Секция «10.5 Компьютерное право и информационная безопасность»

Проблемы правового регулирования информационной безопасности в Российской Федерации

Научный руководитель – Морозов Андрей Витальевич

Белоусов Степан Михайлович
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия
E-mail: belousov-stepan@inbox.ru

Правовое регулирование информационной безопасности в Российской Федерации формировалось фрагментарно, в ответ на отдельные технологические и социально-политические вызовы, что обусловило наличие устойчивого комплекса концептуальных, нормативных и организационных проблем. При том что Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» создают базовый каркас регулирования, они не обеспечивают полноты и внутренней согласованности правового режима информационной безопасности во всех сферах. Дополнительное значение имеют Доктрина информационной безопасности Российской Федерации и специальные законы (например, о безопасности критической информационной инфраструктуры), но их развитие также происходит не в форме единой системной кодификации, а через множество разноуровневых актов.

На основе проведенного анализа удалось разделить существующие проблемы правового регулирования информационной безопасности в Российской Федерации на три группы.

Первая группа носит концептуальный характер и связана с недостаточной определённостью понятийно-категориального аппарата, используемого в законодательстве об информации и информационной безопасности. В действующих нормативных актах отсутствуют закреплённые определения ряда базовых категорий («информационная безопасность личности», «киберинцидент», «цифровой след» и др.), а ключевые термины (например, «информация», «информационная система», «защита информации») раскрываются преимущественно через общие формулы без учёта сложившихся технических подходов. Это порождает различие между юридическим и техническим пониманием угроз и инцидентов: профессиональное сообщество оперирует тактиками, техниками и сценариями атак, тогда как правовые нормы описывают угрозы в статичной и часто устаревающей терминологии, не отражающей реальную структуру современных киберрисков. Дополнительную сложность создаёт поиск баланса между интересами государства и общества в обеспечении безопасности, конституционными правами человека на неприкосновенность частной жизни, тайну связи и свободу информации, а также экономическими интересами бизнеса, для которого чрезмерно жёсткие регуляторные меры могут выступать фактором сдерживания инноваций и цифровой трансформации. Концептуальный уровень проблем дополняется фрагментарностью и несистемностью регулирования.

Вторая группа имеет нормативный характер и связана с содержанием и структурой действующей правовой базы в сфере информационной безопасности. Существенная часть современных технологий (искусственный интеллект, большие данные, интернет вещей, облачные и платформенные сервисы, распределённые реестры) пока не получила полноценного нормативного осмысления с точки зрения требований к обеспечению информационной безопасности и распределения ответственности между участниками.

Третья группа— организационная — связана с институциональной архитектурой обеспечения информационной безопасности и уровнем компетенций акторов, вовлечённых в правоприменение и реализацию требований. Функции по регулированию и надзору в области информационной безопасности, защиты информации и персональных данных распределены между несколькими государственными органами и ведомствами, что объективно приводит к дублированию функционала, пересечению полномочий и конкуренции подходов к оценке рисков и нарушений. В правоприменительной практике существенное влияние оказывает недостаточный уровень технической экспертизы у судов и представителей правоохранительных органов, что осложняет квалификацию сложных инцидентов, оценку цифровых доказательств и установление причинно-следственных связей между нарушениями и наступившими последствиями. В частном секторе сохраняется невысокая вовлечённость, особенно среди малого и среднего предпринимательства, которое нередко рассматривает требования информационной безопасности как затратный формальный балласт, а не как элемент собственной устойчивости и конкурентоспособности. При этом именно малый и средний бизнес всё чаще используется злоумышленниками как «слабое звено» в цепочке поставок и контрагентских отношений для компрометации более крупных организаций, что требует переосмысления подходов к распределению обязанностей и ответственности в многосторонних цифровых экосистемах.

Комплексное решение обозначенных проблем предполагает систематизацию и унификацию законодательной базы, формирование устойчивого понятийного аппарата, сопрягающего юридические и технические подходы к описанию угроз и инцидентов, а также выработку согласованных критериев допустимого вмешательства государства в информационную сферу с учётом конституционных прав и экономических интересов. Перспективным направлением представляется создание кодифицированного акта либо масштабная модернизация базового закона об информации и защите информации, дополненная обновлением Доктрины информационной безопасности и профильных стратегий, что позволило бы перейти от реактивного и фрагментарного регулирования к системному и предсказуемому режиму правовой защиты информации в условиях цифровой трансформации.

Источники и литература

1) 1. Федеральный закон от 27.07.2006 № 149 ФЗ «Об информации, информационных технологиях и о защите информации».
2) 2. Федеральный закон от 27.07.2006 № 152 ФЗ «О персональных данных».
3) 3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ).
4) 4. П.В. Ересько. Правовые проблемы обеспечения информационной безопасности личности // Научное издание.
5) 5. Правовое регулирование деятельности в сфере информационной безопасности в Российской Федерации: достижения, проблемы и перспективы развития // Вестник. 2025.
6) 6. Правовые проблемы информационной безопасности // Учебные и научные материалы (электронный ресурс).
7) 7. Материалы по практике применения законодательства о персональных данных и защите информации (аналитические обзоры и комментарии).