ВВЕДЕНИЕ

Влияние развития информационных технологий проникает во все сферы жизнедеятельности общества. Анализ государственных решений в области применения административно-правовых средств стимулирования отрасли информационных технологий в Российской Федерации свидетельствует о смещении публичного интереса с обычного управления на цифровое как наиболее предпочтительное для создания эффективного и прозрачного процесса управления, ориентированного на независимость Российской Федерации в технологическом плане, информационную безопасность, устойчивость граждан к иностранной пропаганде и действию зарубежных спецслужб, использование лучших международных и отечественных разработок для создания технологического преимущества.

Захватить мировое господство в технологической области стремятся все ведущие страны, имеющие такие возможности. Отставание в этой сфере ведет не только к проигрышу в международном пространстве, но и к серьезным проблемам внутри страны в контексте развития отечественных сегментов экономики и безопасности критической информационной инфраструктуры.

Актуальность выбранной темы исследования обусловлена следующими факторами.

Во-первых, в связи с беспрецедентным развитием информационных и инновационных технологий эта отрасль российской экономики требует особого подхода к административно-правовому регулированию правоотношений, возникающих внутри нее, или совокупного регулирования в других отраслевых и межотраслевых правоотношениях, что диктует повышенное внимание со стороны государства. При этом межотраслевая интеграция информационных технологий, продолжающих активно развиваться, предопределяет серьезные угрозы для суверенитета государства и общественных интересов, что требует усиления административно-правового регулирования.

Во-вторых, в системе национальной и информационной безопасности Российской Федерации административно-правовое регулирование в отрасли информационных технологий (далее – ИТ-отрасль) занимает особое место и обеспечивается совокупностью различных средств: правовых, технических, экономических и др.

Административно-правовое регулирование в ИТ-отрасли включает в себя ряд аспектов, таких как цели, задачи и принципы государственной политики в сфере информационных технологий; система органов государственного управления, иных органов, организаций и учреждений, участвующих в реализации государственной политики в сфере защиты инфраструктуры информационных технологий и повышения ее эффективности и результативности, а также распределение между ними полномочий; определение правового статуса хозяйствующих субъектов в области информационных технологий, оценка нормативно-правовой базы и ее совершенствование с учетом новых задач и перспектив развития общества и государства; взаимосвязь административных институтов регистрации, учета, отчетности, лицензирования, аттестации, аккредитации, сертификации, стандартизации, метрологии, государственных закупок, контроля (надзора), института административной ответственности за правонарушения в области информационных технологий и др.; характеристика мер административного обеспечения; установление мер административного принуждения; выявление проблем и определение путей их решения; совершенствование отдельных элементов механизма правового регулирования и др. Таким образом, административно-правовое регулирование в ИТ-отрасли в Российской Федерации требует системного исследования с точки зрения положений административного права, включая анализ информационных угроз, других существующих проблем, а также выработки мер по их предотвращению.

В-третьих, государство активно вовлечено в решение ключевых задач ИТ-отрасли, в том числе посредством использования ее высокотехнологичной и наукоемкой продукции, что предполагает создание или совершенствование необходимой правовой основы. С помощью информационных технологий могут решаться и решаются отдельные государственные вопросы, относящиеся к области национальных интересов Российской Федерации и особо защищаемые правом. При этом в сфере юриспруденции отсутствуют некоторые определения, позволяющие более точно охарактеризовать сложные управленческие процессы с помощью правовой терминологии, поэтому требуется усилить правотворческую инициативу для совершенствования законодательства в ИТ-сфере.

В-четвертых, процесс внедрения ИТ-решений во все области с целью повышения эффективности работы за счет цифровизации одновременно влечет за собой быстрый рост правонарушений в ИТ-сфере,

что затрагивает государственные интересы и вопросы общественной безопасности. Человеческая цивилизация находится в постоянной динамике. Новые технологические разработки позволяют сделать жизнь человека значительно комфортнее. Вместе с тем по своей природе информатизация может иметь как положительное, так и отрицательное влияние на формирование правового поведения[1].

Динамичность развития и распространенность противоправных деяний, совершаемых с использованием компьютерных технологий, сделали их предметом исследования с позиций уголовного и административного права, криминологии, криминалистики, уголовного процесса и других наук.

Существование возможности доступа человека, находящегося на любом расстоянии и в любой точке мира, к определенному информационному ресурсу с помощью технических средств различных национальных и международных провайдеров, а также наличие компактных портативных компьютерных устройств, имеющих доступ к большому количеству услуг и сервисов, обусловливают возможность совершения представителями криминального сообщества межрегиональных и транснациональных преступлений и административных правонарушений.

В-пятых, влияние глобализации на безопасность несовершеннолетних в условиях цифровой среды также становится отдельным направлением административно-правового регулирования. Положительные и негативные аспекты, связанные с использованием информационного пространства детьми, определяются реализацией социальной роли государства в защите интересов наименее защищенной группы населения. Участие государства в обеспечении безопасности несовершеннолетних должно включать не только своевременное совершенствование законодательства, но и регулирование общественных и частных инициатив, направленных на создание безопасной цифровой среды.

Мировое сообщество обеспокоено влиянием сети «Интернет» и определенного контента на несовершеннолетних, их психическое и физическое здоровье. Все официальные и неофициальные лица, выступающие в международном и национальном информационных

[1] См.: Безручко Е.В., Рысай Б.Г. Некоторые проблемы административной ответственности в сфере связи и информации // Юристъ-Правоведъ. 2020. № 1 (92). С. 180.

пространствах, признают опасность влияния интернета на детей вне зависимости от страны их проживания. Закономерное развитие процессов цифровизации под влиянием постоянно совершенствующихся технологий влечет за собой разработку и формирование правовых форм и методов защиты несовершеннолетних в сети «Интернет», углубление связей между группами стран по данному вопросу. При этом использование методов сравнительного правоведения при анализе опыта Российской Федерации и, например, КНР как страны, которая нашла собственное решение в рассматриваемой области, позволяет выявить общее и специфическое в административно-правовом регулировании обеспечения защиты детей в сети «Интернет», установить возможность или неприемлемость заимствования правовых элементов, определить общемировые и национальные тенденции.

В-шестых, новые форматы быстрого взаимодействия между субъектами административных правоотношений создали проблему незащищенности персональных данных лиц, доверивших государству свои личные сведения, подлежащие учету и электронной обработке государственными служащими или иными уполномоченными субъектами. С развитием в сфере государственного управления информационно-телекоммуникационных технологий основной документооборот между должностными лицами органов исполнительной власти был переведен в электронную и цифровую форму. В 2025 г. административно-правовые нормы в области защиты персональных данных подверглись корректировке, в том числе была усилена административная ответственность за нарушение законодательства в области защиты персональных данных, что потребовало как от публичных субъектов власти, так и от большинства компаний, представляющих российское бизнес-сообщество, провести внутренний аудит своей деятельности и разработать более серьезный механизм контроля за аккумулированными данными.

В-седьмых, агрессивное компьютерное вмешательство и DDoS-атаки на информационную систему российских компаний и государственный сектор со стороны «черных хакеров», действующих в интересах недружественных по отношению к России иностранных государств, могут причинять серьезный экономический ущерб национальной безопасности страны и выступать в качестве одного из способов дестабилизации обстановки в российском обществе, создавать основы для различных провокаций.

Государственное регулирование в этом случае должно касаться обучения ИТ- и ИБ-специалистов, повышения цифровых компетенций, развития технологий для расследования киберпреступлений, взаимодействия публичных органов власти и ИТ-компаний, расширения международного сотрудничества и т.д.

В-восьмых, как отмечают некоторые исследователи, одним из типов угроз, исходящих из интернет-пространства, является подрыв легитимности власти и преднамеренное создание информационного хаоса для стремительного возникновения протестных акций. С помощью мобильных технологий и социальных сетей протестным акциям придают более высокую управляемость, организованность, массовость, способствуют повышению активности их участников[2], что создает для сотрудников правоохранительных органов дополнительные трудности в их предотвращении и локализации. Например, использование социальных сетей TikTok, «ВКонтакте», YouTube и Instagram[3] позволило привлечь для участия в несанкционированных массовых акциях, имевших место в г. Москве 23 января 2021 г., 1396 человек, 70 из которых были несовершеннолетними[4]. Действия нарушителей были квалифицированы судебными органами как уголовно наказуемые деяния (ч. 2 ст. 151.2, ст. 167, 213, 318 УК РФ и др.) и административные правонарушения (ст. 19.3, 20.1, 20.2 КоАП РФ).

Актуальным вопросом является также проблема использования правонарушителями восприимчивых граждан или граждан, оказавшихся в тяжелой жизненной ситуации либо приведенных в состояние психологического подчинения, в совершении экстремистской или террористической деятельности в интересах преступников.

---

[2] См.: Масликов В.А. Информационные технологии в социальном протесте // Материалы Афанасьевских чтений. 2018. № 1 (22). С. 5; Малькевич А.А. Роль социальных сетей в протестном политическом участии граждан // Управленческое консультирование. 2020. № 1 (133). С. 35–39.

[3] Компания Meta (признана в РФ экстремистской организацией и запрещена) внесена в соответствующий реестр Минюста. 21 марта 2022 г. Тверской суд г. Москвы удовлетворил иск Генпрокуратуры РФ о запрете деятельности Meta Platforms Inc. на территории России; запрещена деятельность Meta в части реализации продуктов – социальных сетей Facebook и Instagram.

[4] Акции в поддержку Алексея Навального и столкновения с полицией. Главное. Электронный ресурс. URL: https://www.rbc.ru/politics/

24/01/2021/600ae9859a794701e0e62558 (дата обращения: 22.10.2025).

В-девятых, МВД России как главный субъект в области охраны общественного порядка и обеспечения общественной безопасности осуществляет также и противодействие преступлениям и административным правонарушениям в ИТ-сфере, стремясь для повышения эффективности своей деятельности не только по-новому структурировать организационно-штатные элементы, но и добавить результативности в содержательные компоненты исполнения возложенных на них государственных функций. При этом в области предотвращения ИТ-правонарушений особую роль играет взаимодействие МВД с физическими и юридическими лицами, в том числе информирование граждан о видах киберпреступлений и борьбе с ними, а также повышение правовой и финансовой грамотности населения при работе с цифровыми устройствами. В связи с этим особо актуальным является рассмотрение в монографии вопроса о способах противодействия правонарушениям в области информационных технологий.

В-десятых, в современной деятельности рядового сотрудника полиции продолжает существовать проблема коммуникации со специальными субъектами, обеспечивающими информационную безопасность. Рост киберпреступлений и административных правонарушений, совершенных в сфере информационных технологий, влечет за собой изменение способов фиксации цифровых доказательств, а значит, алгоритма получения данных и методики административных и уголовных расследований по данным видам правонарушений, что предполагает расширение цифровых и ИТ-компетенций сотрудников полиции для выполнения служебных обязанностей.

Таким образом, одним из приоритетных направлений в административном праве является рассмотрение административно-правового регулирования в отрасли информационных технологий, которое позволяет научной и правовой доктрине по-новому трансформировать свои устоявшиеся догмы.

Монография содержит большой объем эмпирического материала, проанализированного с точки зрения не только права, но и других научных областей, в т.ч. экономики, социологии, психологии, культурологии, философии и др. В ней приводятся примеры новейшей продукции и значимых событий ИТ-отрасли, оказывающих влияние на все сферы жизни современного человека, актуальная статистика, мнения различных профильных специалистов, ученых, преподавателей, практиков по исследуемым в монографии вопросам,

определяются основные угрозы, связанные с информационными технологиями, анализируется судебная практика и зарубежный опыт, раскрываются некоторые направления административно-правового регулирования в ИТ-отрасли с целью обоснования необходимости защиты прав граждан в условиях беспрецедентного расширения цифровых возможностей государства и частных корпораций, в том числе в сфере контроля за социальной жизнью общества, а также определения роли правовых регуляторов в сдерживании таких процессов.

Отдельно рассматриваются проблемы влияния развития информационных технологий на науку, включая юриспруденцию.

Направления дальнейших исследований, предложенные в монографии, предполагают привлечение широкого круга специалистов к решению ключевых проблем, стоящих перед Российской Федерацией на пороге возможных глобальных информационных войн и подрыва национальной идентичности, бесконтрольного применения цифровизации, технологий искусственного интеллекта во вред человеческим ценностям.

Посредством объединения профессиональных усилий научного сообщества предлагается найти баланс практического применения информационных технологий и административно-правового регулирования в этой отрасли, а также определить границы внедрения ИТ в государственное управление.