Фазулжанова Фатима Маратовна
магистрант
Научный руководитель
Землин Александр Игоревич
заслуженный деятель науки Российской Федерации,
д-р юрид. наук, профессор, заведующий кафедрой

ФГБОУ ВО «Российский государственный
социальный университет»
г. Москва

ПРАВОВОЕ РЕГУЛИРОВАНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВЫХ СЕРВИСАХ

Аннотация: *на основе критического осмысления аналитических документов и научных публикаций исследованы источники российского и международного права, демонстрирующие механизм реализации государственной политики в области информационной безопасности -защиты персональных данных, результаты которого свидетельствуют о необходимости регулирования безопасности в сфере цифровых сервисов. Предметом исследования выступили подходы к обеспечению информационной безопасности и предупреждения утечек персональных данных в рамках влияния цифровизации на жизнь общества, негативные и позитивные свойства внедрения новых информационных технологий в социум, их правовое регулирование, ровно как, и развитие этой отрасли в будущем. Сделан вывод о необходимости изменения подхода государственного контроля, направленного на улучшение правового обеспечения безопасности персональных данных граждан в Российской Федерации.*

Ключевые слова: *персональные данные, информационная безопасность, киберугрозы, цифровые сервисы.*

Введение

На настоящий момент времени острым вопросом в рамках обеспечения защиты информации для государственной политики информационной безопасности Российской Федерации выступает правовое регулирование безопасности персональных данных. Данный тезис обусловлен тем, что информационная сфера как определяющий фактор общественной жизни, оказывает значительное влияние на состояние политической, экономической, оборонной и иных сфер, составляющих безопасность Российской Федерации, где за последние несколько лет в качестве неотъемлемой составляющей упомянутой области стали цифровые сервисы, определяющие не только взаимодействие внутри гражданского общества, так и общества с государством. В рамках указанных цифровых сервисов значительно упрощается взаимодействие граждан в процессе разрешения задач и сопутствующей коммуникации, включая, но не ограничиваясь государственными органами, однако существенно возрастает риск утечки персональных данных. Таким образом, в эпоху цифровизации правовая защита личной информации становится критически важным прямо взаимовлияющим элементом обеспечения не только информационной, но и национальной безопасности Российской Федерации, значимость которого в ходе технического прогресса будет только возрастать.

Актуальность работы обусловлена ростом количества утечек персональных данных и совершенных в связи с этим преступлений в информационной среде. Агрегированные статистические сведения экспертно-аналитического центра свидетельствуют о том, за 2024 год среди проанализированных стран на международной арене Российская Федерация (далее «РФ») заняла второе место по числу инцидентов, где 8,5% всех случаев компрометации данных соотнесены к организациям в РФ [6]. Кроме того, статистические данные МВД РФ о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий за январь-июль 2025 года свидетельствуют о том, что «их количество возросло на 38,9%, чем за аналогичный период предыдущего года и составило 424,9 тыс. преступлений, то есть одну вторую от общего числа зареги-

стрированных преступлений, где превалирующая часть совершенных преступлений относится к категории тяжких и особо тяжких [7]. Отраженная выше динамика устойчивого роста преступности в информационной среде определяет не только высокую степень ее общественной опасности, но и необходимость создания и применения современных мер по борьбе с ней, а также, что еще немаловажно – комплекс мер по борьбе с хищением данных, включая государственный контроль со стороны исполнительных органов власти РФ.

Методология

Методологической основой исследования является комплекс научных методов познания, таких как системный, статистический, исторический, правовой, сравнительно-правовой, логический, диалектический, формально-юридический подход, историко-правовой анализ и другие методы исследования. Автором были исследованы материалы и источники различной научной литературы по предлагаемой теме, проанализированы нормативно-правовые акты Российской Федерации, в том числе основные положения Федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите информации» РФ, Федерального закона №152-ФЗ «О персональных данных» (далее «Закон 152»), Федерального закона №390-ФЗ «О безопасности», Указа Президента РФ №400 «О Стратегии национальной безопасности Российской Федерации», Доктрины информационной безопасности Российской Федерации, которые позволили более детально изучить вопрос механизма реализации правового обеспечения противодействия информационных угроз и киберпреступности, а также обозначить проблемы, возникающие в сфере реализации информационной безопасности в цифровых сервисах в век цифровых технологий.

Основная часть

Утвержденная Указом Президента РФ Доктрина информационной безопасности Российской Федерации №646, является фундаментальным документом для организации государственной политики, развития общественных отношений и применению мер по совершенствованию системы обеспечения информационной

безопасности, где информационная безопасность интерпретируется как состояние защищенности ее национальных интересов в информационной сфере, обуславливающихся комплексом из сбалансированных интересов личности, общества и государства.

Многочисленные вариации толкования понятия «информационная безопасность» приводятся в современных научных произведениях, где можно акцентировать внимание на трех существенно отличающихся подходах к представлению его сущности. «В первом случае информационная безопасность воспринимается в качестве набора из цепи мероприятий в области защиты информации и средств ее передачи, хранения, обработки и накопления» [5, с. 534]. Далее, во втором – как обеспечение защиты от разноплановых информационных воздействий либо как совокупность принятых мер в компетенции по сопротивлению акциям информационной войны Совокупность проблем информационной безопасности в третьем случае охватывает, чуть ли не полностью всю область жизнедеятельности личности, общества и государства, непосредственно сопряженную с такими процессами, как производство, преобразование, потребление, накопление и хранение информации, где не имеют значения применяемые способы и средства для реализации упомянутых процессов [4, с. 5]. Однако, характерная особенность развития правового обеспечения информационной безопасности, напрямую относится к реализации государственной политики в этой области.

Килячков А.А. и Чалдаева Л.А. четко определили, что многообразие сфер общественного уклада общества и государства совместно с общими методами защиты интересов России и ее информационного пространства, опирающимися на то, что информационная безопасность – весомый элемент национальной безопасности страны, указывает на необходимость ориентироваться на особенности данных сфер и применять частные методы [2, с. 8]. Безусловно в глобальной системе информационной безопасности государства правовой институт защиты персональных данных представлен в качестве принципиально важного элемента, в отношении которого за последние два года было введено большое количество изменений в части правового и технического регулирования.

Говоря о связи между понятиями «персональные данные» и «цифровые сервисы», следует отметить то, что последние обрабатывают персональные данные граждан в соответствии с Законом 152, когда как сами персональные данные определяются как «любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу». Однако особенности цифровых платформ, такие как масштаб и автоматизация, выходят за рамки традиционной защиты данных, что в определенных случаях создает правовую неопределенность и требует уточнения. В частности, персональные данные, используемые на таких сервисах, могут включать не только паспортные данные, ИНН, СНИЛС, дату рождения, ФИО, номер телефона, банковские карты и информацию о трудовой деятельности, место жительства, но и метрические данные, иначе определяемые как cookie-файлы, которые на текущий момент времени утверждаются в качестве персональных данных со стороны судов и Роскомнадзора.

Тем не менее, в области обеспечения конфиденциальности и защиты персональных данных существует множество проблем, которые в значительной степени обусловлены недостаточной эффективностью технических средств, предназначенных для обнаружения и предотвращения несанкционированного доступа к информации, что соответственно приводит к утечкам данных, хакерским атакам и кражам личной информации, в том числе денежных средств посредством социальной инженерии, основанной на полученных сведениях о потенциальной жертве со стороны мошенников, создавая тем самым серьезные негативные последствия как для пользователей, так и для организаций. В то же время в некоторых секторах технологических разработок наблюдаются примеры, когда современные технологии могут значительно способствовать защите информации и обеспечению конфиденциальности персональных данных. В частности, носимые устройства, такие как фитнес-браслеты, применяются не только для мониторинга физической активности, геолокации, но и для идентификации пользователей и управления доступом к личной информации. В контексте анализа инструментов для поиска оперативно значимой информации в открытых источниках, Л.Д. Матросова отмечает, что «на главной странице профиля можно получить сведения о

регионе и населенном пункте проживания исследуемого лица, а также о группах, к которым оно принадлежит. Среди этих групп могут быть специализированные сообщества, предоставляющие более глубокое понимание целей и интересов индивидуума, позволяющие сформировать достаточно полное представление о личности» [3, с. 66]. Нельзя не утверждать, что вышеизложенные тезисы в том числе приоткрывают преступникам потенциальные вариации осуществления мошеннических действий на основании этих данных.

Дополнительно в рамках рассматриваемой проблематики правового регулирования безопасности персональных данных в цифровых сервисах нельзя не отметить факт скорости прогресса технологий над процессом издания регулирующих нормативно-правовых актов и их реализации. Таким образом, разработка законодательства, касающегося новых технологий, представляет собой сложную и многогранную задачу, требующую глубокого анализа и системного подхода. Сложность применения законодательства о персональных данных также вызывает значительные трудности, обусловленные его многослойностью и неоднозначностью.

Наиболее запутанными являются данные общего характера, поскольку точная идентификация личности возможна лишь при соотнесении информации с фамилией, именем и отчеством, которые выступают основным идентификатором гражданина в правовом обороте, что подтверждается положениями пункта 1 статьи 19 Гражданского кодекса Российской Федерации. Необходимо отметить, что именно органы законодательной власти определяют многоразличные правовые меры как охраны, так и защиты информации, где меры ответственности, установленные Кодексом об административных правонарушениях (далее – «КоАП РФ») играют принципиально большую роль. Весьма обоснованной представляется точка зрения Е.В. Климович, где, «...особая роль в обеспечении реализации и сохранения правопорядка в информационной сфере отведена институту административной ответственности».

Для адекватного и достаточно эффективного реагирования на существующие проблемы, располагающиеся в рамках правового регулирования информационных отношений в цифровых сервисах, следует подчеркнуть многочисленные варианты, которые сводятся к повышению эффективности действующих норм права посредством разграничения составов правонарушений с учетом ущерба, нанесенного правонарушителем юридическому или физическому лицу, кардинального роста размеров штрафных санкций, в отношении как уголовной, так и административной ответственности, не исключая необходимости снабдить дополнительными полномочиями органов государственной власти в контексте административного производства, в том числе праве доступа в информационные системы проверяемых субъектов.

Заключение

Представляет интерес процесс интенсивного становления информационного законодательства в Российской Федерации, которое с начала его формирования по данный момент находится в стагнации. При проведении исследования, выяснилось, что действующая нормативно-правовая база, включающая в свою структуру множество обособленных законодательных актов в значительной мере противоречива, в то время как ее понятийный и терминологический аппарат вовсе не являются совершенными.

Изучение проблем, препятствующих развитию государственной политики в области обеспечения защиты информации, позволяет сделать следующие выводы, где базовыми направлениями и способами совершенствования российского законодательства выступают:

− закрепление норм в Законе 152 в отношении правового регулировании правоотношений в рамках информационной сети;

− принятие поправок в законодательство об информационной сфере касательно оценки и последующих разграничений правового статуса персональных данных, размещаемых в публичном интернет-пространстве.

− издание и закрепление правовых норм, упорядочивающих полномочия органов власти в контексте административного производства, в праве доступа в информационные системы проверяемых субъектов.

Считаем целесообразным вышеизложенные направления и способы совершенствования законодательства, что увеличат вероятность устранения пробелов в этой области и значительно облегчит правоприменительную практику.

Список литературы

1. Правовое обеспечение профессиональной деятельности для специальности «Информационные системы и программирование»: учебник / А.И. Землин, Д.Ю. Левшиц, Е.С. Митячкина, М.В. Мамонова. – М.: КноРус, 2024. – 128 с. EDN DLIPYY

2. Чалдаева Л.А. Методы обеспечения информационной безопасности компании / Л.А. Чалдаева, А.А. Килячков // Финансы и кредит. – 2002. – №21(111). – URL: https://cyberleninka.ru/article/n/metody-obespecheniya-informatsionnoy-bezopasnosti-kompanii (дата обращения: 29.07.2026).

3. Матросова Л.Д. Инструменты для поиска оперативно-значимой информации по открытым источникам / Л.Д. Матросова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2022. – №4(93). – С. 65–72. EDN HPIIUY

4. Статьев В.Ю. Информационная безопасность распределенных информационных систем / В.Ю. Статьев, В.А. Тиньков // Информационное общество. – 1997. – Вып. 1. – С. 68–71.

5. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов / В.И. Ярочкин. – 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

6. Утечки информации в мире: статистика и анализ за 2024 год. – URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-mire-i-otdelnykh-stranakh-za-god (дата обращения: 13.10.2025).

7. В России за январь-июль 2025 года ущерб от IT-преступлений вырос на 16% и составил почти 120 млрд рублей. – URL: https://alrf.ru/news/v-rossii-za-

yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/ (дата обращения: 13.10.2025).