Волкова Ольга Денисовна
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

DOI 10.31483/r-153117

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: *в статье представлено исследование организационно-правовых механизмов обеспечения информационной безопасности в контексте глобального процесса цифровизации. Анализируется специфика современных угроз информационной безопасности, порождаемых цифровой средой, рассматривается комплекс нормативно-правовых актов, регулирующих данную сферу в Российской Федерации, и ключевые организационные меры, реализуемые на различных уровнях для построения эффективных систем защиты информации.*

Ключевые слова: *информационная безопасность, цифровизация, нормативно-правовое регулирование, угрозы информационной безопасности, защита информации, персональные данные, критическая информационная инфраструктура.*

Развитие современного общества сегодня тесно связано с цифровизацией различных областей жизни: экономики через внедрение цифрового рубля, государственного управления, поскольку сейчас функционируют сервисы «Госуслуги», «Работа в России» и другие, социального взаимодействия через широкое

использование мессенджеров и социальных сетей и повседневной жизни, ведь практически в каждом доме есть умная колонка «Яндекс Алиса». Искусственный интеллект и информационные технологии с каждым годом все плотнее входят в жизнь людей, укореняясь в самых разных сферах: от образования до медицины. Широкое распространение информационных технологий, облачных хранилищ, технологий больших данных и, конечно, искусственного интеллекта несет как преимущества, так и недостатки, порождая новые вызовы в сфере информационной безопасности.

Информация стала стратегическим ресурсом, а ее защита стала критической задачей обеспечения безопасности как индивида, так и государства в целом. В условиях цифровизации обеспечение информационной безопасности требует не только применения современных технических средств, но и формирования надежной организационно-правовой основы. Эта основа должна установить правила, определить ответственность, регламентировать сам процесс защиты информации и создать условия для эффектного противодействия информационным угрозам.

Е.В. Катрин под цифровизацией понимает процесс, включающий создание, внедрение и применение цифровых систем и технологий и (или) трансформацию инструментов (объектов, систем и технологий) взаимодействия государства и человека.

Однако цифровая среда, как уже было упомянуто, является «плодородной почвой» для возникновения различных угроз информационной безопасности. К числу наиболее актуальных относятся киберпреступные действия, включающие мошенничество, кражу финансовых средств и конфиденциальных данных, а также вымогательство с использованием вредоносного программного обеспечения. Серьезную опасность представляют такие явления, как: кибертерроризм, выражающийся в целенаправленных атаках на критическую информационную инфраструктуру государств (далее – КИИ), такую как объекты энергетики, транспорта, связи и финансового сектора, с целью дестабилизации обстановки, нанесения значительного ущерба или шантажа.

Особую сложность для обнаружения и устранения представляют атаки, нацеленные на длительное скрытное присутствие в системах для хищения

данных или нарушения функционирования системы. Значительный урон наносят ситуации, связанные с утечками данных, когда конфиденциальная информация становится доступной неопределенному кругу лиц из-за эксплуатации уязвимостей, небрежности персонала или злого умысла. Распространенными остаются атаки, нарушающие доступность информационных ресурсов, к ним относятся атаки типа отказа в обслуживании, известный как DDoS-атаки, которые делают сервисы недоступными для пользователей. Несут опасность также угрозы, связанные с намеренным или случайным искажением информации, и возникающие из уязвимостей глобальных цепочек поставок, когда использование небезопасного стороннего программного обеспечения или оборудования ставит под угрозу безопасность системы.

Говоря про правовое регулирование информационной безопасности в Российской Федерации, стоит обратиться к нескольким нормативным и ненормативным правовым актам, которые представляют собой взаимосвязанную систему. Начать стоит с Конституции Российской Федерации, которая закладывает базовые гарантии, провозглашая право граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки и иных сообщений, а также право на доступ к информации, что формирует конституционные основы защиты информации. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации, определяет информационную безопасность как один из ключевых стратегических приоритетов и задает основные векторы государственной политики в этой области. Доктрина информационной безопасности Российской Федерации, также утвержденная Указом Президента, служит основополагающим документом, детально определяющим национальные интересы в информационной сфере, классифицирующим виды угроз информационной безопасности, а также устанавливающим стратегические цели и основные направления обеспечения безопасности.

Но помимо указанных актов, также существует несколько Федеральных законов, регулирующих обращение информации. Например, Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите

информации» устанавливает базовые понятия и принципы регулирования в информационной сфере. Он регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу и распространение информации, закрепляет принцип ответственности за нарушения законодательства и возлагает на операторов информационных систем обязанности по обеспечению их безопасности. Этот же закон вводит понятие государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. Федеральный закон №152-ФЗ «О персональных данных» детально регламентирует обработку персональных данных операторами, устанавливает требования к их защите, включая обязательность определения уровня защищенности и применения соответствующих организационно-технических мер, определяет права субъектов персональных данных и полномочия Роскомнадзора как уполномоченного органа контроля.

Безопасность наиболее важных информационных систем регулируется Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Он определяет объекты критической информационной инфраструктуры, устанавливает категории их значимости и вводит обязательные требования к обеспечению безопасности значимых объектов. Эти требования включают создание систем безопасности, проведение их аттестации, сертификацию средств защиты и обязательное информирование об инцидентах, разграничивая полномочия ФСТЭК России и ФСБ России в данной сфере.

Ответственность за нарушения в области информационной безопасности, помимо указанных выше федеральных законов, устанавливается также Кодексом Российской Федерации об административных правонарушениях (статья 17), Уголовным кодексом Российской Федерации (статьи 272–275), и Трудовым кодексом Российской Федерации, в котором установлен правовой режим обработки персональных данных работника.

Несмотря на развивающуюся правовую базу и принимаемые организационные усилия, в сфере обеспечения информационной безопасности в условиях цифровизации сохраняется ряд серьезных проблем. К ним относятся опережающие темпы развития угроз и атакующих технологий, по отношению к которым

законодательство и стандарты не всегда успевают адаптироваться. Отмечается сложность и некоторая фрагментированность нормативной базы, обусловленная множеством регуляторов и документов, требующих сложной интерпретации и согласования.

Российская Федерация сформировала развитую систему нормативно-правового регулирования в сфере информационной безопасности, охватывающую ключевые аспекты: общие вопросы защиты информации, специфику работы с персональными данными и безопасность критически важной информационной инфраструктуры. Тем не менее стремительная эволюция цифровых технологий требует постоянного совершенствования законодательства. Поскольку развитие цифровизации в России является приоритетной и долгосрочной целью, необходимо найти пути решения постоянно возникающих проблем, ведь информационные технологии также породили трудности, которых ранее не было. Однако представить жизнь без «Интернета» или связи теперь уже невозможно, а потому необходимо разрабатывать более «подвижное» законодательство, которое сможет быстро адаптироваться под быстро меняющуюся реальность.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru (дата обращения: 10.06.2025).

2. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 02.07.2021 №400 // Собрание законодательства Российской Федерации. – 2021. – №27 (ч. II). – Ст. 5351.

3. Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 №646 // Собрание законодательства Российской Федерации. – 2016. – №50. – Ст. 7074.

4. Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 09.05.2017 №203 // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru (дата обращения: 10.06.2025).

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ (ред. от 24.02.2023) // Собрание законодательства Российской Федерации. – 2006. – №31 (ч. 1). – Ст. 3448.

6. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации. – 2006. – №31 (ч. 1). – Ст. 3451.

7. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (ред. от 02.07.2021) // Собрание законодательства Российской Федерации. – 2017. – №31 (ч. I). – Ст. 4736.

8. Приказ ФСТЭК России «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 №239 (ред. от 27.11.2020) (зарегистрировано в Минюсте России 08.02.2018 №49947) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru (дата обращения: 10.06.2025).

9. Катрин Е.В. «Цифровизация»: научные подходы к определению термина / Е.В. Катрин // Вестник Забайкальского государственного университета. – 2022. – №5. – С. 49–54. DOI 10.21209/2227-9245-2022-28-5-49-54. EDN LPWVIC

10. Организационное и правовое обеспечение информационной безопасности: учебник для вузов / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова [и др.]. – 2-е изд. – М.: Юрайт, 2025. – 357 с.