

**Цифровой суверенитет как основа национальной безопасности РФ: новая доктрина информационной безопасности**

**Научный руководитель – Каменева Анна Николаевна**

*Гендугова Элина Эдуардовна*

*Студент (бакалавр)*

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия

*E-mail: elinagendugova@mail.ru*

В цифровую эпоху информация становится важнейшим стратегическим ресурсом, напрямую влияющим на обороноспособность государства и его стабильное экономическое развитие. Исходя из этого категория информационного суверенитета страны приобретает ключевое значение, так как именно он обеспечивает способность государства самостоятельно управлять цифровой инфраструктурой и свободно распоряжаться информационными ресурсами, что в современных реалиях превращает информационную безопасность в фундамент, на котором базируется система национальной безопасности России [1].

Как следует из заявления помощника секретаря Совета Безопасности Российской Федерации Дмитрия Грибкова, в ведомстве началась подготовка новой редакции доктрины Информационной безопасности РФ [2]. Основной идеей обновленного стратегического документа, вызванной изменениями в современной геополитической и технологической обстановке в мире, является достижение полноценного информационного суверенитета страны посредством разработки и обслуживания отечественной IT-инфраструктуры.

На этапе цифровизации всех сфер жизни общества информационные инструменты все чаще используются в качестве механизмов, активно применяемых в военных и криминальных целях. В связи с этим перед государством возникает потребность в защите национальных интересов от посягательств недружественных стран посредством компьютерной разведки и использования цифровых технологий в качестве инструмента ведения информационной войны в нынешних политических реалиях.

Следует отметить усиление роли государственно-частного партнерства, связанное с невозможностью обеспечения информационной безопасности без участия коммерческих компаний. Современная критическая информационная инфраструктура представляет собой не обособленные государственные объекты, а сложный механизм, соединяющий государственный сегмент и частные компании для достижения финансовой и информационной стабильности посредством консолидации усилий.

Особую сложность вызывает внедрение информационных инструментов в финансовую сферу государства и цифровизация экономики. Данный процесс несмотря на преобладающие позитивные изменения носит противоречивый характер. С одной стороны, развитие отечественных цифровых инструментов создает благоприятные условия для обеспечения финансовой безопасности страны. С другой стороны, эти же инновации порождают новые вызовы и угрозы, требующие незамедлительного реагирования путем выработки как комплексного подхода к регулированию системы национальной безопасности в целом, так и совершенствования законодательства в сфере оборота цифровых финансовых инструментов и использования информационных технологий.

Достижение национальных интересов требует сбалансированного подхода к регулированию цифровых финансовых рынков. В качестве примера следует привести криптовалютно-

ты, которые по-прежнему остаются инструментом для теневой экономики, обхода санкций, легализации денежных средств и финансирования терроризма [3]. Данная проблема актуализирует необходимость модернизации законодательства для эффективного противодействия незаконной деятельности с криптоактивами. Именно здесь наиболее активно проявляется взаимосвязь информационной и финансовой безопасности: несовершенства в информационной среде порождают серьезные проблемы в экономической сфере жизни общества. В условиях усиления влияния современных технологий разработка нормативно-правового регулирования в области цифровой среды обуславливает необходимость законодательного регулирования критической информационной инфраструктуры на федеральном уровне [4].

Таким образом, разработка новой доктрины информационной безопасности и развитие законодательства в области регулирования IT-технологий, направленные на достижение информационного суверенитета страны, является стратегическим курсом на сохранение Российской Федерацией своей субъектности в цифровую эпоху.

### Источники и литература

- 1) Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» №646 от 5 декабря 2016 года
- 2) Новая доктрина информационной безопасности России: главные положения // РБК. 2025
- 3) Антропов В.В. Современные цифровые технологии в международных расчетах как инструменты обхода антироссийских санкций. // Экономика. Налоги. Право. 2024. с. 47-55
- 4) Полякова Т.А., Троян Н.А. Стратегические задачи обеспечения технологического и цифрового суверенитета: правовые аспекты формирования новой информационной среды // Правовая информатика. 2025. №1, с. 70-78