

ТЕНДЕНЦИИ РАЗВИТИЯ ИНСТИТУТА АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ СВЯЗИ И ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Обеспечение информационной безопасности и защита цифрового суверенитета являются приоритетными задачами политики Республики Беларусь. В соответствии с Концепцией национальной безопасности [1], противодействие угрозам в цифровой среде отнесено к стратегическим направлениям деятельности, а административно-правовые меры выступают ключевым инструментом обеспечения интересов личности и государства.

В современной юридической литературе Г. А. Василевич справедливо отмечает, что в информационной сфере объектом посягательства становятся не только отношения в области управления, но и устойчивость критической информационной инфраструктуры [2]. Как подчеркивает В. К. Ладутько, правовая природа административного деликта в сфере связи неразрывно связана с категорией «информационной безопасности», что требует переосмысления классических подходов к институту ответственности [4]. Важным элементом системы является регламентация деятельности специальных субъектов – операторов электросвязи и владельцев информационных ресурсов. Меры главы 23 КоАП выполняют превентивную функцию, обеспечивая соблюдение регламентов безопасности [5].

Теоретические аспекты трансформации ответственности дополняются исследованиями других ученых. А. Н. Крамник обосновывает важность соблюдения принципа законности [6], В. В. Лосев указывает на необходимость пересмотра подходов к субъективной стороне правонарушения в эпоху алгоритмов [7]. В этой связи нами предлагается переосмысление технической категории «алгоритмическая безопасность» и её перевод в правовую плоскость. Под алгоритмической безопасностью в контексте административно-деликтного права следует понимать состояние защищенности программно-аппаратных комплексов и алгоритмов принятия решений, при котором обеспечивается их контролируемость, правомерность функционирования и минимизация рисков причинения вреда интересам личности, общества или государства. Дальнейшее развитие законодательства требует уточнения категории «цифровой вины» как несоблюдения правовых стандартов такой безопасности.

В настоящее время профильными ведомствами прорабатываются механизмы повышения эффективности административного процесса для создания прозрачной системы правовой подотчетности. Дальнейшее укрепление цифрового суверенитета требует гармонизации технических стандартов с правовыми нормами, что позволит максимально реализовать превентивные цели ответственности, обеспечив неизбылемость конституционных гарантий прав личности в цифровом обществе.

Список использованных источников

1. Концепция национальной безопасности РБ: Указ Президента Респ. Беларусь от 09.11.2021 № 406 (ред. от 12.02.2024) // Эталон-Беларусь. – 2026.
2. Василевич, Г. А. Конституционные основы информационной безопасности / Г. А. Василевич // Право.by. – 2023. – № 4. – С. 5–11.
3. Ладутько, В. К. Трансформация институтов ответственности в условиях цифровизации / В. К. Ладутько // Вестник БГЭУ. – 2024. – № 2. – С. 42
4. Кодекс РБ об административных правонарушениях: 6 янв. 2021 г. № 91-3 (ред. от 05.01.2024) // Эталон-Беларусь. – 2026.
5. Крамник, А. Н. Административно-деликтное право / А. Н. Крамник. – Минск, 2020.
6. Лосев, В. В. Юридическая ответственность в эпоху алгоритмов / В. В. Лосев // Право и демократия. – 2024. – Вып. 35.