплательщиками, плательщиками сборов, плательщиками страховых взносов и (или) налоговыми агентами при осуществлении зачёта и возврата сумм денежных средств, формирующих положительное сальдо единого налогового счета, а также излишне уплаченной (взысканной) государственной пошлины" // URL: http://www.pravo.gov.ru.

184. Решение Совета директоров Банка России от 23.12.2022 "Об определении перечня информации кредитных организаций, некредитных финансовых организаций, а также организаций, оказывающих профессиональные услуги на финансовом рынке, подлежащей раскрытию в соответствии с законодательством Российской Федерации или нормативными актами Банка России, которую кредитные организации, некредитные финансовые организации, а также организации, оказывающие профессиональные услуги на финансовом рынке, вправе не раскрывать с 1 января 2023 года до 1 июля 2023 года, и перечня информации, предусмотренной законодательством Российской Федерации или нормативными актами Банка России, которую Банк России вправе не раскрывать на своём официальном сайте в информационно-телекоммуникационной сети "Интернет" с 1 января 2023 года до 1 июля 2023 года" // URL: http://www.cbr.ru.

Международные и национальные стандарты

185. Межгосударственный стандарт. "ГОСТ 28270-89 (ИСО 8211-85). Системы обработки информации. Спецификация файла описания данных для обмена информацией" (утверждён Постановлением Госстандарта СССР от 27.09.1989 № 2942) // М.: Стандартинформ, 2006.

186. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 9594-8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8.

Основы аутентификации" (утверждён Постановлением Госстандарта РФ от 19.05.1998 № 215) // М.: ИПК Издательство стандартов, 1998.

187. Национальный стандарт РФ. "ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации" (утверждён Постановлением Госстандарта РФ от 18.03.1999 № 77) // М.: ИПК Издательство стандартов, 1999.

188. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 10746-2-2000. Информационная технология. Взаимосвязь открытых систем. Управление данными и открытая распределённая обработка. Часть 2. Базовая модель" (утверждён Постановлением Госстандарта РФ от 26.12.2000 № 413-ст) // М.: ИПК Издательство стандартов, 2001.

189. Рекомендации по стандартизации РФ. "Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации" (утверждены Приказом Росстандарта РФ от 06.04.2005 № 77-ст) // М.: Стандартинформ, 2005.

190. Рекомендации по стандартизации РФ. "Р 50.1.056-2005. Техническая защита информации. Основные термины и определения" (утверждены Приказом Росстандарта РФ от 29.12.2005 № 479-ст) // М.: Стандартинформ, 2006.

191. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. Приказом Росстандарта РФ от 19.12.2006 № 317-ст) // М.: Стандартинформ, 2007.

192. Межгосударственный стандарт. "ГОСТ 12.0.230-2007. Система стандартов безопасности труда. Системы управления охраной труда. Общие требования" (утверждён Приказом Росстандарта РФ от 10.07.2007 № 169-ст) // М.: Стандартинформ, 2007.

193. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура" (утверждён Приказом Росстандарта РФ от 25.12.2007 № 403-ст) // М.: Стандартинформ, 2008.

194. Национальный стандарт РФ. "ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утверждён Приказом Росстандарта РФ от 17.12.2008 № 430-ст) // М.: Стандартинформ, 2009.

195. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 29109-1-2012. Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определённых в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщённая методология испытаний на соответствие" (утверждён Приказом Росстандарта РФ от 18.09.2012 № 349-ст) // М.: Стандартинформ, 2014.

196. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 29100-2013. Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности" (утверждён Приказом Росстандарта РФ от 08.11.2013 № 1539-ст) // М.: Стандартинформ, 2014.

197. Межгосударственный стандарт. "ГОСТ ISO/IEC 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура" (утверждён Приказом Росстандарта РФ от 20.11.2015 № 1928-ст) // М.: Стандартинформ, 2018.

198. Международный стандарт. "ГОСТ ISO/IEC 17067-2015. Оценка соответствия. Основные положения сертификации продукции и руководящие указания по схемам сертификации продукции" (утверждён Приказом Росстандарта РФ от 24.12.2015 № 2199-ст) // М.: Стандартинформ, 2016.

199. Межгосударственный стандарт. "ГОСТ ISO/IEC 15459-(1-6)-2016. Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 1. Индивидуальные транспортируемые единицы. Часть 2. Порядок регистрации. Часть 3. Общие правила. Часть 4. Штучные изделия и упакованные единицы продукции. Часть 5. Индивидуальные возвратные транспортные упаковочные средства. Часть 6. Группы" (принят Межгосударственным советом по стандартизации, метрологии и сертификации по переписке, протокол от 27.07.2016 № 89-П) // М.: Стандартинформ, 2018.

200. Межгосударственный стандарт. "ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии. Словарь" (утверждён Приказом Росстандарта РФ от 22.09.2016 № 1189-ст) // М.: Стандартинформ, 2016.

201. Национальный стандарт РФ. "ГОСТ Р ИСО 11064-7-2016. Эргономическое проектирование центров управления. Часть 7. Принципы верификации и валидации" (утверждён Приказом Росстандарта РФ от 02.11.2016 № 1583-ст) // М.: Стандартинформ, 2016.

202. Национальный стандарт РФ. "ГОСТ Р 7.0.97-2016. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная

документация. Требования к оформлению документов" (утверждён Приказом Росстандарта РФ от 08.12.2016 № 2004-ст) // М.: Стандартинформ, 2017.

203. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 19794-14-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК" (утверждён Приказом Росстандарта РФ от 09.06.2017 № 528-ст) // М.: Стандартинформ, 2018.

204. Национальный стандарт РФ. "ГОСТ Р ИСО 15489-1-2019. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы" (утв. Приказом Росстандарта РФ от 26.03.2019 № 101-ст) // М.: Стандартинформ, 2019.

205. Национальный стандарт РФ. "ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018). Информационные технологии. Биометрия. Общие положения и примеры применения" (утверждён Приказом Росстандарта РФ от 19.11.2019 № 1184-ст) // М.: Стандартинформ, 2019.

206. Национальный стандарт РФ. "ГОСТ Р 59026-2020. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе стандарта LTE в режиме NB-IoT. Основные параметры" (утв. Приказом Росстандарта РФ от 15.09.2020 № 649-ст) // М.: Стандартинформ, 2020.

207. Межгосударственный стандарт. "ГОСТ 30721-2020 (ISO/IEC 19762:2016). Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь" (утв. Приказом Росстандарта РФ от 22.09.2020 № 6606-ст) // М.: Стандартинформ, 2020.

208. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27010-2020. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности при обмене информацией между отраслями и организациями" (утв. и введён в действие Приказом Росстандарта РФ от 10.11.2020 № 1041-ст) // М.: Стандартинформ, 2020.

209. Предварительный национальный стандарт РФ. "ПНСТ 516-2021. Информационные технологии. Интернет вещей. Спецификация LoRaWAN RU" (утв. Приказом Росстандарта РФ от 28.01.2021 № 5-пнст) // М.: Стандартинформ, 2021.

210. Предварительный национальный стандарт РФ. "ПНСТ 518-2021 (ИСО/МЭК 20924:2018). Информационные технологии. Интернет вещей. Термины и определения" (утв. Приказом Росстандарта РФ от 28.01.2021 № 7-пнст) // М.: Стандартинформ, 2021.

211. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии (ИТ). Методы и средства обеспечения безопасности.

Системы менеджмента информационной безопасности. Общий обзор и терминология" (утв. Приказом Росстандарта РФ от 19.05.2021 № 392-ст) // М.: Стандартинформ, 2021.

212. Национальный стандарт РФ. "ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (утв. Приказом Росстандарта РФ от 30.11.2021 № 1653-ст) // М.: Стандартинформ, 2021.

Международные нормативные акты

213. "Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948) // "Российская газета", № 67, 05.04.1995.

214. "Конвенция о защите прав человека и основных свобод" (заключена в гор. Риме 04.11.1950) // "Собрание законодательства РФ", 08.01.2001, № 2, ст. 163.

215. "Международный пакт о гражданских и политических правах" (принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // "Бюллетень Верховного Суда РФ", № 12, 1994.

216. "Конвенция о защите физических лиц при автоматизированной обработке персональных данных" (заключена в гор. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 419.

217. "Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации" (заключено в гор. Минске 01.06.2001) // Бюллетень международных договоров. 2009. № 6. С. 12-17.

218. Декларации принципов "Построение информационного общества - глобальная задача в новом тысячелетии" (принята в гор. Женева 12.12.2003) // URL: http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf.

219. "Модельный закон о праве на доступ к информации" (принят в гор. Санкт-Петербурге 17.04.2004 Постановлением 23-14 на 23-ем пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2004. № 34. С. 258-270.

220. "Соглашение между Правительством Российской Федерации и Правительством Словацкой Республики о взаимной защите секретной информации" (заключено в гор. Москве 07.11.2006) // Бюллетень международных договоров. 2016. № 10. С. 53-58.

221. "Договор о Евразийском экономическом союзе" (подписан в гор. Астане 29.05.2014) // URL: http://www.pravo.gov.ru.

222. Регламент № 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" (принят в гор. Брюсселе 27.04.2016) // URL: http://eur-lex.europa.eu.

223. Решение Совета Евразийской экономической комиссии от 03.11.2016 № 81 "Об утверждении Правил надлежащей лабораторной практики Евразийского экономического союза в сфере обращения лекарственных средств" // URL: http://www.eaeunion.org.

224. "Концепция ответственного обмена геномными данными и данными, связанными со здоровьем человека" // https://www.ga4gh.org/wp-content/uploads/ Framework-Russian-translation.pdf.

Нормативные правовые акты других государств

225. Закон Новой Зеландии. "Закон об официальных секретах 1951 года" (1951 № 77) // URL: http://www.nzlii.org/nz/legis/hist_act/osa19511951n77183.

226. "Протокол обозначений маркировки конфиденциальной информации" (англ. Traffic Light Protocol). Официальный сайт Департамента внутренней безопасности США. // URL: https://www.us-cert.gov/tlp.

227. Закон об информации США. "Classified National Security Information". Executive Order 13526 of December 29, 2009 // URL: https://www.govinfo.gov/content/pkg/FR-2010-01-08/pdf/C1-2009-31418.pdf.

228. Закон об информации Великобритании. "Security Policy Framework" (SPF) // URL: https://www.gov.uk/ government/publications security-policy-framework.

229. Декрет Президента Республики Беларусь от 21.12.2017 № 8 "О развитии цифровой экономики" // URL: http://president.gov.by/ru/official_documents_ru/view/ dekret-8-ot-21-dekabrja-2017-g-17716.

230. "Федеральный акт о защите персональных данных" (Datenschutzgesetz 2000 – DSG 2000) // URL: https://wipolex.wipo.int/ru/ legislation/profile/SE.

231. "Калифорнийский закон о защите прав потребителей 2018 года" (CCPA) // URL: https://www. dlapiperdataprotection.com/?t=law&c=US.

232. "Федеральный закон о защите данных Германии" (Bundesdatenschutzgesetz - BDSG) от 05.07.2017 года // URL: https://www. dlapiperdataprotection.com/?t=law&c=DE.

233. "Law No. 78-17 of January 6, 1978 "On information technology, data files and civil liberties, the principal law regulating data protection in France", от 01.07.2019 года // URL: https://www.dlapiperdataprotection.com/?t=law&c=FR.

234. "Council of Europe Committee of Ministers. Recommendation № R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes", 1989 // URL: http://www.coe.int/t/dg3/healthbioethic/texts_and_ documents/Rec(89)2E.pdf.

Научная и учебная литература

235. Агапов А.Б. Основы федерального информационного права России. М.: Экономика, 1995. 230 с.

236. Авакьян С.А. Конституционное право России: Учебный курс. В 2-х томах. Том 1. М.: Юристъ, 2005. 617 с.

237. Апарин Г.А., Городецкий И.Е. Допуски и технические измерения, 4-е изд., М., 1956.

238. Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991. 272 с.

239. Бачило И.Л. Информационное право: учебник для академического бакалавриата. 5-е изд., пер. и доп. М.: Юрайт, 2019. 419 с.

240. Бизнес: толковый словарь / Г.Бетс [и др.]. / Под общ. ред. И.М.Осадчей. М.: ИНФРА-М, 1998. 760 с.

241. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации. № 1. 5-е изд., сущ. пер. и доп. М.: Либроком, 2021. 464 с.

242. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. № 2. 6-е изд., стереотип. М.: Ленанд, 2022. 368 с.

243. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. № 8. 3-е изд., стереотип. М.: Ленанд, 2020. 224 с.

244. Борисов М.А. Правовое регулирование допуска и доступа к информации в условиях цифровой экономики № 20. М.: Ленанд, 2021. 224 с.

245. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997. 537 с.

246. Глоссарий по информационному обществу / М.Р.Когаловский [и др.]. / Под общ. ред. Ю.Е.Хохлова. М.: Институт развития информационного общества, 2009. 160 с.

247. Городов О.А. Информационное право. 2-е изд. М.: Проспект, 2018. 304 с.

248. Даль В.И. Толковый словарь живого великорусского языка. В 4-х томах, 6-е издание, стереотипное, М.: Дрофа, 2011. 2734 с.

249. Дёмушкин А.С. Документы и тайна. М.: Городец, 2003. 400 с.

250. Защита персональных данных. Опыт правового регулирования / Сост. Е.К.Волчинская; Предисл. А.К.Симонов. М.: Галерея, 2001. 173 с.

251. Информационное общество: Информационные войны. Информационное управление. Информационная безопасность. / Под ред. М.А. Вуса. СПб.: СПбГУ, 1999. 212 с.

252. Информационное право: учебник для бакалавриата, специалитета и магистратуры / М.А.Федотов, А.А.Тедеев [и др.] / Под ред. М.А.Федотова. М.: Юрайт, 2020. 497 с.

253. Информационные технологии в юридической деятельности: учебник для академического бакалавриата / П.У.Кузнецов [и др.]. / Под общ. ред. П.У.Кузнецова. 3-е изд., перераб. и доп. М.: Юрайт, 2018. 325 с.

254. Комментарий к Федеральному закону от 3 декабря 2008 г. № 242-ФЗ "О государственной геномной регистрации в Российской Федерации" (постатейный) / Отв. ред. Е.Н. Холопова // СПС КонсультантПлюс. 2016.

255. Копылов В.А. Информационное право. 2-е изд., перераб. и доп. М.: Юристъ, 2005. 512 с.

256. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой И.А. Основы управления информационной безопасностью. М.: Горячая линия - Телеком, 2013. 244 с.

257. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство / МВД России, Санкт-Петербургский ун-т. СПб.: Университет, 2000. 424 с.

258. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. М.: Палеотип, 2002. 148 с.

259. Малюк А.А., Королёв В.И., Фомичёв В.М. Введение в информационную безопасность: Учебное пособие для вузов / Под ред. В.С. Горбатова. М.: Горячая линия - Телеком, 2011. 288 с.

260. Минбалеев А.В. Правовое регулирование рекламной деятельности: Учебное пособие для студентов вузов, обучающихся по специальности 030501 "Юриспруденция". / Под ред. В.В. Кваниной. М.: Юриспруденция, 2010. 223 с.

261. Новицкий В.А. Теория российского процессуального доказывания и правоприменения: Монография. Ставрополь: Изд-во СГУ, 2002. 584 с.

262. Ожегов С.И. Словарь русского языка: Ок. 53000 слов / Под общ. ред. проф. Л.И.Скворцова. 24-е изд., испр. М.: Оникс, Мир и Образование, 2007. 1200 с.

263. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Под ред. Т.А.Поляковой, А.А.Стрельцова. М.: Юрайт, 2016. 325 с.

264. Рассолов И.М. Информационное право: учебник и практикум для академического бакалавриата. 5-е изд., перераб. и доп. М.: Юрайт, 2017. 347 с.

265. Российская энциклопедия по охране труда: В 3-х томах. / Рук. проекта М.Ю.Зурабов / Отв. ред. А.Л.Сафонов. 2-е изд., перераб. и доп. М.: НЦ ЭНАС, 2007.

266. Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью / Сост.: Ю.Н.Жданов, В.П.Зимин, Т.Н.Москалькова, В.С.Овчинский, Н.Б.Слюсарь, В.В.Черников. М.: СПАРК, 1998. 388 с.

267. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации" (постатейный). М.: Статут, 2015. 320 с.

268. Северин В.А. Комплексная защита информации на предприятии: Учебник для вузов / Под ред. проф. Б.И.Пугинского. М.: Городец, 2008. 368 с.

269. Словарь финансово-экономических терминов / Под ред. И.З. Ярыгиной, Н.Г. Кондрахиной. М: Финансовый университет, 2012. 172 с.

270. Словарь финансово-экономических терминов / Под общ. ред. д.э.н., проф. М.А. Эскиндарова. 2-е изд. М.: Дашков и К°, 2017. 1168 с.

271. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. / Под ред. В.А. Садовничего и В.П. Шерстюка. М.: МЦНМО, 2002. 296 с.

272. Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: Монография. М.: ИНФРА-М, 2016. 227 с.

273. Ушаков Д.Н. Толковый словарь русского языка. В 3-х томах на основе 4-х томного издания 1948 г. М.: Вече, Си ЭТС, 2001. 890 с.

274. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: Учебное пособие. М.: Юрист, 2001. 412 с.

275. Цифровая трансформация: вызовы праву и векторы научных исследований: Монография [Электронный ресурс]. / Под общ. ред. А.Н. Савенкова. / Отв. ред. Т.А. Полякова, А.В. Минбалеев. Электрон. дан. (1,3 Мб). М.: Институт государства и права РАН, 2020.

276. Цифровое право : учебник / под общ. ред. В.В.Блажеева, М.А.Егоровой. М.: Проспект, 2020. 640 с.

277. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. 2-е изд. М.: Академический Проект, Гаудеамус, 2004. 544 с.

278. Min Chen, Shiwen Mao, Yin Zhang, Victor C.M. Leung. Big Data. Related Technologies, Challenges, and Future Prospects. Spinger, 2014. 100 p.

Диссертации и авторефераты

279. Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: Автореферат диссертации кандидата юридических наук. – Москва, 2005.

Публикации в периодических изданиях

280. Бикбулатова Ю.С., Дупан А.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт // Российская юстиция, 2019, № 9.

281. Богданова Е.Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация // Lex russica, 2019, № 6.

282. Борисов М.А. К вопросу о моделировании системы защиты информации в условиях информационного противоборства. Научный журнал Вестник РГГУ. Серия Информатика. Защита информации. Математика. // М.: РГГУ, 2010, № 12(55)/10. С. 285-289.

283. Борисов М.А. К вопросу о совершенствовании системы лицензирования деятельности в области криптографической защиты информации в условиях развития цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2018, № 6. С. 286-288.

284. Борисов М.А. К вопросу о совершенствовании допуска к государственной тайне в условиях развития цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2018, № 6. С. 289-291.

285. Борисов М.А. Совершенствование системы доступа субъектов к электронным документам // Пробелы в российском законодательстве, М.: Юр-ВАК, 2019, № 2. С. 213-215.

286. Борисов М.А., Заводцев И.В. Проблемы совершенствования допуска и доступа субъектов в информационные системы в условиях цифровой экономики // Проблемы экономики и юридической практики, М.: Юр-ВАК, 2019, № 2. С. 267-270.

287. Борисов М.А., Северин В.А. К вопросу о совершенствовании системы классификации информации в условиях развития цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2019, № 6. С. 234-237.

288. Борисов М.А., Северин В.А. Проблемы допуска и доступа субъектов к коммерческой и служебной тайне в условиях цифровой экономики // Пробелы в российском законодательстве, М.: Юр-ВАК, 2019, № 6. С. 238-241.

289. Борисов М.А. "Проблемы публикационной активности в современных условиях" // "Информационное право", М.: РНИ-ИИС, 2023, № 1 (75), С. 24-27.

290. Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право, 2008, № 4 // URL: http://lawinfo.ru/catalog.

291. Заводцев И.В., Борисов М.А., Бондаренко Н.Н., Мелешко В.А. Моделирование угроз безопасности информации и определение их актуальности для информационных систем объектов информатизации федеральных органов исполнительной власти // Computational nanotechnology, М.: Юр-ВАК, 2022, Т. 9, № 1, С. 106-114.

292. Зражевская Т.Д., Савченко С.А. Воздействие конституционного законодательства на формирование правовой системы России // Вестник ВГУ, Серия: Право, 2011, № 1(10).

293. Ищейнов В.Я. Организация доступа сотрудников к конфиденциальным массивам электронных документов и базам данных. // Делопроизводство, 2018, № 1. С. 63-65.

294. Кудрявцев М.А. Информационные права личности: проблема институциональных гарантий // Конституционное и муниципальное право, 2018, № 6. С. 26-30.

295. Лапидус Л.В. Эволюция цифровой экономики // Ежегодная Международная Научная конференция Ломоносовские чтения-2018. Секция экономических наук. "Цифровая экономика: человек, технологии, институты".

296. Лыжник О.В. Можно ли излечиться от наркомании // URL: https://kubnews.ru/obshchestvo/2018/10/12/mozhno-li-izlechitsya-ot-narkomanii.

297. Матвеев И.А. Электронная экономика: сущность и этапы развития // Управление экономическими системами: электронный научный журнал, 2012, Вып. 6 (42).

298. Морозов А.В. Проблемы правового регулирования цифровых технологий в России и за рубежом // Вестник университета имени О.Е.Кутафина (МГЮА), 2019, № 12. С. 170-172.

299. Основное препятствие: "Греф назвал главную проблему России". "Бизнес", 14.03.2019 // URL: https://www.gazeta.ru/business/2019/03/14/12242413.shtml.

300. Пази. М. "Кибер-ДНК", "Эксперт", 2019, № 16 // URL: https://expert.ru/russian_reporter/2019/16/kiber-dnk.

301. Полякова Т.А., Бойченко И.С. Информационная безопасность через призму национального проекта "Цифровая экономика": правовые проблемы и векторы решений // Право и государство, 2019, № 2. С. 97-100.

302. Полякова Т.А., Минбалеев А.В. Цифровые инновации и проблемы развития механизма правового регулирования в России // Информационное право, 2019, № 4. С. 12-15.

303. Сабанов А.Г., Смолина С.Г. Сравнительный анализ методов биометрической идентификации личности // М.: Труды ИСА РАН, Том 66, № 3/2016.

304. Северин В.А., Коржова И.В. Вопросы безопасности при обращении криптовалюты // Вестник Московского университета. Серия 26. Государственный аудит, 2019, № 4. С. 81-89.

305. Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право, 2016, № 4. С. 13-19.

306. Смолян Г.Л., Черешкин Д.С. О формировании информационного общества в России. // Информационное общество, 1998, Вып. 6. С. 8-13.

307. Хургин В.М. Право на доступ к информации, или Как (и чем) сражаться с бюрократом // Информационное общество, 2001, № 4. С. 35-43.

308. Kevin Ashton. "Internet Of Things". Gartner IT glossary. Gartner, 5 May 2012 // URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things.

309. Kevin Ashton. "That ‘Internet of Things’ Thing. In the real world, things matter more than ideas". RFID Journal, 22 June 2009 // URL: https://www.webcitation.org/6DuYQRsDZ?url=http://www.rfidjournal.com/article/pdf/4986/1/1/rfidjournal-article4986.pdf.

310. "Disruptive Civil Technologies. Six Technologies with Potential Impacts on US Interests out to 2025". National Intelligence Council, 11 April 2008 // URL: https://fas.org/irp/nic/disruptive.pdf.

311. Opinion 1/2010 On the concepts of "controller" and "processor". Article 29 Data Protection Working Party. 16 February.

312. Macmanus M. A guide to recommender systems. January, 2009 // URL: http://readwrite.com/2009/01/26/recommender_systems.

313. Nicu Popescu. Hybrid tactics: neither new nor only Russian // European Union Institute for Security Studies, January 2015.

Судебная практика

314. Постановление Конституционного Суда РФ от 03.02.1998 № 5-П // URL: http://www.consultant.ru.

315. Определение Верховного Суда РФ от 12.10.2000 № 4-Г00-18 // URL: http://www.consultant.ru.

316. Определение Верховного Суда РФ от 13.01.2004 № 66-г03-19 // URL: http://www.consultant.ru.

317. Постановление ФАС Волго-Вятского округа от 09.03.2011 по делу № А82-9212/2010 // URL: http://www.consultant.ru.

318. Определение Верховного Суда РФ от 12.04.2011 № 206-Г11-2 // URL: http://www.consultant.ru.

319. Постановление Конституционного Суда РФ от 18.07.2012 № 19-П // URL: http://www.consultant.ru.

320. Постановление Президиума ВАС РФ от 15.10.2013 № 7070/13 по делу № А28-770/2002 // URL: http://www.consultant.ru.

321. Постановление Пленума Высшего Арбитражного Суда РФ от 25.12.2013 № 100 "Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)" // URL: http://www.consultant.ru.

322. Постановление ФАС Московского округа от 12.03.2014 № Ф05-1766/2014 по делу № А40-23492/13-138-219 // URL: http://www.consultant.ru.

323. Постановление Восемнадцатого арбитражного апелляционного суда от 05.08.2014 № 18АП-7541/2014 // URL: http://www.consultant.ru.

324. Определение Конституционного Суда РФ от 23.06.2015 № 1538-О // URL: http://www.consultant.ru.

325. Постановление Президиума Нижегородского областного суда от 06.07.2016 по делу № 44г-49/2016 // URL: http://www.consultant.ru.

326. Апелляционное определение Санкт-Петербургского городского суда от 27.09.2016 № 33-17808/2016 // URL: http://www.consultant.ru.

327. Определение Конституционного Суда РФ от 29.09.2016 № 1863-О // URL: http://www.consultant.ru

328. Постановление Двадцатого арбитражного апелляционного суда от 09.11.2016 № 20АП-6427/2016 // URL: http://www.consultant.ru.

329. Постановление Арбитражного суда Московского округа от 27.04.2018 № Ф05-5117/2018 по делу № А40-127318/2017 // URL: http://www. consultant.ru.

330. Определение Конституционного Суда РФ от 28.11.2019 № 3012-О // URL: http://www.consultant.ru.

331. Определение Верховного Суда РФ от 23.03.2020 № 4-КГ20-8 // URL: http://www.consultant.ru.

Справочные информационные ресурсы

332. Официальный сайт: "Единый реестр российских программ для электронных вычислительных машин и баз данных" // URL: https://reestr.minsvyaz.ru/reestr.

333. Официальный сайт: "Реестр зарегистрированных систем добровольной сертификации" // URL: https://www.gost.ru/portal/gost/home/activity/compliance/VoluntaryAcknowledgement/reestr.

334. Официальный сайт: "Федеральный портал проектов нормативных правовых актов" // URL: https://regulation.gov.ru.

335. Официальный сайт: "Система межведомственного электронного взаимодействия" // URL: https://smev.gosuslugi.ru/portal.

336. Официальный сайт: "Официальный интернет-портал правовой информации" // URL: http://www.pravo.gov.ru.

337. Официальный сайт: "Портал открытых данных Российской Федерации" // URL: https://data.gov.ru.

338. Официальный сайт: "Информационный портал Евразийского экономического союза" // URL: https://portal.eaeunion.org/ru-ru/public/main.aspx.

339. Официальный сайт: "Единый реестр доменных имён, указателей страниц сайтов в сети "Интернет" // URL: http://eais.rkn.gov.ru.

340. Официальный сайт: "Global Manufacturing Execution Systems (MES) Market 2009-2013" // URL: http://www.tadviser.ru/index.php/MES.

341. Официальный сайт: Данные судебной статистики. Судебный департамент // URL: http://www.cdep.ru/index.php?id=79&item=3212.

342. Официальный сайт: ОСЭР // URL: http://oecdru.org/oecd_rf.html.

343. Доклад о мировом развитии "Цифровые дивиденды". World Bank Group, 2016 // URL: https://openknowledge.worldbank.org/handle/10986/23347.

344. Реестр иностранных агентов: // URL: https://minjust.gov.ru/uploaded/files/reestr-inostrannyih-agentov-01-12-2022.pdf.

345. Реестр гидрологических данных // URL: URL: https://www.meteorf.gov.ru/opendata/7703092752-reestrav.

346. Анализ НП "ЦМАПК" "Наука, технологии, высокотехнологичное оборудование" // URL: http://www.forecast.ru.

Приложение 1

ОСНОВНЫЕ ВИДЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ПРИНЯТЫЕ В ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Виды информации с ограниченным доступом	**Правовая регламентация защиты**
I. Информация, составляющая государственную тайну	
Информация, составляющая государственную тайну или государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.	ст. 2 Закона РФ от 21.07.1993 № 5485-1 (ред. от 05.12.2022) "О государственной тайне"
II. Информация, составляющая коммерческую тайну, служебную тайну и иную тайну	
Коммерческая тайна	
Информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны.	ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ (ред. от 14.07.2022) "О коммерческой тайне"
Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления	ст. 1465 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)

Виды информации с ограниченным доступом	Правовая регламентация защиты
профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путём введения режима коммерческой тайны. Секретом производства не могут быть признаны сведения, обязательность раскрытия которых либо недопустимость ограничения доступа к которым установлена законом или иным правовым актом.	
Условия договора инвестиционного товарищества не подлежат раскрытию и охраняются в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ "О коммерческой тайне", за исключением раскрытия условий данного договора третьим лицам в случаях, предусмотренных настоящим Федеральным законом и договором инвестиционного товарищества.	ст. 12 Федерального закона от 28.11.2011 № 335-ФЗ (ред. от 02.07.2021) "Об инвестиционном товариществе"
Служебная тайна	
К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.	п. 1.2 Постановления Правительства РФ от 03.11.1994 № 1233 (ред. от 06.08.2020) "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии и

Виды информации с ограниченным доступом	Правовая регламентация защиты
	уполномоченном органе по космической деятельности"
Служебную тайну в области обороны составляют сведения, которые образуются при осуществлении полномочий органами государственной власти Российской Федерации, функций органами государственной власти субъектов Российской Федерации, органами местного самоуправления и организациями по организации и выполнению мероприятий в области обороны, распространение которых может нанести вред при выполнении указанных мероприятий.	ст. 3.1 Федерального закона от 31.05.1996 № 61-ФЗ (ред. от 04.11.2022) "Об обороне"
Иная тайна	
Информация об авторском праве – это любая информация, которая идентифицирует произведение, автора или иного правообладателя, либо информация об условиях использования произведения, которая содержится на оригинале или экземпляре произведения, приложена к нему или появляется в связи с сообщением в эфир или по кабелю либо доведением такого произведения до всеобщего сведения, а также любые цифры и коды, в которых содержится такая информация.	ст. 1300 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)
В отношении любой информации, которая идентифицирует объект смежных прав или правообладателя, либо информации об условиях использования этого объекта, которая содержится на соответствующем материальном носителе, приложена к нему или появляется в связи с сообщением в эфир или по кабелю либо доведением этого объекта до всеобщего сведения, а также любых цифр и кодов, в которых содержится такая информация (информация о смежном праве), соответственно применяются положения статей 1300 и 1311 настоящего Кодекса.	ст. 1310 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)

Изобретение, полезная модель или промышленный образец, созданные работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, признаются соответственно служебным изобретением, служебной полезной моделью или служебным промышленным образцом.	ст. 1370 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)
Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю. Гражданин, которому в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства.	ст. 1470 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)
III. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна)	
Адвокатская тайна	
Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с её оказанием.	ст. 8 Федерального закона от 31.05.2002 № 63-ФЗ (ред. от 10.11.2022) "Об адвокатской деятельности и адвокатуре в Российской Федерации"
Аудиторская тайна	
Аудиторскую тайну составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и её работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг, предусмотренных настоящим Федеральным законом, за исключением: сведений, разглашённых самим лицом, которому оказывались услуги, либо с его согласия, сведений о заключении договора оказания аудиторских услуг, сведений о величине оплаты аудиторских услуг.	ст. 9 Федерального закона от 30.12.2008 № 307-ФЗ (ред. от 17.02.2023) "Об аудиторской деятельности"

Банковская тайна	
Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам, а также иным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.	ст. 857 Гражданского кодекса РФ (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 08.07.2021)
Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах её клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.	ст. 26 Федерального закона от 02.12.1990 № 395-1 (ред. от 29.12.2022) "О банках и банковской деятельности"
Банк России на своём официальном сайте в информационно-телекоммуникационной сети "Интернет" раскрывает информацию, содержащуюся в отчётности кредитных организаций (банковских групп) и представляемую в Банк России в соответствии со статьёй 43 Федерального закона "О банках и банковской деятельности", за исключением сведений, составляющих банковскую тайну. Состав указанной информации и порядок её раскрытия устанавливаются нормативным актом Банка России.	ст. 57 Федерального закона от 10.07.2002 № 86-ФЗ (ред. от 14.07.2022) "О Центральном банке Российской Федерации (Банке России)"
На финансовые органы, получающие от органов Федерального казначейства сведения о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, являющиеся информацией ограниченного доступа, распространяются требования о защите и об использовании информации, установленные федеральными законами.	ст. 241 Бюджетного кодекса РФ от 31.07.1998 № 145-ФЗ (ред. от 28.12.2022)

Пользователи кредитных историй, источники формирования кредитных историй и иные лица, получившие в соответствии с настоящим Федеральным законом доступ к информации, входящей в состав кредитной истории, и (или) к коду субъекта кредитной истории, обязаны не разглашать третьим лицам указанную информацию. За разглашение или незаконное использование данной информации указанные лица несут ответственность в порядке, предусмотренном законодательством Российской Федерации. Бюро кредитных историй обеспечивает хранение записи кредитной истории в течение семи лет со дня последнего изменения информации, содержащейся в этой записи кредитной истории. Запись и (или) иные данные кредитной истории аннулируются (исключаются из состава сведений, включаемых в кредитные отчёты, и перемещаются в архив кредитных историй соответствующего бюро кредитных историй для хранения в нем в течение трёх лет).	ст. 6, 7 Федерального закона от 30.12.2004 № 218-ФЗ (ред. от 28.12.2022) "О кредитных историях"
Если иное не предусмотрено федеральным законом, кредитор или лицо, действующее от его имени и (или) в его интересах, при совершении действий, направленных на возврат просроченной задолженности, не вправе без согласия должника передавать (сообщать) третьим лицам или делать доступными для них сведения о должнике, просроченной задолженности и её взыскании и любые другие персональные данные должника. Лица, получившие сведения, указанные в части 3 настоящей статьи, в ходе переговоров о заключении договора или выдаче доверенности, обязаны сохранять их конфиденциальность и в том случае, если они не будут впоследствии осуществлять действия, направленные на возврат просроченной задолженности соответствующих физических лиц. Если в ходе переговоров о заключении договора или выдаче доверенности сторона получает сведения, которые передаются ей другой стороной в качестве конфиденциальных, она обязана не раскрывать эти сведения и не использовать их ненадлежащим образом для своих целей независимо от того, будет ли заключён договор. При нарушении этой обязанности лицо обязано возместить должнику убытки, причинённые в результате раскрытия конфиденциальных сведений или использования их для своих целей.	ст. 6 Федерального закона от 03.07.2016 № 230-ФЗ (ред. от 20.10.2022) "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях"

Кредитное рейтинговое агентство обязано соблюдать условия конфиденциальности информации, полученной от рейтингуемого лица, а также соблюдать требования к сохранности и защите информации, полученной в процессе деятельности кредитного рейтингового агентства, установленные Банком России.	ст. 9 Федерального закона от 13.07.2015 № 222-ФЗ (ред. от 19.12.2022) "О деятельности кредитных рейтинговых агентств в Российской Федерации, о внесении изменения в статью 76.1 Федерального закона "О Центральном банке Российской Федерации (Банке России)" и признании утратившими силу отдельных положений законодательных актов Российской Федерации"
Трансфер-агенты обязаны соблюдать конфиденциальность информации, полученной в связи с осуществлением функций трансфер-агента. Держатели реестра и депозитарии обязаны обеспечить конфиденциальность информации о лице, которому открыт лицевой счёт (счёт депо), а также информации о таком счёте, включая операции по нему. При осуществлении полномочий, предоставленных настоящим Федеральным законом, Банк России обязан обеспечивать конфиденциальность предоставляемой ему информации, за исключением информации, раскрываемой в соответствии с законодательством Российской Федерации о ценных бумагах.	ст. 8.1, 8.6, 15.8, 44.1 Федерального закона от 22.04.1996 № 39-ФЗ (ред. от 19.12.2022) "О рынке ценных бумаг"
Центральный депозитарий обязан обеспечить конфиденциальность информации о счетах и об операциях его клиентов. Правила защиты информации центральным депозитарием должны предусматривать процедуры доступа к ней должностных лиц и сотрудников центрального депозитария, а также правила её предоставления иным лицам.	ст. 14 Федерального закона от 07.12.2011 № 414-ФЗ (ред. от 14.07.2022) "О центральном депозитарии"

Клиринговая организация и лицо, осуществляющее функции центрального контрагента, обязаны обеспечить конфиденциальность информации об обязательствах, в отношении которых проводится клиринг, конфиденциальность сведений, предоставляемых участниками клиринга в соответствии с частью 3 статьи 11 настоящего Федерального закона, конфиденциальность информации о торговых счетах депо и торговых товарных счетах и конфиденциальность информации об операциях по указанным счетам, о которой стало известно в связи с оказанием клиринговых услуг и (или) осуществлением функций центрального контрагента.	ст. 20 Федерального закона от 07.02.2011 № 7-ФЗ (ред. от 02.07.2021) "О клиринге, клиринговой деятельности и центральном контрагенте"
Лица, оказывающие услуги по проведению организованных торгов на товарном и (или) финансовом рынках на основании лицензии биржи или лицензии торговой системы, обязаны предоставлять уполномоченному органу по его запросу информацию об участниках торгов и их клиентах, а также о поданных ими заявках и заключаемых ими договорах в порядке и объёме, установленных Банком России по согласованию с уполномоченным органом. Организатор торговли, клиринговая организация и центральный контрагент не вправе разглашать факт передачи в уполномоченный орган информации, указанной в пунктах 1 - 3 настоящей статьи.	ст. 7.1-1 Федерального закона от 07.08.2001 № 115-ФЗ (ред. от 18.03.2023) "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма"
Запрещается использование инсайдерской информации: для осуществления операций с финансовыми инструментами, иностранной валютой и (или) товарами, которых касается инсайдерская информация, за свой счёт или за счёт третьего лица, за исключением совершения операций в рамках исполнения обязательства по покупке или продаже финансовых инструментов, иностранной валюты и (или) товаров, срок исполнения которого наступил, если такое обязательство возникло в результате операции, совершенной до того, как лицу стала известна инсайдерская информация; путём передачи её другому лицу, за исключением случаев передачи этой информации лицу, включённому в список инсайдеров, в связи с исполнением обязанностей, установленных федеральными законами, либо в связи с исполнением трудовых обязанностей или исполнением договора; путём дачи рекомендаций	ст. 6 Федерального закона от 27.07.2010 № 224-ФЗ (ред. от 07.10.2022) "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации"

третьим лицам, обязывания или побуждения их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров. Запрещается осуществлять действия, относящиеся в соответствии с настоящим Федеральным законом к манипулированию рынком. Передача инсайдерской информации для её опубликования редакции средства массовой информации, её главному редактору, журналисту и иному её работнику, а также её опубликование в средстве массовой информации не являются нарушением запрета, установленного пунктом 2 части 1 настоящей статьи. При этом передача такой информации для её опубликования или ее опубликование не освобождают от ответственности за незаконное получение, использование, разглашение сведений, составляющих государственную, налоговую, коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну, и от соблюдения обязанности по раскрытию или предоставлению инсайдерской информации.	
Агент по выдаче, погашению и обмену инвестиционных паёв в соответствии с настоящим Федеральным законом, нормативными актами Банка России и договором, заключённым с управляющей компанией, обязан соблюдать конфиденциальность информации, полученной в связи с осуществлением деятельности по выдаче, погашению и обмену инвестиционных паёв.	ст. 28 Федерального закона от 29.11.2001 № 156-ФЗ (ред. от 27.01.2023) "Об инвестиционных фондах"
Саморегулируемая организация обязана обеспечивать конфиденциальность ставших ей известными сведений о финансовых организациях, являющихся членами саморегулируемой организации, финансовых организациях, представивших документы для приёма в члены, в кандидаты в члены саморегулируемой организации, в том числе сведений об их клиентах. Саморегулируемой организацией должны быть предусмотрены меры по защите при получении, использовании, обработке и хранении информации, неправомерное использование которой работниками саморегулируемой организации может причинить моральный вред и (или) имущественный ущерб лицам, указанным в части 3 настоящей статьи, или создать предпосылки для причинения таким вреда и (или) ущерба.	ст. 13 Федерального закона от 13.07.2015 № 223-ФЗ (ред. от 02.07.2021) "О саморегулируемых организациях в сфере финансового рынка"

Налоговая тайна	
Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов, за исключением сведений: являющихся общедоступными, в том числе ставших таковыми с согласия их обладателя - налогоплательщика (плательщика страховых взносов), об идентификационном номере налогоплательщика и др. Налоговая тайна не подлежит разглашению налоговыми органами, органами внутренних дел, следственными органами, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом. К разглашению налоговой тайны относится, в частности, использование или передача другому лицу информации, составляющей коммерческую тайну (секрет производства) налогоплательщика, плательщика страховых взносов и ставшей известной должностному лицу налогового органа, органа внутренних дел, следственного органа, органа государственного внебюджетного фонда или таможенного органа, привлечённому специалисту или эксперту при исполнении ими своих обязанностей.	ст. 102 Налогового кодекса РФ (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 18.03.2023)
Содержание данных налогового учёта (в том числе данных первичных документов) является налоговой тайной. Лица, получившие доступ к информации, содержащейся в данных налогового учёта, обязаны хранить налоговую тайну. За её разглашение они несут ответственность, установленную действующим законодательством.	ст. 313 Налогового кодекса РФ (часть вторая) от 05.08.2000 № 117-ФЗ (ред. от 18.03.2023)
Экспертные организации должны обеспечивать конфиденциальность сведений, полученных в процессе проведения экспертизы, и использовать эти сведения только в целях, для которых они предоставлены. Оператор фискальных данных обязан обеспечивать конфиденциальность фискальных данных. При этом передача фискальных данных в налоговые органы не признается нарушением конфиденциальности.	ст. 3.1, 4.1, 4.5 Федерального закона от 22.05.2003 № 54-ФЗ (ред. от 29.12.2022) "О применении контрольно-кассовой техники при осуществлении

	наличных денежных расчётов и (или) расчётов с использованием электронных средств платежа"
Врачебная тайна	
Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением установленных случаев. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.	ст. 13, 92 Федерального закона от 21.11.2011 № 323-ФЗ (ред. от 29.12.2022) "Об основах охраны здоровья граждан в Российской Федерации"
Результаты обследования лица, вступающего в брак, составляют врачебную тайну и могут быть сообщены лицу, с которым оно намерено заключить брак, только с согласия лица, прошедшего обследование.	ст. 15 Семейного кодекса РФ от 29.12.1995 № 223-ФЗ (ред. от 19.12.2022)
Сведения о факте обращения гражданина за психиатрической помощью, состоянии его психического здоровья и диагнозе психического расстройства, иные сведения, полученные при оказании ему психиатрической помощи, составляют врачебную тайну, охраняемую законом. Для реализации прав и законных интересов лица, страдающего психическим расстройством, по его просьбе либо по просьбе его законного представителя им могут быть предоставлены сведения о состоянии психического здоровья данного лица и об оказанной ему психиатрической помощи.	ст. 9 Закона РФ от 02.07.1992 № 3185-1 (ред. от 30.12.2021) "О психиатрической помощи и гарантиях прав граждан при её оказании"

Врачам и иным сотрудникам учреждения здравоохранения запрещается разглашать сведения о доноре и реципиенте. Разглашение таких сведений влечёт ответственность в соответствии с законодательством Российской Федерации.	ст. 14 Закона РФ от 22.12.1992 № 4180-1 (ред. от 01.05.2022) "О трансплантации органов и (или) тканей человека"
Информация о персональных данных донора не подлежит разглашению реципиенту, равно как и персональные данные реципиента не подлежат разглашению донору.	ст. 13 Федерального закона от 20.07.2012 № 125-ФЗ (ред. от 28.06.2022) "О донорстве крови и её компонентов"
Тайна страхования	
Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несёт ответственность в соответствии с правилами, предусмотренными настоящим Кодексом.	ст. 946 Гражданского кодекса РФ (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 08.07.2021)
Медицинские организации, страховые медицинские организации, Федеральный фонд и территориальные фонды определяют работников, допущенных к работе с данными персонифицированного учёта сведений о медицинской помощи, оказанной застрахованным лицам, и обеспечивают их конфиденциальность в соответствии с установленными законодательством Российской Федерации требованиями по защите персональных данных.	ст. 47 Федерального закона от 29.11.2010 № 326-ФЗ (ред. от 19.12.2022) "Об обязательном медицинском страховании в Российской Федерации"
Фонд в установленных законодательством Российской Федерации случаях и порядке вправе получать, обрабатывать и хранить информацию, доступ к которой ограничен в соответствии с федеральными законами, в том числе осуществлять обработку персональных данных вкладчиков - физических лиц, страхователей - физических лиц, участников, застрахованных лиц, выгодоприобретателей и правопреемников участников и застрахованных лиц. Фонд не вправе передавать информацию, в отношении которой в	ст. 15 Федерального закона от 07.05.1998 № 75-ФЗ (ред. от 27.01.2023) "О негосударственных пенсионных фондах"

соответствии с федеральными законами установлена обязанность соблюдать её конфиденциальность, третьим лицам, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами. Указанная информация может быть передана специализированному депозитарию фонда в связи с осуществлением им функций, предусмотренных настоящим Федеральным законом и другими федеральными законами, правопреемникам участников и застрахованных лиц, а также в установленных законодательством Российской Федерации случаях по требованию следственных, судебных, налоговых органов, Банка России, Агентства по страхованию вкладов.	
Сведения, содержащиеся в индивидуальных лицевых счетах, относятся к информации, в отношении которой установлено требование об обеспечении её конфиденциальности.	ст. 6 Федерального закона от 01.04.1996 № 27-ФЗ (ред. от 28.12.2022) "Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования"
Страховщик обязан обеспечивать конфиденциальность полученных в результате своей деятельности сведений о страхователе, застрахованном и лицах, имеющих право на получение страховых выплат. Ограничение доступа к информации о страхователе осуществляется в порядке, установленном статьёй 18.2 настоящего Федерального закона. Информация ограниченного доступа не подлежит разглашению страховщиком и его должностными лицами, органами внутренних дел, следственными органами, за исключением случаев, предусмотренных федеральными законами.	ст. 18, 18.2 Федерального закона от 24.07.1998 № 125-ФЗ (ред. от 03.04.2023) "Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний"
Нотариальная тайна	
Нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности. Суд может освободить нотариуса от обязанности сохранения тайны, если против нотариуса возбуждено уголовное дело в связи с совершением нотариального действия. Должностные лица нотариальной палаты обязаны	ст. 16, 28 "Основы законодательства Российской Федерации о нотариате" (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от

сохранять тайну совершения нотариальных действий. За разглашение тайны и причинение нотариусу, занимающемуся частной практикой, ущерба виновные несут ответственность в соответствии с законодательством Российской Федерации.	29.12.2022)
Консульское должностное лицо, совершающее нотариальные действия, обязано соблюдать тайну совершения нотариальных действий. Консульское должностное лицо, виновное в разглашении тайны совершения нотариальных действий, несёт ответственность в соответствии с законодательством Российской Федерации.	ст. 26 Федерального закона от 05.07.2010 № 154-ФЗ (ред. от 05.12.2022) "Консульский устав Российской Федерации"
Тайна завещания	
Нотариус, другое удостоверяющее завещание лицо, переводчик, исполнитель завещания, свидетели, супруг, участвующий в совершении совместного завещания супругов, супруг, присутствующий при удостоверении завещания другого супруга, сторона наследственного договора, нотариусы, имеющие доступ к сведениям, содержащимся в единой информационной системе нотариата, и лица, осуществляющие обработку данных единой информационной системы нотариата, а также гражданин, подписывающий завещание или наследственный договор вместо завещателя или наследодателя, не вправе до открытия наследства разглашать сведения, касающиеся содержания завещания или наследственного договора, их совершения, заключения, изменения или отмены. Лицо, не являющееся исполнителем завещания, нотариусом или другим удостоверяющим завещание лицом, не вправе разглашать указанные сведения и после открытия наследства, если разглашение указанных сведений будет противоречить статье 152.2 настоящего Кодекса.	ст. 1123 Гражданского кодекса РФ (часть третья) от 26.11.2001 № 146-ФЗ (ред. от 03.04.2023)
Тайна усыновления	
Тайна усыновления ребёнка охраняется законом. Судьи, вынесшие решение об усыновлении ребёнка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомлённые об усыновлении, обязаны сохранять тайну усыновления ребёнка.	ст. 139 Семейного кодекса РФ от 29.12.1995 № 223-ФЗ (ред. от 19.12.2022)

Тайна ЗАГСа	
Записи актов гражданского состояния, а также иные сведения, содержащиеся в Едином государственном реестре записей актов гражданского состояния в соответствии с настоящим Федеральным законом, подлежат постоянному хранению, их уничтожение и изъятие не допускаются. В случае внесения исправлений или изменений в записи актов гражданского состояния, содержащиеся в Едином государственном реестре записей актов гражданского состояния, ранее составленные записи актов гражданского состояния сохраняются. Ведение Единого государственного реестра записей актов гражданского состояния, включая формирование, сбор, хранение, обработку и предоставление информации, осуществляется в федеральной государственной информационной системе ведения Единого государственного реестра записей актов гражданского состояния (далее - федеральная информационная система), функционирование которой обеспечивается в том числе в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных". Оператор федеральной информационной системы осуществляет защиту сведений, содержащихся в федеральной информационной системе.	ст. 13.1 Федерального закона от 15.11.1997 № 143-ФЗ (ред. от 03.04.2023) "Об актах гражданского состояния"
Тайна ломбарда	
К информации, составляющей профессиональную тайну при осуществлении ломбардом своей деятельности, относится информация, полученная ломбардом от заёмщика или поклажедателя в связи с заключением договора займа или договора хранения, за исключением наименования, описания технических, технологических и качественных характеристик невостребованной вещи, на которую в порядке, установленном статьёй 12 настоящего Федерального закона, обращено взыскание. Ломбард и его работники обязаны соблюдать конфиденциальность информации, составляющей в соответствии с частью 1 настоящей статьи профессиональную тайну, и в случае её разглашения несут ответственность в порядке, установленном законодательством Российской Федерации.	ст. 3 Федерального закона от 19.07.2007 № 196-ФЗ (ред. от 13.07.2020) "О ломбардах"

Тайна исповеди	
Тайна исповеди охраняется законом. Священнослужитель не может быть привлечён к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди.	ст. 3 Федерального закона от 26.09.1997 № 125-ФЗ (ред. от 29.12.2022) "О свободе совести и о религиозных объединениях"
Не подлежат допросу в качестве свидетелей священнослужитель об обстоятельствах, ставших ему известными из исповеди.	ст. 56 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)
Не подлежат допросу в качестве свидетелей священнослужители религиозных организаций, прошедших государственную регистрацию, об обстоятельствах, которые стали им известны из исповеди.	ст. 69 Гражданского процессуального кодекса РФ от 14.11.2002 № 138-ФЗ (ред. от 18.03.2023)
Не подлежат допросу в качестве свидетелей священнослужители религиозных организаций, прошедших государственную регистрацию, - об обстоятельствах, которые стали им известны из исповеди.	ст. 51 Кодекса административного судопроизводства РФ от 08.03.2015 № 21-ФЗ (ред. от 17.02.2023)
Тайна социального обеспечения	
Социальное обслуживание осуществляется также на следующих принципах - конфиденциальность. Не допускается разглашение информации, отнесённой законодательством Российской Федерации к информации конфиденциального характера или служебной информации, о получателях социальных услуг лицами, которым эта информация стала известна в связи с исполнением профессиональных, служебных и (или) иных обязанностей. Разглашение информации о получателях социальных услуг влечёт за собой ответственность в соответствии с законодательством Российской Федерации.	ст. 4, 6 Федерального закона от 28.12.2013 № 442-ФЗ (ред. от 28.12.2022) "Об основах социального обслуживания граждан в Российской Федерации"

Тайна статистического учёта	
Сведения о населении, содержащиеся в переписных листах, являются информацией ограниченного доступа, не подлежат разглашению или распространению и используются только в целях формирования официальной статистической информации. Лица, которые имеют доступ к сведениям о населении, содержащимся в переписных листах, и допустили утрату или разглашение этих сведений либо фальсифицировали их или содействовали их фальсификации, несут ответственность в соответствии с законодательством Российской Федерации. Обязанность не разглашать информацию ограниченного доступа о населении, полученную в ходе проведения переписи населения, должна предусматриваться договорами, заключёнными с гражданами, привлечёнными к работе по проведению переписи населения, а в отношении должностных лиц - нормативными правовыми актами Правительства Российской Федерации.	ст. 8 Федерального закона от 25.01.2002 № 8-ФЗ (ред. от 24.04.2020) "О всероссийской переписи населения"
Первичные статистические данные, содержащиеся в формах федерального статистического наблюдения, являются информацией ограниченного доступа, за исключением информации, недопустимость ограничения доступа к которой установлена федеральными законами. Субъекты официального статистического учёта обязаны обеспечить конфиденциальность информации ограниченного доступа. Первичные статистические данные, являющиеся информацией ограниченного доступа, не подлежат разглашению (распространению и (или) предоставлению) и используются только в целях формирования официальной статистической информации.	ст. 9 Федерального закона от 29.11.2007 № 282-ФЗ (ред. от 28.02.2023) "Об официальном статистическом учёте и системе государственной статистики в Российской Федерации"
Содержащиеся в переписных листах сведения об объектах сельскохозяйственной переписи являются информацией ограниченного доступа, не подлежат разглашению (распространению) и используются в целях формирования соответствующих государственных информационных систем. Обязанность не разглашать сведения об объектах сельскохозяйственной переписи, являющиеся информацией ограниченного доступа и полученные в ходе проведения сельскохозяйственной переписи, должна предусматриваться	ст. 12 Федерального закона от 21.07.2005 № 108-ФЗ (ред. от 24.04.2020) "О Всероссийской сельскохозяйственной переписи"

договорами, заключаемыми с лицами, осуществляющими сбор сведений об объектах сельскохозяйственной переписи, либо в отношении должностных лиц нормативными правовыми актами Правительства Российской Федерации.	
Тайна охраны труда	
Государственные инспекторы труда обязаны хранить охраняемую законом тайну (государственную, служебную, коммерческую и иную), ставшую им известной при осуществлении ими своих полномочий, а также после оставления своей должности, считать абсолютно конфиденциальным источник всякой жалобы на недостатки или нарушения положений трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, воздерживаться от сообщения работодателю сведений о заявителе, если проверка проводится в связи с его обращением, а заявитель возражает против сообщения работодателю данных об источнике жалобы.	ст. 358 Трудового кодекса РФ от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022)
Сведения о результатах проведения специальной оценки условий труда, в том числе в отношении рабочих мест, условия труда на которых декларируются как соответствующие государственным нормативным требованиям охраны труда, подлежат передаче в информационную систему учёта, за исключением сведений, составляющих государственную или иную охраняемую законом тайну, с учётом требований законодательства Российской Федерации о персональных данных. Участники информационного взаимодействия обязаны соблюдать конфиденциальность сведений, содержащихся в информационной системе учёта, обеспечивать защиту этих сведений от несанкционированного доступа в соответствии с законодательством Российской Федерации.	ст. 18 Федерального закона от 28.12.2013 № 426-ФЗ (ред. от 28.12.2022) "О специальной оценке условий труда"
Тайна ЕГЭ	
Информация, содержащаяся в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации, относится к информации ограниченного доступа. Порядок разработки, использования и хранения контрольных измерительных материалов (включая требования к режиму их защиты, порядку и условиям размещения	ст. 59 Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 17.02.2023) "Об образовании в Российской Федерации"

информации, содержащейся в контрольных измерительных материалах, в сети "Интернет") устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере образования.	
Тайна политических партий	
Информация о членах политической партии, представляемая для сведения в уполномоченные органы, относится к информации с ограниченным доступом. Разглашение информации, указанной в настоящем пункте, без согласия соответствующих членов политической партии влечёт за собой ответственность, установленную законодательством Российской Федерации.	ст. 19 Федерального закона от 11.07.2001 № 95-ФЗ (ред. от 05.12.2022) "О политических партиях"
Ведомственная тайна	
Военнослужащие, федеральные государственные гражданские служащие, работники органов федеральной службы безопасности, а также лица, уволенные из органов федеральной службы безопасности, обязаны соблюдать конфиденциальность информации о деятельности органов федеральной службы безопасности, составляющей профессиональную тайну. К профессиональной тайне органов федеральной службы безопасности относится информация, не содержащая сведений, составляющих государственную и иную охраняемую законом тайну, разглашение (распространение) которой может создать угрозу собственной безопасности органов федеральной службы безопасности и (или) нанести ущерб их репутации.	ст. 7 Федерального закона от 03.04.1995 № 40-ФЗ (ред. от 29.12.2022) "О федеральной службе безопасности"
В интересах личной безопасности военнослужащих (сотрудников) войск национальной гвардии и членов их семей не допускается распространение в публичных выступлениях, в средствах массовой информации сведений о местах дислокации или о передислокации органов управления войсками национальной гвардии, объединений, соединений, воинских частей войск национальной гвардии, а также обеспечивается конфиденциальность сведений о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей.	ст. 23 Федерального закона от 03.07.2016 № 226-ФЗ (ред. от 06.02.2023) "О войсках национальной гвардии Российской Федерации"

В федеральном органе исполнительной власти в сфере внутренних дел, его территориальных органах, подразделениях ведутся личные дела, документы учёта сотрудников органов внутренних дел, банки данных о сотрудниках и гражданах, поступающих на службу в органы внутренних дел, содержащие персональные данные сотрудников, сведения об их служебной деятельности и стаже службы, а также персональные данные членов семей сотрудников и граждан, поступающих на службу в органы внутренних дел. Сведения, содержащиеся в личном деле и документах учёта сотрудника органов внутренних дел, являются конфиденциальной информацией (служебной тайной) и (или) сведениями, составляющими государственную и иную охраняемую законом тайну.	ст. 39, 40 Федерального закона от 30.11.2011 № 342-ФЗ (ред. от 05.12.2022) "О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации"
В федеральном органе исполнительной власти в области пожарной безопасности, подразделениях ведутся личные дела, документы учёта сотрудников федеральной противопожарной службы, банки данных о сотрудниках и гражданах, поступающих на службу в федеральную противопожарную службу, содержащие персональные данные сотрудников, сведения об их служебной деятельности и стаже службы (выслуге лет), а также персональные данные членов семей сотрудников и граждан, поступающих на службу в федеральную противопожарную службу.	ст. 39 Федерального закона от 23.05.2016 № 141-ФЗ (ред. от 29.12.2022) "О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации"
Тайна связи	
Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.	ст. 23 Конституции РФ (принятой 12.12.1993)
Тайна связи – тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств,	ст. 2, 15 Федерального закона от 17.07.1999 № 176-ФЗ (ред. от 18.03.2023) "О почтовой связи"

телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям. Должностные и иные лица, работники организаций почтовой связи, допустившие нарушения указанных положений, привлекаются к ответственности в порядке, установленном законодательством Российской Федерации.	
Сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.	ст. 53, 63 Федерального закона от 07.07.2003 № 126-ФЗ (ред. от 18.03.2023) "О связи"
Оператор связи обязан обеспечить соблюдение тайны сообщений, передаваемых по сети передачи данных. Ограничение права на тайну сообщений, передаваемых по сети передачи данных, допускается только в случаях, предусмотренных федеральными законами.	Постановление Правительства РФ от 31.12.2021 № 2606 "Об утверждении Правил оказания услуг связи по передаче данных"
Оператор связи обязан обеспечивать соблюдение тайны телеграфной связи и принимать все возможные совместимые с применяемой системой телеграфной связи меры с целью обеспечить соблюдение тайны передаваемых текстовых сообщений. Пользователям гарантируется соблюдение тайны текстовых сообщений, передаваемых по сетям телеграфной связи. Ограничение права на тайну текстовых сообщений допускается только в случаях, предусмотренных федеральными законами.	Постановление Правительства РФ от 28.05.2022 № 968 "Об утверждении Правил оказания услуг телеграфной связи"
Тайна СМИ	
Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве	ст. 41 Закона РФ от 27.12.1991 № 2124-1 (ред. от 29.12.2022) "О средствах массовой информации"

делом. Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.	
Тайна транспортной безопасности	
Порядок обращения со сведениями о результатах проведённой оценки уязвимости объектов транспортной инфраструктуры, судов ледокольного флота, используемых для проводки по морским путям, судов, в отношении которых применяются правила торгового мореплавания и требования в области охраны судов и портовых средств, установленные международными договорами Российской Федерации, а также со сведениями, содержащимися в планах и паспортах обеспечения транспортной безопасности объектов транспортной инфраструктуры и (или) транспортных средств, которые являются информацией ограниченного доступа, устанавливается Правительством Российской Федерации. Информационные ресурсы единой государственной информационной системы обеспечения транспортной безопасности являются информацией ограниченного доступа.	ст. 5, 9, 11 Федерального закона от 09.02.2007 № 16-ФЗ (ред. от 03.04.2023) "О транспортной безопасности"
Тайна энергетической безопасности	
Информация, содержащаяся в паспортах безопасности объектов топливно-энергетического комплекса, является информацией, доступ к которой ограничен в соответствии с федеральными законами.	ст. 8 Федерального закона от 21.07.2011 № 256-ФЗ (ред. от 28.06.2022) "О безопасности объектов топливно-энергетического комплекса"
Информация, в отношении которой установлено требование об обеспечении её конфиденциальности и которая получена членами саморегулируемой организации в области энергетического обследования в ходе проведения энергетического обследования, не подлежит разглашению, за исключением случаев, установленных законодательством	ст. 18 Федерального закона от 23.11.2009 № 261-ФЗ (ред. от 14.07.2022) "Об энергосбережении и о повышении энергетической

Российской Федерации.	эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации"
Тайна договора (торгов)	
Корпоративный договор заключается в письменной форме путём составления одного документа, подписанного сторонами. Информация о корпоративном договоре, заключённом акционерами публичного акционерного общества, должна быть раскрыта в пределах, в порядке и на условиях, которые предусмотрены законом об акционерных обществах. Если иное не установлено законом, информация о содержании корпоративного договора, заключённого участниками непубличного общества, не подлежит раскрытию и является конфиденциальной.	ст. 67.2 Гражданского кодекса РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.04.2023)
Если сторона благодаря исполнению своего обязательства по договору подряда получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны, сторона, получившая такую информацию, не вправе сообщать ее третьим лицам без согласия другой стороны. Порядок и условия пользования такой информацией определяются соглашением сторон.	ст. 727 Гражданского кодекса РФ (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 08.07.2021)
Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре. Каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.	ст. 771 Гражданского кодекса РФ (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 08.07.2021)

Организатор торговли обязан обеспечить конфиденциальность информации, составляющей коммерческую и иную охраняемую законом тайну, конфиденциальность сведений, предоставляемых участниками торгов в соответствии с правилами организованных торгов.	ст. 23 Федерального закона от 21.11.2011 № 325-ФЗ (ред. от 02.07.2021) "Об организованных торгах"
Оператор электронной площадки обязан обеспечить конфиденциальность информации об участниках электронного аукциона, подавших заявки на участие в таком аукционе, и информации, содержащейся в первой и второй частях данной заявки и предусмотренной частями 3-5 настоящей статьи, а также информации, содержащейся в электронных документах (их копиях), предусмотренных частью 8.2 настоящей статьи, до размещения на электронной площадке протокола проведения такого аукциона. За нарушение указанного требования оператор электронной площадки несёт ответственность в соответствии с законодательством Российской Федерации. Оператор электронной площадки обязан обеспечивать при проведении электронного аукциона конфиденциальность информации о его участниках.	ст. 66, 68 Федерального закона от 05.04.2013 № 44-ФЗ (ред. от 28.12.2022) "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"
Информация, предоставленная федеральным органам исполнительной власти, осуществляющим полномочия в области экспортного контроля, участниками внешнеэкономической деятельности в соответствии с настоящим Федеральным законом и иными нормативными правовыми актами Российской Федерации в области экспортного контроля, используется исключительно в целях экспортного контроля. Информация, составляющая государственную, коммерческую и иную охраняемую законом тайну, не должна разглашаться, использоваться должностными лицами указанных органов в личных целях, передаваться третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации. Действия должностных лиц органа государственного контроля при проведении проверок российских участников внешнеэкономической деятельности не должны причинять неправомерный ущерб лицам, деятельность которых проверяется. Полученная в ходе таких проверок информация является	ст. 15, 17 Федерального закона от 18.07.1999 № 183-ФЗ (ред. от 26.03.2022) "Об экспортном контроле"

информацией ограниченного доступа, и на неё распространяется действие статьи 15 настоящего Федерального закона	
Информация, представляемая заинтересованным лицом в орган, проводящий расследования, рассматривается в качестве конфиденциальной при представлении этим лицом обоснований, свидетельствующих о том, что раскрытие такой информации предоставит преимущество в условиях конкуренции третьему лицу либо повлечёт за собой неблагоприятные последствия для лица, представившего такую информацию, или для лица, у которого данное лицо получило такую информацию. Конфиденциальная информация не должна разглашаться без разрешения представившего её заинтересованного лица, за исключением случаев, предусмотренных федеральными законами.	ст. 32 Федерального закона от 08.12.2003 № 165-ФЗ (ред. от 08.12.2020) "О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров"
Организатор торгов обязан обеспечить конфиденциальность сведений и предложений, содержащихся в представленных заявках на участие в торгах, или предложений о цене предприятия до начала торгов либо до момента открытия доступа к представленным в форме электронных документов заявкам на участие в торгах.	ст. 110 Федерального закона от 26.10.2002 № 127-ФЗ (ред. от 28.12.2022) "О несостоятельности (банкротстве)"
Контрсанкционная информация	
Под контрсанкционной информацией понимаются сведения любого характера (производственные, технические, экономические, организационные и другие) о совершенных или планируемых к совершению российскими физическими и (или) юридическими лицами - участниками внешнеторговой деятельности сделках, осуществляемых в области внешней торговли товарами, работами, услугами, информацией и (или) интеллектуальной собственностью в целях обеспечения потребностей внутреннего рынка Российской Федерации, распространение которых может повлечь за собой введение в отношении сторон таких сделок иностранными государствами, государственными объединениями, союзами и (или) международными организациями, совершающими недружественные и противоречащие международному праву действия в отношении Российской Федерации, российских юридических лиц и граждан Российской Федерации, мер ограничительного характера.	ст. 21.4 Федеральный закон от 08.03.2022 № 46-ФЗ (ред. от 03.04.2023) "О внесении изменений в отдельные законодательные акты Российской Федерации"

Тайна лотерей	
Участники размещения заказа, подавшие заявки на участие в конкурсе, организатор лотереи обязаны обеспечить конфиденциальность сведений, содержащихся в таких заявках до вскрытия конвертов с заявками на участие в конкурсе и открытия доступа к поданным в форме электронных документов заявкам на участие в конкурсе. Лица, осуществляющие хранение конвертов с заявками на участие в конкурсе и заявок на участие в конкурсе, поданных в форме электронных документов, не вправе допускать повреждение таких конвертов и заявок до момента их вскрытия в соответствии со статьёй 24.11 настоящего Федерального закона.	ст. 24.10 Федерального закона от 11.11.2003 № 138-ФЗ (ред. от 02.07.2021) "О лотереях"
Тайна следствия	
Данные предварительного расследования не подлежат разглашению. Данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя или дознавателя и только в том объёме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав, свобод и законных интересов участников уголовного судопроизводства.	ст. 161 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)
Подозреваемый в кратчайший срок, но не позднее 3 часов с момента его доставления в орган дознания или к следователю имеет право на один телефонный разговор на русском языке в присутствии дознавателя, следователя в целях уведомления близких родственников, родственников или близких лиц о своём задержании и месте нахождения, о чем делается отметка в протоколе задержания. При необходимости сохранения в интересах предварительного расследования в тайне факта задержания уведомление по мотивированному постановлению дознавателя, следователя с согласия прокурора может не производиться, за исключением случаев, если подозреваемый является несовершеннолетним.	ст. 96 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)

Отдельные лица могут с их согласия привлекаться к подготовке или проведению оперативно-розыскных мероприятий с сохранением по их желанию конфиденциальности содействия органам, осуществляющим оперативно-розыскную деятельность, в том числе по контракту. Эти лица обязаны сохранять в тайне сведения, ставшие им известными в ходе подготовки или проведения оперативно-розыскных мероприятий, и не вправе предоставлять заведомо ложную информацию указанным органам.	ст. 17 Федерального закона от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) "Об оперативно-розыскной деятельности"
Член общественной наблюдательной комиссии не вправе разглашать данные предварительного расследования, ставшие ему известными при осуществлении своих полномочий, за исключением случаев, предусмотренных уголовно-процессуальным законодательством Российской Федерации. Лицо, производящее дознание, или следователь в необходимых случаях предупреждает члена общественной наблюдательной комиссии о недопустимости разглашения данных предварительного расследования, ставших ему известными при осуществлении своих полномочий, о чем у члена общественной наблюдательной комиссии берётся подписка о предупреждении об уголовной ответственности в соответствии со статьёй 310 Уголовного кодекса Российской Федерации.	ст. 20 Федерального закона от 10.06.2008 № 76-ФЗ (ред. от 05.12.2022) "Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания"
Органы и учреждения системы профилактики безнадзорности и правонарушений несовершеннолетних в пределах своей компетенции обязаны обеспечивать соблюдение прав и законных интересов несовершеннолетних, осуществлять их защиту от всех форм дискриминации, физического или психического насилия, оскорбления, грубого обращения, сексуальной и иной эксплуатации, выявлять несовершеннолетних и семьи, находящиеся в социально опасном положении. Информация, указанная в пункте 2 настоящей статьи, подлежит хранению и использованию в порядке, обеспечивающем её конфиденциальность.	ст. 9 Федерального закона от 24.06.1999 № 120-ФЗ (ред. от 21.11.2022) "Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних"
При наличии угрозы посягательства на жизнь, здоровье и имущество защищаемых лиц органом, обеспечивающим безопасность, налагается временный запрет на выдачу находящихся у оператора сведений о личности защищаемых лиц и об их имуществе (о персональных данных), за исключением случаев, если такие сведения выясняются в	ст. 9 Федерального закона от 20.04.1995 № 45-ФЗ (ред. от 01.07.2021) "О государственной защите судей, должностных лиц

установленном порядке в связи с производством по уголовному делу. Обеспечение конфиденциальности сведений о защищаемых лицах и об их имуществе осуществляется оператором на основании решения органа, обеспечивающего безопасность, в порядке, установленном Правительством Российской Федерации.	правоохранительных и контролирующих органов"
Тайна судопроизводства	
Судьи не вправе разглашать суждения, имевшие место при обсуждении и постановлении приговора, или иным способом раскрывать тайну совещания судей.	ст. 298 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)
Присяжные заседатели не могут разглашать суждения, имевшие место во время совещания.	ст. 341 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)
Совещание судей происходит в порядке, предусмотренном статьёй 15 настоящего Кодекса. Судьи не могут разглашать суждения, высказывавшиеся во время совещания.	ст. 194 Гражданского процессуального кодекса РФ от 14.11.2002 № 138-ФЗ (ред. от 18.03.2023)
При изложении своего особого мнения судья не вправе сообщать кому бы то ни было сведения о содержании обсуждения при принятии судебного акта, о позиции отдельных судей, входивших в состав суда, и иным способом раскрывать тайну совещания судей.	ст. 20 Арбитражного процессуального кодекса РФ от 24.07.2002 № 95-ФЗ (ред. от 18.03.2023)
Судьи не могут разглашать сведения, которые имели место при обсуждении и принятии решения, и иным способом раскрывать тайну совещания судей. При этом изложение судьёй особого мнения в порядке, предусмотренном статьёй 30 настоящего Кодекса, не может рассматриваться как нарушение тайны совещания судей.	ст. 175 Кодекса административного судопроизводства РФ от 08.03.2015 № 21-ФЗ (ред. от 17.02.2023)

Эксперт не вправе самостоятельно собирать материалы для проведения экспертизы, вступать в личные контакты с участниками судебного процесса, если это ставит под сомнение его незаинтересованность в исходе административного дела, а также разглашать сведения, которые стали ему известны в связи с проведением экспертизы, или сообщать о результатах экспертизы кому-либо, за исключением суда, её назначившего.	ст. 49 Кодекса административного судопроизводства РФ от 08.03.2015 № 21-ФЗ (ред. от 17.02.2023)
По решению органа, осуществляющего меры безопасности, может быть наложен запрет на распространение информации, содержащей сведения о защищаемом лице (персональные данные), выдачу находящихся у оператора сведений о защищаемом лице (персональных данных), также могут быть заменены абонентские номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств. В исключительных случаях, связанных с производством по другому уголовному, гражданскому либо административному делу, сведения о защищаемом лице могут быть представлены в органы предварительного расследования, прокуратуру или суд на основании письменного запроса прокурора или суда (судьи) с разрешения органа, принявшего решение об осуществлении государственной защиты. Порядок осуществления мер безопасности в виде обеспечения конфиденциальности сведений о защищаемом лице устанавливается Правительством Российской Федерации.	ст. 9 Федерального закона от 20.08.2004 № 119-ФЗ (ред. от 01.07.2021) "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства"
Сотрудники органов принудительного исполнения обязаны хранить государственную и иную охраняемую законом тайну, а также не разглашать ставшие им известными в связи с исполнением должностных обязанностей сведения, затрагивающие частную жизнь, честь и достоинство граждан, другую конфиденциальную информацию.	ст. 6.4 Федерального закона от 21.07.1997 № 118-ФЗ (ред. от 21.12.2021) "Об органах принудительного исполнения Российской Федерации"
Если стороны не договорились об ином или иное не предусмотрено федеральным законом, арбитраж является конфиденциальным, а слушание дела проводится в закрытом заседании. Арбитры, сотрудники постоянно действующего арбитражного учреждения не вправе разглашать сведения, ставшие им известными в ходе арбитража, без согласия сторон. Арбитр не подлежит допросу в качестве свидетеля о сведениях, ставших ему известными в ходе арбитража.	ст. 21 Федерального закона от 29.12.2015 № 382-ФЗ (ред. от 27.12.2018) "Об арбитраже (третейском разбирательстве) в Российской Федерации"

При проведении процедуры медиации сохраняется конфиденциальность всей относящейся к указанной процедуре информации, за исключением случаев, предусмотренных федеральными законами, и случаев, если стороны не договорились об ином. Медиатор не вправе разглашать информацию, относящуюся к процедуре медиации и ставшую ему известной при её проведении, без согласия сторон.	ст. 5 Федерального закона от 27.07.2010 № 193-ФЗ (ред. от 26.07.2019) "Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)"
IV. Информация о частной жизни гражданина (физического лица), в том числе составляющая личную или семейную тайну (персональные данные)	
Жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, неприкосновенность жилища, личная и семейная тайна, свобода передвижения, свобода выбора места пребывания и жительства, имя гражданина, авторство, иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом.	ст. 150 Гражданского кодекса РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.04.2023)
В случае нарушения личных неимущественных прав автора их защита осуществляется, в частности, путём признания права, восстановления положения, существовавшего до нарушения права, пресечения действий, нарушающих право или создающих угрозу его нарушения, компенсации морального вреда, публикации решения суда о допущенном нарушении.	ст. 1251 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022)
Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.	ст. 23, 24 Конституции РФ (принятой 12.12.1993)

Если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни. Стороны обязательства не вправе разглашать ставшую известной им при возникновении и (или) исполнении обязательства информацию о частной жизни гражданина, являющегося стороной или третьим лицом в данном обязательстве, если соглашением не предусмотрена возможность такого разглашения информации о сторонах.	ст. 152.2 Гражданского кодекса РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.04.2023)
Доступ к архивным документам может быть ограничен в соответствии с международным договором Российской Федерации, законодательством Российской Федерации, а также в соответствии с распоряжением собственника или владельца архивных документов, находящихся в частной собственности. Ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов.	ст. 25 Федерального закона от 22.10.2004 № 125-ФЗ (ред. от 28.12.2022) "Об архивном деле в Российской Федерации"
Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных). Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.	ст. 3, 7 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) "О персональных данных"
Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображён) допускаются только с согласия этого гражданина.	ст. 152.1 Гражданского кодекса РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.04.2023)
Условия хранения и использования дактилоскопической информации должны исключать возможность её утраты, искажения и несанкционированного доступа к ней. Хранение, систематизация и использование дактилоскопической информации осуществляются органами внутренних дел. Государственные органы обязаны соблюдать конфиденциальность	ст. 12 Федерального закона от 25.07.1998 № 128-ФЗ (ред. от 14.07.2022) "О государственной дактилоскопической регистрации

дактилоскопической информации и обеспечивать её безопасность. Должностные лица государственных органов несут предусмотренную законодательством Российской Федерации ответственность за нарушение законодательства Российской Федерации в области персональных данных.	в Российской Федерации"
Сведения о доходах, об имуществе и обязательствах имущественного характера, представляемые гражданским служащим в соответствии с настоящей статьёй, являются сведениями конфиденциального характера, если федеральным законом они не отнесены к сведениям, составляющим государственную тайну.	ст. 20 Федерального закона от 27.07.2004 № 79-ФЗ (ред. от 29.12.2022) "О государственной гражданской службе Российской Федерации"
Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, представляемые муниципальным служащим в соответствии с настоящей статьёй, являются сведениями конфиденциального характера, если федеральными законами они не отнесены к сведениям, составляющим государственную и иную охраняемую федеральными законами тайну.	ст. 15 Федерального закона от 02.03.2007 № 25-ФЗ (ред. от 28.12.2022) "О муниципальной службе в Российской Федерации"
Сведения о доходах, об имуществе и обязательствах имущественного характера относятся к информации ограниченного доступа. Не допускается использование сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых гражданином, служащим или работником, для установления либо определения его платёжеспособности и платёжеспособности его супруги (супруга) и несовершеннолетних детей, для сбора в прямой или косвенной форме пожертвований (взносов) в фонды общественных объединений либо религиозных или иных организаций, а также в пользу физических лиц. Лица, виновные в разглашении сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых гражданином, служащим или работником либо в использовании этих сведений в целях, не предусмотренных федеральными законами, несут ответственность в соответствии с законодательством Российской Федерации.	ст. 8 Федерального закона от 25.12.2008 № 273-ФЗ (ред. от 18.03.2023) "О противодействии коррупции"

Лицо, замещающее (занимающее) одну из должностей, обязано ежегодно в сроки, установленные для представления сведений о доходах, об имуществе и обязательствах имущественного характера, представлять сведения о своих расходах, а также о расходах своих супруги (супруга) и несовершеннолетних детей по каждой сделке по приобретению земельного участка, другого объекта недвижимости, транспортного средства, ценных бумаг, акций (долей участия, паёв в уставных (складочных) капиталах организаций), цифровых финансовых активов, цифровой валюты, совершенной им, его супругой (супругом) и (или) несовершеннолетними детьми в течение календарного года, предшествующего году представления сведений, если общая сумма таких сделок превышает общий доход данного лица и его супруги (супруга) за три последних года, предшествующих отчётному периоду, и об источниках получения средств, за счёт которых совершены эти сделки. Сведения представленные в соответствии с настоящим Федеральным законом, относятся к информации ограниченного доступа. Если федеральным законом такие сведения отнесены к сведениям, составляющим государственную тайну, они подлежат защите в соответствии с законодательством Российской Федерации о государственной тайне.	ст. 2, 4, 8 Федерального закона от 03.12.2012 № 230-ФЗ (ред. от 18.03.2023) "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам"

Приложение 2

ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Действующая редакция нормативного правового акта	**Предлагаемое изменение (дополнение) в нормативный правовой акт**
Закон РФ от 21.07.1993 № 5485-1 (ред. от 05.12.2022) "О государственной тайне"	
Статья 5. Перечень сведений, составляющих государственную тайну Государственную тайну составляют: 2) сведения в области экономики, науки и техники: о содержании планов подготовки Российской Федерации и её отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объёмах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов; об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства; о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищённости объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях	**после** об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства; **дополнить** об информации, содержащейся в "Единой информационной системе персональных данных Российской Федерации"; об информации, содержащейся в "Федеральной базе данных геномной информации";

обеспечения безопасности государства; об объёмах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции; о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства; о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объёмах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);	
Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться: права выезда за границу на срок, оговорённый в трудовом договоре (контракте) при оформлении допуска гражданина к государственной	**после** права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

тайне; права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.	**дополнить** права на размещение общедоступной информации, а также данных, позволяющих идентифицировать должностное лицо или гражданина, на сайтах и (или) страницах сайтов в информационно-коммуникационной сети "Интернет";
Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации"	
Статья 2. Основные понятия, используемые в настоящем Федеральном законе В настоящем Федеральном законе используются следующие основные понятия: 7) конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;	**изложить в следующей редакции** 7) режим конфиденциальности информации – установленный правовой режим ограничения доступа к информации, предусматривающий ограничение на предоставление указанной информации третьим лицам без письменного согласия правообладателя, а также запрет на распространение указанной информации каким либо способом, если иное не установлено федеральным законом;
Статья 9. Ограничение доступа к информации 1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. 2. Обязательным является соблюдение конфиденциальности	**дополнить** 1.1. К информации, доступ к которой ограничен федеральными законами, относится: а) информация, составляющая государственную тайну; б) информация, составляющая коммерческую тайну,

информации, доступ к которой ограничен федеральными законами. 2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. 3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. 4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за её разглашение. 5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. 6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.	служебную тайну и иную тайну; в) информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна); г) информация о частной жизни гражданина (физического лица), в том числе составляющая личную и семейную тайну (персональные данные). **исключить** 7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе. 8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами. 9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.	
Статья 14. Государственные информационные системы 1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. 3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления. 4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия её предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании	**дополнить** 3.1. При обработке информации, доступ к которой ограничен федеральными законами, указанный в части 1.1. статьи 9 настоящего федерального закона, кроме информации, составляющей государственную тайну, относится к государственной информации.

или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьёй 14 Федерального закона от 9 февраля 2009 года № 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", государственные информационные системы должны обеспечивать размещение такой информации в сети "Интернет" в форме открытых данных.	
Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) "О персональных данных"	
Статья 1. Сфера действия настоящего Федерального закона 2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при: 1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных; 2) организации хранения, комплектования, учёта и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации; 4) обработке персональных данных, отнесённых в установленном порядке к сведениям, составляющим государственную тайну;	**исключить** 4) обработке персональных данных, отнесённых в установленном порядке к сведениям, составляющим государственную тайну;

Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 29.12.2022) "Об основах охраны здоровья граждан в Российской Федерации"	
Статья 94. Сведения о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования В системе персонифицированного учёта осуществляется обработка следующих персональных данных о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования: 1) фамилия, имя, отчество (последнее - при наличии); 2) пол; 3) дата рождения; 4) место рождения; 5) гражданство; 6) данные документа, удостоверяющего личность; 7) место жительства; 8) место регистрации; 9) дата регистрации; 10) страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования; 11) номер полиса обязательного медицинского страхования застрахованного лица (при наличии);	**изложить в следующей редакции** 21) сведения о проведённых медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты, в том числе и наличие медицинских противопоказаний, медицинских показаний и медицинских ограничений к управлению транспортным средством, для работы с использованием сведений, составляющих государственную тайну;

12) анамнез; 13) диагноз; 14) сведения об организации, осуществляющей медицинскую деятельность; 15) вид оказанной медицинской помощи; 16) условия оказания медицинской помощи; 17) сроки оказания медицинской помощи; 18) объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах; 19) результат обращения за медицинской помощью; 20) серия и номер выданного листка нетрудоспособности (при наличии); 21) сведения о проведённых медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты; 22) применённые стандарты медицинской помощи; 23) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь, проводивших медицинские экспертизы, медицинские осмотры и медицинские освидетельствования.	
Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
Статья 2. Основные понятия, используемые в настоящем Федеральном законе Для целей настоящего Федерального закона используются следующие основные понятия: 8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские	**изложить в следующей редакции** 8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные

юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.	предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, обработки биометрической и геномной информации, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горно-добывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей, а также государственные информационные системы, в которых обрабатываются персональные данные всех граждан Российской Федерации;
Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 29.10.2022) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"	
В соответствии с Законом Российской Федерации "О государственной тайне" Правительство Российской Федерации постановляет: 3. Предоставить Федеральной службе безопасности Российской Федерации право давать государственным органам, органам местного	**пункт 3 – отменить**

самоуправления и организациям разъяснения по вопросам применения Инструкции, утверждённой настоящим Постановлением.	
"Инструкция о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне", утверждённой Постановлением Правительства РФ от 06.02.2010 № 63 (ред. от 29.10.2022)	
15. Допуск гражданина к государственной тайне может быть прекращён по решению должностного лица, уполномоченного на принятие решения о допуске гражданина к государственной тайне, в случае: а) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий; б) однократного нарушения им обязательств, связанных с защитой государственной тайны; в) возникновения обстоятельств, являющихся в соответствии с пунктом 12 настоящей Инструкции основанием для отказа гражданину в допуске к государственной тайне.	**изложить в следующей редакции** 15. Допуск гражданина к государственной тайне может быть прекращён по решению должностного лица, уполномоченного на принятие решения о допуске гражданина к государственной тайне, в случае: **а) – отменить** б) однократного нарушения им обязательств, связанных с защитой государственной тайны; в) возникновения обстоятельств, являющихся в соответствии с пунктом 12 настоящей Инструкции основанием для отказа гражданину в допуске к государственной тайне. **дополнить** 15.1. Допуск гражданина к государственной тайне без проведения проверочных мероприятий может быть прекращён по решению должностного лица, принявшего решение о его допуске к государственной тайне, в случае расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий.

28. Граждане, которым оформляется допуск к государственной тайне, представляют собственноручно заполненную анкету (форма 4), документы, удостоверяющие личность и подтверждающие сведения, указанные в анкете (паспорт, военный билет, трудовую книжку и (или) сведения о трудовой деятельности, предусмотренные статьёй 66.1 Трудового кодекса Российской Федерации, свидетельство о рождении, свидетельство о заключении (расторжении) брака, диплом об образовании и т.п.), а также справку об отсутствии медицинских противопоказаний для работы со сведениями, составляющими государственную тайну. Форму и порядок получения справки устанавливает федеральный орган исполнительной власти, уполномоченный в области здравоохранения и социального развития.	**дополнить** 28.1. Граждане, которым оформляется допуск к государственной тайне, регистрируются в единой системе идентификации и аутентификации и предоставляют согласие на обработку биометрической информации в автоматизированной информационной системе Федеральной службы безопасности Российской Федерации".
44. В отношении граждан, которые переведены на должности, не предусматривающие наличие допуска к государственной тайне, уволились из организации, в том числе при расторжении трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий, закончили обучение в учебном заведении и т.п. и на которых в течение 6 месяцев не затребованы карточки (форма 1), действие допуска прекращается.	**изложить в следующей редакции** 44. В отношении граждан, которые переведены на постоянную работу к другому работодателю, уволились из организации, в том числе при расторжении трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий, закончили обучение в учебном заведении и т.п. и на которых в течение 6 месяцев не затребованы карточки (форма 1), действие допуска прекращается не позднее даты расторжения трудового договора (контракта).

45. Решение о прекращении допуска гражданина к государственной тайне оформляется записью в позиции 8 карточки (форма 1), которая заверяется подписью соответствующего должностного лица и печатью организации (при наличии печати).	**отменить и дополнить** 46.1. Решение о прекращении допуска гражданина к государственной тайне оформляется записью в позиции 8 карточки (форма 1) датой принятия соответствующего решения, но не позднее даты расторжения трудового договора (контракта), которая заверяется подписью соответствующего должностного лица и печатью организации (при наличии печати).
60. Переоформление допуска к государственной тайне по первой форме производится через 10 лет, по второй и третьей (с проведением органами безопасности проверочных мероприятий) формам производится через 15 лет с даты окончания проведения проверочных мероприятий органами безопасности в случае перехода указанных граждан на другое место работы (службы). Переоформление допуска к государственной тайне граждан, постоянно работающих в организации, оформившей им данный допуск, не производится.	**изложить в следующей редакции** 60. Переоформление допуска к государственной тайне по первой форме производится через 10 лет, по второй и третьей (с проведением органами безопасности проверочных мероприятий) формам производится через 15 лет с даты окончания проведения проверочных мероприятий органами безопасности в случае перехода указанных граждан на другое место работы (службы) и изменения развёрнутого перечня сведений, подлежащих засекречиванию.

"Положение о единой государственной информационной системе в сфере здравоохранения", утверждённым Постановлением Правительства РФ от 09.02.2022 № 140 (ред. от 30.11.2022) "О единой государственной информационной системе в сфере здравоохранения"	
II. Структура и порядок ведения единой системы 4. Единая система включает в себя следующие подсистемы: а) федеральный регистр медицинских и фармацевтических работников; б) федеральный реестр медицинских и фармацевтических организаций; в) федеральная электронная регистратура; г) федеральная интегрированная электронная медицинская карта; д) федеральный реестр электронных медицинских документов; е) подсистема ведения специализированных регистров пациентов по отдельным нозологиям и категориям граждан, мониторинга организации оказания специализированной, в том числе высокотехнологичной, медицинской помощи и санаторно-курортного лечения; ж) подсистема ведения реестров лекарственных препаратов для медицинского применения; з) информационно-аналитическая подсистема мониторинга и контроля в сфере закупок лекарственных препаратов для обеспечения государственных и муниципальных нужд; и) подсистема автоматизированного сбора информации о показателях системы здравоохранения из различных источников и представления отчётности; к) федеральный реестр нормативно-справочной информации в сфере здравоохранения;	**дополнить** г.1) федеральный реестр граждан Российской Федерации, получивших заключение об отсутствии медицинских противопоказаний на работу с государственной тайной; г.2) федеральный реестр иностранцев и лиц без гражданства, получивших заключение об отсутствии медицинских противопоказаний на работу с государственной тайной;

л) подсистема обезличивания персональных данных; м) геоинформационная подсистема; н) подсистема защиты информации; о) подсистема обеспечения отраслевого ситуационного центра в сфере здравоохранения; п) интеграционные подсистемы; р) иные подсистемы в случаях, предусмотренных законодательством Российской Федерации.	
VIII. Порядок обмена информацией с использованием единой системы 56. Единая система взаимодействует со следующими информационными системами: государственная информационная система в сфере обязательного медицинского страхования; автоматизированная информационная система Федеральной налоговой службы "Налог-3"; федеральная государственная информационная система "Федеральный реестр инвалидов"; федеральная государственная информационная система "Единая автоматизированная вертикально-интегрированная информационно-аналитическая система по проведению медико-социальной экспертизы"; федеральная государственная информационная система "Единая интегрированная информационная система "Соцстрах" Фонда социального страхования Российской Федерации; информационные системы Федерального медико-биологического агентства, в том числе единая ведомственная медицинская	**после** информационная система Федеральной службы по надзору в сфере здравоохранения; **дополнить** автоматизированная информационная система Федеральной службы безопасности Российской Федерации";

информационно-аналитическая система, единая база данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и её компонентов, развитием, организацией и пропагандой донорства крови и её компонентов; федеральная государственная информационная система ведения Единого государственного реестра записей актов гражданского состояния; государственный реестр медицинских изделий и организаций (индивидуальных предпринимателей), осуществляющих производство и изготовление медицинских изделий; государственная информационная система миграционного учёта; единый портал государственных и муниципальных услуг; единая информационная система в сфере закупок; информационная система Федеральной службы по надзору в сфере здравоохранения; сводный реестр лицензий на осуществление медицинской и фармацевтической деятельности; единая система межведомственного электронного взаимодействия; единая система идентификации и аутентификации; государственные информационные системы в сфере здравоохранения субъектов Российской Федерации; медицинские информационные системы медицинских организаций государственной, муниципальной и частной систем здравоохранения; информационные системы фармацевтических организаций; система мониторинга движения лекарственных препаратов для медицинского применения; государственная информационная система, оператором которой	

является федеральный орган исполнительной власти, уполномоченный в сфере оборота оружия; официальный сайт для размещения информации о государственных и муниципальных учреждениях; федеральная государственная информационная система территориального планирования; федеральная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приёма граждан в образовательные организации для получения среднего профессионального и высшего образования; информационные системы, указанные в части 5 статьи 91 Федерального закона и использующие данные, обрабатываемые в единой системе, и (или) представляющие такие данные в единую систему, в том числе для предоставления гражданам услуг в сфере здравоохранения в электронной форме; Федеральный регистр лиц, имеющих право на получение государственной социальной помощи; Единая государственная информационная система социального обеспечения; федеральная государственная информационная система сведений санитарно-эпидемиологического характера; федеральная информационная система "Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении"; единая государственная система предупреждения и ликвидации чрезвычайных ситуаций;	

федеральная государственная информационная система "Единая система нормативной справочной информации"; иные информационные системы, взаимодействие с которыми предусмотрено нормативными правовыми актами, с соблюдением требований, установленных законодательством Российской Федерации в области персональных данных, и соблюдением врачебной тайны.	
"Перечень вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные медицинские осмотры при поступлении на работу и периодические медицинские осмотры" (утверждён Приказом Минтруда России № 988н, Минздрава России № 1420н от 31.12.2020)	
VI. Выполняемые работы 6. Работы на высоте: … 7. Работа лифтёра … 8. Работа в качестве крановщика … 9. Работы, связанные с техническим обслуживанием электроустановок … 10. Работы по валке, сплаву, транспортировке, первичной обработке, охране и восстановлению лесов. 11. Работы в особых географических регионах с местами проведения работ, транспортная доступность которых от медицинских учреждений, оказывающих специализированную медицинскую помощь в экстренной форме, превышает 60 минут … 12. Работы, непосредственно связанные с обслуживанием оборудования, работающего под избыточным давлением … 13. Работы, непосредственно связанные с применением легковоспламеняющихся и взрывчатых материалов, работы во взрыво- и пожароопасных производствах, работы на коксовой батарее на открытых производственных зонах.	**дополнить** 23. Работа с государственной и иной охраняемой законом тайной.

14. Работы, выполняемые аварийно-спасательной службой, аварийно-спасательными формированиями, спасателями, а также работы, выполняемые пожарной охраной при тушении пожаров. 15. Работы, выполняемые непосредственно на механическом оборудовании, имеющем открытые движущиеся (вращающиеся) элементы конструкции, в случае если конструкцией оборудования не предусмотрена защита (ограждение) этих элементов (в том числе токарные, фрезерные и другие станки, штамповочные прессы). 16. Подземные работы, включая работы на рудниках. 17. Работы, выполняемые непосредственно с применением средств индивидуальной защиты органов дыхания изолирующих и средств индивидуальной защиты органов дыхания фильтрующих с полной лицевой частью. 18. Управление наземными транспортными средствами … 19. Водолазные работы … 20. Работы по оказанию медицинской помощи внутри барокамеры при проведении лечебной рекомпрессии или гипербарической оксигенации. 21. Кессонные работы, работы в барокамерах и других устройствах в условиях повышенного давления воздушной и газовой среды (за исключением работ, указанных в пунктах 19 и 20). 22. Работы, при выполнении которых разрешено ношение оружия и его применение …	