# СУБЪЕКТЫ И ОБЪЕКТЫ ФУНКЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА ПРИ ПРИМЕНЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**Э.Д. Гаврилова,** *студент*
**Волгоградский государственный университет**
**(Россия, г. Волгоград)**

*DOI:10.24412/2500-1000-2026-2-2-201-205*

***Аннотация.*** *Автор теоретически прорабатывает структуру государственной функции по обеспечению безопасности личности, общества и страны при применении информационных технологий, характеризуя субъекты ее осуществления и выделяя объект – общественные отношения по обеспечению безопасности информационных систем. Отмечено, что объектом рассматриваемой функции может также выступать платформенная среда. В рамках исследования анализируются альтернативные способы повышения эффективности деятельности контролирующих информационную безопасность субъектов: 1) усиление правоохранительной функции Роскомнадзора; 2) уход от монополизации силовой составляющей деятельности Роскомнадзора; 3) организационное разукрупнение ведомства с выделением отдельных служб с целью смягчения нагрузки на ведомство.*

***Ключевые слова:*** *функция государства; структура функции; информационные технологии; информационная безопасность; субъект осуществления функции; объект функции государства.*

Развитие информационного общества ассоциируется с ростом числа компьютерных и цифровых устройств и сетей, связано с появлением новых технологий и способов управления обществом со стороны государства: справочно-информационных систем законодательства, электронных порталов государственных и муниципальных услуг, сетевых общественных демократических структур, цифрового гражданского оборота и т.п. Анализ практической стороны деятельности государства требует новых научных достижений, наработок, предложений в сфере реализации государственных функций в цифровую эпоху.

Законодательное обеспечение цифрового суверенитета в России значительно отстает от потребностей сегодняшнего дня: остро ощущается проблема защиты национальных информационных ресурсов, технологий и данных. Несмотря на то, что на настоящий момент действуют законы об основах информатизации и информационной политики, защите прав и интересов детей при пользовании Интернетом, практически отсутствует законодательное регулирование режимов оборота цифровых данных. Кроме государственных стратегий отсутствуют также конкретные правовые акты по вопросам эффективного национального использования робототехники и систем искусственного интеллекта. А проекты, направленные на обеспечение цифровой защищенности объектов критической информационной инфраструктуры, только начинают реализовываться (программные продукты Росатома, антивирусное обеспечение Касперского, Сбербанка России и пр.).

Все изложенное свидетельствует о бесспорной актуальности исследования такой функции государства как обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных на современном этапе, освещения элементов этой функции. Ранее нами были рассмотрены цели и задачи, а также предметное содержание данной функции, однако для полноты исследования немаловажным остается уточнить роль основных субъектов осуществления данной функции и ее объекты.

Так, субъектом функции обеспечения безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных являются в той или иной мере все органы государственной власти. органы местного самоуправления, другие органы и учреждения публично-правовой сферы, использующие цифровые

технологии для регулирования и защиты свой деятельности.

В систему субъектов обеспечения информационной безопасности включены федеральные государственные органы нормотворчества, контроля и надзора в информационной сфере:

1) Правительство РФ;

2) Министерство цифрового развития, связи и массовых коммуникаций;

3) Роскомнадзор;

4) ФСБ России;

5) ФСТЭК России;

6) Центральный Банк Российской Федерации и др.

В целом контроль и надзор осуществляются за деятельностью граждан, общественных институтов и государственных органов, учреждений, применяющих информационно-коммуникативные технологии, в том числе сеть Интернет, и оперирующих в своей повседневной деятельности большими объемами данных [1, с. 40], при этом основная функциональная роль этих властных акторов – обеспечить безопасное применение информационных технологий и цифровых решений. Комплекс полномочий Правительства РФ по вопросам безопасности информации и цифровых данных субъектов права включен в направление деятельности органа по обеспечению законности, прав и свобод граждан в правоохранительной сфере. Однако в России также создан специальный орган, в задачи которого как раз входит реализация информационной политики и сопровождение цифровизации жизни общества, обеспечение информационно-цифровой безопасности – это Минцифры России.

Особенностью правового статуса Минцифры России является межотраслевой характер его управленческой деятельности, подчеркивающий системный и комплексный характер рассматриваемой функции государства. Согласно установленной сфере деятельности, Минцифры России обеспечивает реализацию государственной политики в обширном перечне секторов государственного управления: информационных технологий, теле- и радио вещание, электросвязь и почтовая связь, массовые коммуникации сети Интернет, электронная продукция и программное обеспечение, обработка персональных данных, защита детей от опасной и причиняющей вред их здоровью информации.

Вместе с тем, столь объемный перечень сфер деятельности порождает некоторые сомнения в целесообразности концентрации в руках одного ведомства целого блока государственной политики. В ведении Минцифры России находится лишь одна служба, осуществляющая лицензионно-разрешительные и надзорные функции, – Роскомнадзор. В научных источниках исследуется необходимость усиления правоохранительной функции Роскомнадзора в сфере информационной безопасности в части защиты отечественного информационного пространства от действия противоправного контента [2, с. 117]. Возможно, это один из вариантов решения. Однако, на наш взгляд, следует также отметить, что сегодня в мире имеются передовые технологии искусственного интеллекта, позволяющие на основе технологий машинного обучения обрабатывать гигантские массивы данных и отличать реальные события от фейковых и негативно-разрушительных материалов в сети. При этом, этот вопрос ни в Положении о Минцифры России, на в Положении о Роскомнадзоре никак не отражен.

Другой вариант решения – уход от монополизации силовой составляющей деятельности Роскомнадзора, которая по признанию экспертов сегодня и таки расширена до невероятных пределов. Тем не менее, многие вопросы по-прежнему решаются по усмотрению должностных лиц: Генеральной прокуратуры РФ – в части инициирования незамедлительной блокировки информации, и Роскомнадзора – в части непосредственно организационного и технологического ограничения доступа к этой информации в сети Интернет. В гражданском обществе назрел запрос на повышение прозрачности оснований принятия решений по ограничению и блокировке доступа к информации.

Третий вариант решения – это выделение блока телевидения, радио, печати, почты и электросвязи в отдельную федеральную службу, что позволит разукрупнить и смягчить нагрузку на Роскомнадзор. Однако это наименее предпочтительный вариант, поскольку он не решает проблему изнутри, а предполагает оптимизацию лишь штатов и финансового обеспечения деятельности ра-

ботников, основные же функции по предмету деятельности обоснованно относятся к компетенции Минцифры России.

Следующим значимым субъектом осуществления функции обеспечения безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных является Федеральная служба безопасности. Первоначально права ФСБ России в области информационной безопасности не были четко выделены в законодательстве, впоследствии закреплено направление деятельности – обеспечение информационной безопасности: разработка и осуществление государственной научно-технической политики по сохранности, поддержанию режима секретности и защищенности критически важной государственной и общественной информации с помощью передовых инженерно-технических и криптографических средств. В Федеральном законе от 03.04.1995 № 40-ФЗ [3] определены условия конфиденциального доступа к материалам и результатам этой деятельности службы и правила защиты соответствующей служебной информации в интересах государства. В целом, деятельность рассматриваемого субъекта осуществления функции отличается активной координацией контрразведывательной деятельности тех органов исполнительной власти, которые по закону имеют право на ее осуществление. Например, разделение данных на различные уровни доступа и установка механизмов контроля доступа помогают обеспечить, что только авторизованные сотрудники будут иметь доступ к значимой информации об оперативно-розыскных, дактилоскопических и иных базах данных [4, с. 110]. Получается, что на современном этапе степень актуальности и масштабности угроз информационной безопасности определяет повышенный уровень защищенности цифровых данных. В этой связи ускорение кибератак на российский сектор, усложнение и нарастание массовых инцидентов в информационной сфере настоятельно требуют нормативного закрепления автоматизации моделирования и оценки этих угроз, что соответствует новым вызовам времени [5, с. 99].

Вместе с тем, к числу действенных способов обеспечения информационной безопасности ученые предлагают относить также использование устойчивого к взломам хранения и надежного шифрования данных, безопасных алгоритмов искусственного интеллекта [6, с. 20]. Действительно, учет данных предложений позволит в дальнейшем улучшить прозрачность финансовых операций, укрепить финансовую и налоговую систему (онлайн-кассы, цифровой анализ налоговой отчетности, налоговые чат-боты для информирования налогоплательщиков в социальных сетях и т.д.). Обеспечение информационной безопасности есть ключевое условие достижения экономической безопасности.

Сказанное выше относится к обеспечению информационной безопасности государства. Сегодня ряд нормативных актов предусматривает охрану и защиту объектов критической информационной инфраструктуры Российской Федерации: науки, медицины, связи, транспорта, энергетики, банковской сфере и др.). С одной стороны, правильно подчеркивается необходимость внедрения национальной общественной правовой экспертизы документов и технологий транснациональных цифровых корпораций [7, с. 30]. Данная процедура уже активно используется для воздействия государства на их деятельность.

С другой стороны, требуется системный подход к обеспечению общественной безопасности. Например, на железнодорожном транспорте востребовано использование государственных и ведомственных информационных и технических систем, отслеживающих стандартные и нештатные ситуации: «Безопасный город», «Розыск-магистраль» и т.д. Их применение требует постоянного внимания и совершенствования технической составляющей и координации механизмов взаимодействия, ибо транспорт – это наиболее уязвимая сфера, где совершаются терроризм и другие криминальные преступления, нарушающие общественную безопасность.

Несмотря на это, конечным пользователем функциональной деятельности органов государственной власти и общественных институтов в условиях цифровой эпохи является человек как главный субъект общества, организованного как население и народ государства, наделенные конституционной правосубъектностью. В процессе взаимодействий внутри общества физическое лицо может выступать в качестве гражданина государства, наемного

работника, предпринимателя, государственного служащего, научного работника, студента, ученика, пенсионера и т.п. Очень важно, чтобы в условиях цифрового общества граждане получили новые знания и права, связанные с защитой их личного цифрового суверенитета на персональные данные, активы в материальном и цифровом виде, интеллектуальную собственность и т.д.

Например, за последние 7 лет выросло число преступлений с применением сети Интернет и напротив снизилась примерно на 8-10% раскрываемость подобных преступлений. Посягательство на информационную безопасность личности часто происходит ввиду нарушения требований конфиденциальности, целостности и доступности. Тем не менее, должен находиться в разумной пропорции баланс между ужесточением правовой ответственности за правонарушения в информационной сфере и повышением цифровой культуры личности в информационном обществе.

Исходя из изложенного, функцию обеспечения безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных, можно вполне охарактеризовать как основную. Она вызвана к жизни потребностями эпохи глобализации и мирового сотрудничества в информационной сфере, является крайне актуальной и злободневной в российском обществе.

В свою очередь, объект предложенной функции составляют общественные отношения, возникающие в процессе обеспечения безопасности информационных систем и цифровых данных: их создания, хранения, передачи, использования и защиты на основе современных технологий. Учитывая, что информационные технологии проникают во все сферы общественной жизни, в область действия этой новой функции могут попадать в зависимости от разных факторов любые общественные отношения, подлежащие «цифровизации».

В частности, объектом рассматриваемой функции может быть платформенная среда, так как цифровая платформа – это разновидность цифровых сервисов, имеющая два аспекта: организационный и технический. В рамках организационного аспекта платформа рассматривается как коммуникационная площадка, на базе которой субъекты цифрового общества начинают выстраивать свои отношения через информационные взаимодействия и реализацию цифровых услуг (государственных и сертифицированных частных). Заинтересованные участники, взаимодействующие посредством платформы, рассматриваются как информационная или цифровая экосистема. В рамках технического аспекта платформа рассматривается как набор компонентов (инфраструктурных и прикладных), позволяющих вышеупомянутым участникам реализовывать взаимодействия и сервисы.

В Указе Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» (далее – Стратегия) обозначена позиция России в контексте мировой трансформации – защита цифрового суверенитета, создание и использование отечественных информационных технологий, формулируется понятие «информационное общество». По нашему мнению, это очень важный этап осознания объекта новой функции. Стратегия очертила целевые горизонты развития России до 2030 г. – как создание цифрового (информационного) общества. Однако для усиления позитивных начал и минимизации рисков необходима интенсивная работа по обеспечению информационной безопасности и защите цифровой автономии граждан.

Таким образом, рассматриваемая нами функция государства имеет четко организованную структуру, позволяющую отличить ее от других: объект, субъект, нормативную основу, однородный характер деятельности, а также цель осуществления. Круг субъектов осуществления данной функции обширен. К ним относятся: Правительство Российской Федерации; Минцифры России; Роскомнадзор; ФСБ России; ФСТЭК России; Банк России и др. В свою очередь, объект функции составляют общественные отношения, возникающие в процессе обеспечения безопасности информационных систем и цифровых данных: их создания, хранения, передачи, использования и защиты на основе современных технологий.

**Библиографический список**

1. Пестов И.Е., Виткова Л.А., Шемякин С.Н. Технологии обеспечения информационной безопасности больших данных. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций имени профессора Бонч-Бруевича, 2025. – С. 94 – EDN MXVKON.
2. Солдаткина О.Л. Совершенствование правоохранительных функций Роскомнадзора по обеспечению информационной безопасности как направление современной российской правовой политики // Государство и право. – 2022. – № 12. – С. 112-118.
3. Федеральный закон «О федеральной службе безопасности» от 03.04.1995 N 40-ФЗ // СЗ РФ 10.04.1995. N 15. ст. 1269.
4. Каюшникова Ю.Е. Некоторые вопросы обеспечения информационной безопасности при применении технических средств в деятельности правоохранительных органов // Безопасность в современном мире: материалы VI Международной научно-практической конференции, Волгоград, 02 марта 2024 года. – Волгоград: РАНХиГС, 2024. – С. 109-111.
5. Тихомирова А.А., Яковлев А.В., Алексеев В.В. Формальное описание моделирования угроз безопасности информации по методике ФСТЭК // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 94-100.
6. Айвазян Д.П. Давыдова Н.А., Савинская Д.Н. Применение цифровых технологий в финансовой сфере в целях обеспечения экономической безопасности // Тенденции развития науки и образования. – 2023. – № 104-5. – С. 18-21.
7. Овчинников А.И., Фатхи В.И. Цели и задачи правовых экспертиз в сфере применения цифровых технологий: обеспечение безопасности общества и прав человека // Философия права. – 2024. – № 4 (111). – С. 27-34.

## SUBJECTS AND OBJECTS OF THE FUNCTION OF ENSURING THE SECURITY OF THE PERSON, SOCIETY, AND THE STATE IN THE USE OF INFORMATION TECHNOLOGIES

**E.D. Gavrilova,** *Student*
**Volgograd State University**
**(Russia, Volgograd)**

***Abstract.*** *The author theoretically develops the structure of the state function of ensuring the security of the individual, society, and the country in the use of information technologies, characterizing the subjects of its implementation and identifying the object – social relations in ensuring the security of information systems. It is noted that the object of this function can also be the platform environment. The study analyzes ways to improve the effectiveness of entities overseeing information security: 1) strengthening the law enforcement function of Roskomnadzor; 2) moving away from the monopolization of the enforcement component of Roskomnadzor's activities; 3) organizational disaggregation of the agency with the creation of individual services to reduce the agency's workload.*

***Keywords:*** *state function; function structure; information technology; information security; subject of the function; object of the state function.*