Секция «Конфликты в цифровом обществе: источники, специфика, механизмы решения»

Методы обеспечения информационной безопасности в документах стратегического планирования России и США: политологический аспект

Научный руководитель – Манойло Андрей Викторович

Зеленова Владислава Антоновна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет политологии, Москва, Россия
E-mail: yavosj7@gmail.com

Обеспечение информационной безопасности является одним из приоритетных направлений государственной политики в настоящее время. Данная статья посвящена вопросам правовой защиты информации в рамках документов стратегического планирования России и США.

В сегодняшней мировой практике существуют два основных подхода к обеспечению безопасности в медиапространстве. Первый из них – это информационная безопасность, предполагающая комплексную защиту данных как внутри глобальной сети, так и вне ее. Второй – кибербезопасность, защищающая данные внутри киберсферы. Российская модель обеспечения безопасности в медиапространстве олицетворяет первый подход. Главным документом стратегического планирования в этой области является Доктрина информационной безопасности РФ (05.12.2016 г.) [1]. Развитие системы стратегического планирования в России началось относительно недавно, твердым шагом в эту сторону стало принятие федерального закона «О стратегическом планировании в Российской Федерации» (28.06.2014) [2]. В отличие от предшествующего документа в доктрине, во-первых, обозначается возможность применения спецслужбами различных государств (без конкретики) инструментов информационно-психологического воздействия, с целью дестабилизации социальной ситуации внутри страны, а также в военных целях. Во-вторых, отмечается вероятность дискредитации образа того или иного государства, в рамках формирования отрицательного политического имиджа в международном сообществе. В-третьих, обозначается возможность технологического противостояния, связанного с кражей данных, нарушения конфиденциальности и др.

В системе документов стратегического планирования также следует выделить еще один документ, который отражает официальные взгляды на способы формирования системы международной информационной безопасности: «Основы государственной политики Российской Федерации в области международной информационной безопасности» (12.04.2021) [5]. Следует отметить, что Россия предлагает консолидированное решение по проблеме международной информационной безопасности и в главном стратегическом документе Российской Федерации – Стратегии национальной безопасности (02.07.2021) [4] сказано, что одним из ключевых интересов является защита граждан от информационно-психологического воздействия, конечной целью которого является поляризация общества и достижение внутриполитической дестабилизации.

В США последним разработанным стратегическим документом в области обеспечения кибербезопасности является «Стратегия национальной кибербезопасности» (02.03.2023) [7]. Однако действительно инновационной с точки зрения подхода к обеспечению безопасного функционирования киберпространства является ее предыдущая версия 2018 года [6]. В ней говорится, что различные государства, террористические организации и преступные группировки предпринимают активные попытки хищения интеллектуальной собственности, личных данных и пытаются нанести ущерб федеральной инфраструктуре Соединенных Штатов, а также подорвать американскую демократию с помощью широкого спектра

киберинструментов, что дестабилизирует ситуацию в США и наносит вред американским национальным интересам. Также подчеркивается массовость подобных явлений, что фактически вынуждает отменить ограничения, наложенные президентской Директивой №20 (PPD-20), на кибероперации наступательного характера, наложенные администрацией Барака Обамы. Ввиду этого Минобороны США стало придерживаться стратегии «defend forward» для обеспечения безопасности в киберпространстве и удержания мирового превосходства в нем. Тезис о мировом лидерстве в глобальной сетевой среде упоминается также в стратегии объединенного киберкомандования ВС США «Завоевание и удержание превосходства в киберпространстве» (2018 год) [3]. Этот документ можно считать корректировочным этапом нормативно-правовой базы с целью выстраивания нового курса в сфере обеспечения информационной безопасности. Он указывает на цели, задачи и методы ведения боевых действий в этой среде.

В отличие от нашей стратегии недружественные страны указаны конкретно и в двух последних документах они не менялись – это Россия, Китай, Иран и КНДР. «Их безрассудное пренебрежение верховенством закона и правами человека в киберпространстве угрожает национальной безопасности и экономическому процветанию США» [7], – говорится в Стратегии 2023 года.

Таким образом, одной из важнейших государственная задач на современном этапе является обеспечение информационной безопасности как на внутригосударственном, там и на международном уровне. Как Россия, так и США принимают активное участие в вопросах кибербезопасности глобальной сети. Вышепредставленный анализ позволил провести сходства и различия методов обеспечения информационной безопасности в документах стратегического планирования России и США.

Источники и литература

1) Указ Президента РФ от 05.12.2016 No 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. No 50. Ст. 7074.

2) Федеральный закон от 28 июня 2014 г. No 172-ФЗ «О стратегическом планировании в Российской Федерации» // Собрание законодательства Российской Федерации, 2014, No 26 (часть I), ст. 3378.

3) http://pentagonus.ru/doc/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf

4) http://www.kremlin.ru/acts/bank/47046

5) http://www.scrf.gov.ru/security/information/document114/

6) https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf

7) https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf