Дата поступления рукописи в редакцию: 14.07.2026 г. DOI: 10.24412/2224-9133-2026-8-321-324
Дата принятия рукописи в печать: 01.09.2026 г.

БЕТРОЗОВА Мадина Амирхановна,
преподаватель кафедры организации правоохранительной деятельности Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России, кандидат исторических наук,
e-mail: mail@law-books.ru

К ВОПРОСУ О ПРИМЕНЕНИИ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В представленной статье проведен анализ современного состояния административного законодательства и правоприменительной практики в сфере информационной безопасности. Авторы положительно характеризуют динамику совершенствования законодательства об административной ответственности, начиная от ужесточения санкций и заканчивая введением новых составов правонарушений. Акцентируется внимание на практических проблемах и сложностях применения административной ответственности, которые получили распространение в современной практике.*

Ключевые слова: *административная ответственность, информационная безопасность, правоприменение, административное законодательство.*

BETROZOVA Madina Amirkhanovna,
Lecturer at the Department of Law Enforcement Organization of the North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, candidate of historical sciences

ON THE APPLICATION OF ADMINISTRATIVE RESPONSIBILITY IN THE FIELD OF INFORMATION SECURITY

Annotation. *This article analyzes the current state of administrative legislation and law enforcement practice in the field of information security. The authors positively characterize the dynamics of improvements in administrative liability legislation, ranging from the tightening of sanctions to the introduction of new offenses. They also highlight the practical problems and complexities of applying administrative liability, which have become widespread in modern practice.*

Key words: *administrative liability, information security, law enforcement, administrative legislation.*

В современном российском государстве особое практическое значение для обеспечения стабильного развития современного российского государства имеет информационная безопасность, поскольку в условиях повсеместной информатизации и цифровизации происходит серьезная трансформация информационных правоотношений, а в контексте обострения геополитической напряженности и антироссийской пропаганды – регулярно возникают новые вызовы и угрозы национальной безопасности, проявляющиеся непосредственно в информационной среде. Информация в современном мире активно используется в целях дестабилизации обстановки на определенных территориях, что происходит как посредством системного и организованного информационно-психологического воздействия, так и путем активизации противоправных посяга-

тельств различной направленности.

Проблематика информационной безопасности активно исследуется в современной правовой науке, что объективно обусловлено значительной интенсификацией и масштабированием угроз, возникающих в данной сфере. На наш взгляд особого внимания заслуживает институт юридической ответственности и особенности его развития в сфере информационной безопасности. Во-первых, справедливым представляется сочетание мер административной и уголовной ответственности с учетом степени общественной опасности совершаемых деяний и различного субъектного состава правонарушителей. Во-вторых, институт ответственности имеет важнейшее практическое значение не только для наказания виновных лиц и определения справедливых правовых последствий их деяний, но и наглядно проявляется его профилактический и предупредительный потенциал. В-третьих, ответственность в сфере информационной безопасности активно изменяется за последние годы, что предопределяет необходимость своевременной оценки эффективности данного института в целях его дальнейшего совершенствования.

В рамках представленного исследования видится необходимым сконцентрировать внимание на актуальных вопросах применения административной ответственности в сфере информационной безопасности, поскольку данная разновидность ответственности подвергается наибольшему количеству изменений. Именно выявление и пресечение противоправного функционирования в анализируемой сфере в совокупности с мерами административной ответственности способны наиболее результативно повлиять на отсутствие дальнейшего развития противоправного функционирования. Кроме того, институт административной ответственности характеризуется качественным субъектным составом, что позволяет определить справедливый объем правовых последствий не только для индивидов, но и для юридических лиц, что выступает основой комплексного адресного воздействия с учетом специфики противоправного функционирования конкретной направленности.

Отметим, что согласно действующему российскому законодательству, информационная безопасность определяется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [3]. Данная сфера затрагивает не только интересы государства, на чем активно акцентируется внимание в рамках исследования процесса обеспечения информационной безопасности в контексте национальной безопасности, но и в равной степени актуальна для общества и индивидов, что наглядно проявляется в современных реалиях в части активизации адресного информационно-психологического воздействия на отдельные категории населения и серьезных общественных последствиях интенсификации противоправных посягательств в информационной сфере.

Институт административной ответственности традиционно формируется за счет целого ряда норм КоАП РФ, где выделена отдельная глава 13, регламентирующая ответственность за деяния в области связи и информации. Данная глава достаточно объемная – более 70 статей, закрепляющих ответственность за действия/бездействия различного характера, связанные не только с реализацией и обеспечением права на информацию, но и с противоправным использованием различных средств связи и информационного обмена, а также функционированием средств массовой информации. Однако если говорить о широком понимании информационной безопасности, следует подчеркнуть наличие ряда других административно-правовых норм, которые хоть и структурно отнесены к иным главам КоАП РФ, но в полной мере актуальны для анализируемой сферы общественных отношений (например, ст. 19.7.15 КоАП РФ и др.).

Глава 13 КоАП РФ характеризуется качественным и количественным многообразием составов административных правонарушений, что в полной мере коррелирует с многоаспектностью обеспечения информационной безопасности. В современной научной литературе содержится множество подходов к классификации правонарушений в данной сфере, однако большинство подходов в качестве критерия классификаций объекты и предметы противоправного посягательства [1, с. 29]. На основе анализа действующего административного законодательства следует сделать вывод о том, что его состояние и оперативность совершенствования в полной мере удовлетворяет современным вызовам и угрозам. Однако подчеркнем, что в отдельных сферах информационных правоотношений по-прежнему не удается достигнуть опережающего ограничительного воздействия, что объективно обусловлено непосредственно динамикой развития и трансформации информационной среды, в том числе в трансграничном формате. Представляется, что тенденция введения новых составов административной ответственности в сфере информационной безопасности и совершенствование ранее закрепленных сохранится на протяжении

длительного времени, что напрямую связано с интенсификацией процессов информатизации и цифровизации различных сфер жизнедеятельности российского общества.

Еще одной справедливой современной тенденцией института административной ответственности в сфере информационной безопасности видится не просто соразмерное ужесточение санкций с учетом развития противоправной практики различной направленности, но и введение так называемых «оборотных» штрафов, которые определяют объем от суммы годовой выручки индивидуальных предпринимателей и юридических лиц. Таким образом, административные санкции перестают быть незначительными и слабо ощутимыми для субъектов экономической деятельности, что значительно усиляет превентивное воздействие (например, ч. 4 ст. 13.46, чч. 5 и 6 ст. 13.41 КоАП РФ).

Однако эффективность института административной ответственности зависит не только от состояния отраслевого законодательства, но и от непосредственной его реализации. Анализируя правоприменительную практику, видится необходимым выделить некоторые проблемы, а также предложить пути их решения:

сложности идентификации правонарушителей в случае трансграничного противоправного посягательства. Данная проблема особо актуальна для правонарушений, совершаемых в сети «Интернет» и иных информационных системах. Представляется целесообразным предложить нормативное закрепление принципа экстерриториальности в КоАП РФ: Введение в КоАП РФ нормы (по аналогии со ст. 4.5 или ст. 1.8 УК РФ), согласно которой административная ответственность наступает независимо от места совершения правонарушения, если оно направлено против критической информационной инфраструктуры (КИИ), граждан или организаций РФ.

сложности определения самого события правонарушения, включающего в себя место и время его совершения. На практике распространяется фрагментарная фиксация видимых материальных следов. В данном контексте предлагается введение законодательного переосмысления «места» и «времени» правонарушения, например, введение в процессуальную часть КоАП РФ понятие «виртуального места совершения правонарушения», определяя его по выбору: место нахождения потерпевшего (цели атаки), место нахождения сервера/ресурса или место обнаружения цифрового следа, а также определять время правонарушения как период от начала противоправного воздействия до момента его пресечения или обнаружения (применяя концепцию длящегося правонарушения).

высокая степень латентности правонарушений в сфере информационной безопасности. С одной стороны, в условиях динамики совершенствования информационных и цифровых технологий отдельные деяния крайне сложно выявить. С другой стороны - лица, чье права нарушаются, далеко не всегда обращаются в компетентные органы в целях пресечения противоправного воздействия, что в итоге приводит к его дальнейшему масштабированию. В данном случае, в качестве решения указанной проблемы, следует предложить установление административной ответственности за сокрытие факта утечки персональных данных или взлома ИС (с возможностью смягчения наказания при добровольном и оперативном декларировании).

Вышеназванные проблемы и сложности объективно обусловлены динамикой внедрения информационных и цифровых технологий в различных сферах жизнедеятельности российского общества и государства. В настоящее время большинство информации переведено в электронный формат, а процесс ее создания, хранения и распространения предполагает вовлеченность целого ряда субъектов, от законопослушного поведения которых постоянно зависит эффективность обеспечения информационной безопасности. В данном контексте следует подчеркнуть, что на эффективность института административной ответственности также влияет своевременное совершенствование иных административных процедур, например, таких как лицензирование, сертификация, надзор и др. С одной стороны, их состояние в полной мере должно соответствовать современной практике с учетом возникающих вызовов и угроз. С другой стороны, фрагментарность информирования о нововведениях участников информационных правоотношений приводят одновременно не только к увеличению количества правонарушений, но и исключают возможность выявления рисков противоправных посягательств в отношении их прав и свобод в информационной сфере в целом. В данном контексте значительно актуализируется системная интеграция всех современных административно-правовых механизмов [2, с. 162], а также сопровождение их активным информированием населения.

Таким образом, на основе проведенного анализа следует сделать вывод о том, что решение указанных проблем требует комплексного реформирования как материального и процессуального административного законодательства, так и организационно-технических подходов правоохранительных и иных исполнительных органов государственной власти.

Последние годы институт административной ответственности в области информационной безопасности претерпел существенные изменения:

введены новые составы правонарушений, увеличены сроки привлечения к административной ответственности за отдельные деяния, а также ужесточены санкции административно-правовых норм. Наиболее актуальными представляются практические проблемы и сложности, которые негативно отражаются на эффективности института административной ответственности в целом. Борьба с распространением противоправного поведения в указанной сфере является одним из приоритетных направлений российского государства в современных реалиях.

Список литературы:

[1] Ивакин, А. А. Совершенствование административной ответственности в области защиты информации в условиях гибридной войны против России на современном этапе / А. А. Ивакин, А. Н. Прокопенко // Проблемы правоохранительной деятельности. 2025. № 2(60). С. 26-35.

[2] Нурмухаммадзода, Ф. Д. Системность административно-правового обеспечения информационной безопасности в Российской Федерации и Республике Таджикистан / Ф. Д. Нурмухаммадзода // Евразийский юридический журнал. 2025. № 5(204). С. 161-163.

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

References:

[1] Ivakin, A. A. Improving administrative responsibility in the field of information protection in the context of a hybrid war against Russia at the present stage/A. A. Ivakin, A. N. Prokopenko // Problems of law enforcement. 2025. № 2(60). S. 26-35.

[2] Nurmukhammadzoda, F. D. Consistency of administrative and legal support of information security in the Russian Federation and the Republic of Tajikistan/F. D. Nurmukhammadzoda // Eurasian Legal Journal. 2025. № 5(204). S. 161-163.

[3] Decree of the President of the Russian Federation of 05.12.2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation "// Collection of Legislation of the Russian Federation. 2016. № 50. Art. 7074.