

УДК 347.73

*Вердиева Виктория Эльдаровна,
студент*

*ФГБОУ ВО «Российский государственный
университет правосудия»*

Уральский филиал, юридический факультет

Россия, г. Челябинск

*Научный руководитель: Степанова Марина Николаевна,
заведующая кафедрой*

государственно-правовых дисциплин,

кандидат экономических наук, доцент

Уральский филиал

*ФГБОУ ВО «Российский государственный
университет правосудия»*

Россия, г. Челябинск

ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ РЕАЛЬНОСТИ

***Аннотация:** На сегодняшний день наблюдается активная интеграция информационных процессов, которая охватывает все сферы человеческой жизнедеятельности, а наша страна в этой сфере не является передовой. Развитие цифровизации оказывает большую роль на общество в целом,*

В связи с этим в данной статье рассмотрены актуальные вопросы этой проблемы на различных отраслевых уровнях в современных условиях внедрения прогрессивных технологий.

***Ключевые слова:** национальная безопасность, цифровизация, правовое регулирование, цифровая реальность.*

ENSURING NATIONAL SECURITY IN THE CONDITIONS OF DIGITAL REALITY

***Annotation:** Today, there is an active integration of information processes, which covers all spheres of human activity, and our country is not advanced in this area. The development of digitalization has a big role for society as a whole,*

In this regard, this article discusses topical issues of this problem at various industry levels in modern conditions of the introduction of advanced technologies.

***Key words:** national security, digitalization, legal regulation, digital reality.*

Одной из развивающихся направлений XXI века является цифровизация, поэтому возникновение цифровых и информационных отношений стало причиной формирования правовых норм, регулирующих эти отношения. Информационные технологии постепенно охватывают все сферы общественной жизни, а также определяют аспекты отношений между государствами. В этом процессе участвуют и федеральные органы государственной власти разрабатывая и реализуя государственные программы в данной сфере. В связи с этим цель данной статьи заключается в определении основных направлений реализации правовых норм обеспечения национальной безопасности в условиях цифровизации [1, с. 27].

Понятие «национальной безопасности» обширное и включает в себя все виды безопасности, которые напрямую связаны с развитием деятельности государства. Но если обратиться к такому нормативно правовому акту как Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации", то в главе 1 пункта 5 подпункт 1 увидим определение национальной безопасности. национальная безопасность Российской Федерации (далее - национальная безопасность) - состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных

прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны¹. Исходя из этого определения можно сделать вывод, что национальная безопасность, предусмотренная как Конституцией, так и иным законодательством Российской Федерации включает в себя не только оборону страны, но охватывает и все сферы безопасности и к таковым относятся информационная безопасность, общественная, безопасность личности и многие другие.

Роль цифровых технологий особенно сильно возрастает в тот промежуток времени, когда у государств происходят глобальные изменения. И рассматривая две стороны одной медали, можно сказать, что все хорошо, идет прогресс в развитии. Но другая сторона этой медали создавала угрозу для нормального обеспечения национальной безопасности.

Основной проблемой является угроза «цифровому суверенитету», экономической стабильности государства путем постоянного финансирования расходов на разработки новых технологий. Большие затраты идут на информационные технологии, на все устройства, которые связаны с обработкой персональных данных (планшеты, компьютеры, и т.д.). И с одной стороны данное финансовое стимулирование способствует развитию всех информационных технологий, но с другой стороны создается угроза, например, распространение сведений, которые вводят общество в заблуждение. Существенную роль играет СМИ в пропаганде недостоверной информации. И именно здесь необходимо активное информационное взаимодействие с гражданами и со всеми структурами гражданского общества, которые смогут информировать граждан правдивой позицией политических действий как внутренне, так и внешне [2, с.262].

1. Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации" // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru>, 03.07.2021 (дата обращения 12.04.2023).

Несмотря на то, что есть федеральные законы, такие как ФЗ «О персональных данных»¹, «О безопасности критической информационной инфраструктуры Российской Федерации»² и федеральный закон «Об информации, информационных технологиях и о защите информации»³ содержит основные определения по поводу информации и определяет, какие данные можно считать доступными, а какие конфиденциальными, СМИ все равно пропагандирует информацию, которая существенно умаляет авторитет Российской Федерации во внутригосударственных и международных отношениях.

В связи с этим и возникает проблема отсутствия полного и четкого правового регулирования национальной безопасности в условиях цифровизации.

По этой причине требуется укреплять защиту информационной безопасности, ведь это является приоритетным направлением развития как на законодательном уровне, так и практическом.

В рамках построения стратегии национальной безопасности должно быть направление на снижение уровня угроз, предвидение рисков и исправление этих последствий и самым важным направлением обеспечение национальной безопасности в условиях цифровой реальности. [3, с.38].

Анализируя все вышесказанное, можно выделить следующие варианты устранения проблем. Во-первых, необходимо законодательно и грамотно урегулировать данные аспекты на федеральном, региональном и на уровне субъектов, с соблюдением баланса национальной безопасности государства и национальными интересами, т.е. расширять правоприменительную практику. Но здесь тоже возникает коллизия. Расширение правоприменительной практики будет идти по пути создания специальных нормативно-правовых

1 Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" // "Российская газета", N 165, 29.07.2006,

2 Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ, 31.07.2017, N 31 (Часть I), ст. 4736

3 Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Парламентская газета", N 126-127, 03.08.2006.

актов, которые будут идентичны нормам отраслей права или же изменения и дополнения нынешнего законодательства.

Во-вторых, необходимо предпринять меры для усиления защиты конфиденциальных данных.

Также стоило бы разграничить зоны правового и нормативного регулирования, выделить их рамки. [4, с.10-11]. Это необходимо для предотвращения сговоров между картелями, для профилактики ухода бизнеса в теневой сектор экономики. И если говорить про экономику, то необходимо уменьшить административные барьеры для входа и выхода на рынок.

Для того, чтобы не был умален авторитет Российской Федерации, необходимо установить координацию между российским и международным правом.

Разработка данных мероприятий позволит снизить угрозы и предопределять наступление рисков, также защитить от информационных атак и, соответственно, исправление этих последствий и самое важное то, что будет гарантирована цифровая и информационная безопасность как государства, так и человека в целом.

Исходя из всего вышесказанного, можно с уверенностью сказать, что наше государство, как и любое другое заинтересовано в развитии цифровизации для обеспечения национальной безопасности и интересов общества, но с условием совершенствования действующего законодательства в сфере цифровых технологий для защиты персональных данных государства и человека в целом. Вышеперечисленные меры помогут стабилизировать регулирование цифровизации в условиях национальной безопасности.

Список литературы:

1. Беликова, К.М. Особенности правового регулирования цифровой интеллектуальной экономики // Закон и право. 2018. №8. - с. 26-30. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/osobennosti-pravovogo-regulirovaniya-tsifrovoy-intellektualnoy-ekonomiki/viewer> (дата обращения: 12.04.2023).
2. Плеханов, С.М. Информационная безопасность как приоритет национальной безопасности // Молодой ученый. — 2022. — № 24 (419). — С. 261-263.
3. Кириллов, П. Цифровая платформа для интернета вещей: универсальный продукт для умных производств, городов, зданий / П. Кириллов // Бизнес Территория. – 2018. - № 1. – С. 35-39.
4. Назаров, В.П., Афиногенов Д.А. Проблемы развития общей теории национальной безопасности в контексте корректировки стратегии национальной безопасности Российской Федерации // Власть. 2020. том 28. №1. С. 9-19.