DOI 10.35775/PSI.2025.68.3.006
УДК 316.334.3

С.В. НЕШКОВ
кандидат политических наук,
директор Центра когнитивной обороны,
помощник депутата Государственной думы ФС РФ,
Россия, г. Москва

СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ПОЛИТИЧЕСКОЙ СТАБИЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

Настоящая статья посвящена стратегиям противодействия угрозам политической стабильности в сети Интернет. Автор сосредотачивает внимание на специфике развития политических конфликтов в онлайн-среде на современном этапе, а также выявляет ключевые элементы стратегий противодействия политическим конфликтам в виртуальном пространстве, обеспечивающие их практическую эффективность.

Ключевые слова: *стратегия, политика, стабильность, Интернет, социальные сети, конфликт, нейросети, искусственный интеллект.*

Сохранение и укрепление политической стабильности в российском обществе, избежание столкновений между образующими его социальными общностями – этносами, религиозными объединениями и т.д., представляет собой одну из важнейших задач государства. Необходимость ее эффективного решения определяется тем, что в условиях политической нестабильности представляется затруднительным поддержание устойчивого положения государства в международных отношениях, а также достижение высоких результатов его экономического развития. Необходимо отметить, что опыт мировой политической практики наглядно демонстрирует, что на государственном уровне в течение достаточно длительного периода времени применяются различные инструменты сохранения и укрепления внутренних отношений различных социальных групп, в частности, межэтнических, межконфессиональных и т.д. в целях предотвращения развития конфликтных ситуаций [14. С. 3]. Между тем, несмотря на имеющийся и довольно часто апробируемый на практике арсенал противодействия антиправительственным объединениям, государство нередко проигрывает им, в результате чего нарушается внутренняя стабильность. Особенно опасным в контексте исследуемого вопроса представляется нарушение стабильности политической в силу того, что это формирует угрозу безопасности действующего политического режима и, в конечном счете, угрозу национальной безопасности. В этой связи, повышенное внимание на государственном уровне должно уделяться не только выявлению, но также нейтрализации угроз политической стабильности общества. Ввиду стремительного развития

процессов цифровизации, на сегодняшний день наибольшую опасность представляют угрозы политической стабильности, зарождающиеся в сети Интернет. Особенности социально-политической коммуникации на современном этапе обуславливают переход процессов интеграции радикально настроенных элементов общества из реального в виртуальное пространство, предоставляющее широкие возможности реализации протестной активности. Между тем, не так давно произошедшие политические события в Молдове, на Украине, а также в других государствах (Твиттер-революция, Евромайдан и т.д.) свидетельствуют о том, что именно пространство Интернета и социальных сетей на сегодняшний день представляет собой наиболее опасное поле для развития протестной политической активности. В этой связи, на государственном уровне должны разрабатываться специальные стратегии, целью которых будет противодействие политическим конфликтам, возникающим в пространстве Интернета и социальных сетей.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 4; 5; 7; 8; 9; 12; 15; 16; 17; 18; 19].

Однако проблему противодействия угрозам политической стабильности и протестной политической активности в сети Интернет нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

В рамках анализа различных исследовательских подходов к изучению стратегий противодействия протестной политической активности в Интернете, а также в пространстве социальных сетей, представляет особый интерес точка зрения А.В. Манойло относительно их специфики. В частности, автор отмечает, что указанным стратегиям не должен быть свойственен, по ряду причин, реактивный характер. К числу указанных причин относятся:

– рост уязвимости объекта реакции в рамках применения противником новых методов и ресурсов;– концентрация усилий государства на ликвидации проявлений политической агрессии в пространстве Интернета и социальных сетей в ущерб применению мер предупредительного характера;– недостаток объема доступных ресурсов для нейтрализации действий политического агрессора [10. С. 77-79].Таким образом, обобщение и анализ причин, по которым, в соответствии с точкой зрения А.В. Манойло, стратегии противодействия политическим протестам в Интернете и социальных сетях не должны иметь реактивного характера, позволяют заключить, что основная задача государства состоит не в противодействии подобного рода негативным интервенциям, а в их комплексном предупреждении. Ведь именно предупредительная активность государства в отношении такого рода негативных явлений общественно-политической действительности является залогом эффективного противодействия их возникновению в цифровой среде и, как следствие, их последующему переходу в оффлайн-пространство.Также в отношении разработки стратегий противодействия политическим протестам, возникающим в онлайн-среде, необходимо

отметить, что возможности для возникновения и развития политических угроз и, как следствие, нарушения стабильности российского государства, могут быть заложены в самих цифровых платформах. Таким образом, особой значимостью с точки зрения обретения Российской Федерацией политической стабильности в долгосрочной перспективе, обладает достижение ею технологической независимости. В свою очередь, производство новейших технологий исключительно на территории российского государства позволит устранить возможность их потенциального использования реакционно настроенными зарубежными акторами в целях нарушения политической стабильности в РФ. Некоторые исследователи, в частности, А.Ю. Маруев, в рамках анализа эффективности стратегий противодействия угрозам политической стабильности в сети Интернет, указывают на необходимость не всестороннего, а локального контроля за функционированием отдельных сегментов политического процесса. В свою очередь, облачные информационные системы, по мнению автора, должны обеспечить возможность анализа ситуаций в сфере управления политическими процессами на региональном и муниципальном уровнях. Как следствие, указанные стратегии должны включать в себя инструменты отслеживания активности лидеров общественного мнения в локальных сообществах в пространстве сети Интернет [11. С. 50].Еще одним значимым условием в рамках определения эффективных стратегий противодействия протестной политической активности в онлайн-среде является реализация контроля за производителями нейросетей, использование которых в последнее время набирает стремительную популярность. Это определяется двойственностью природы искусственного интеллекта относительно политической стабильности в обществе: он может являться как фактором, обеспечивающим ее поддержку, так и существенным препятствием к ее достижению. В свою очередь, использование искусственного интеллекта в политическом процессе может быть сопряжено с определенными рисками в случае, если:

– происходит формирование и последующее распространение информации, вводящей пользователей в заблуждение по значимым политическим вопросам (в качестве примера можно указать использование так называемых фейков накануне выборов или референдума, способных существенно подорвать доверие к выборным органам власти) [6. С. 64-69];– формирование зависимости от искусственного интеллекта в политическом процессе;– наличие алгоритмических предпочтений при использовании искусственного интеллекта, что может сформировать определенную предвзятость, например, в период реализации предвыборных кампаний.Наконец, практическое воплощение наиболее эффективных стратегий противодействия угрозам политической стабильности в Интернете и социальных сетях должно опираться на применение не только цифровых инструментов, но также на манипулятивные формы воздействия на акторов протестной активности. В свою очередь, дестабилизация лидеров протестных политических объединений позволит оказать тождественное воздействие на рядовых участников подобного рода локальных групп, нивелировать их

протестную активность. Таким образом, эффективные стратегии должны включать в себя определенные психологические приемы, позволяющие, в случае возникновения очагов протестной активности, вносить раскол в генерирующие их объединения. В частности, Н.Ю. Митюрина и Н.В. Бобков, рассуждая об информационной безопасности российского государства, указывали, что в рамках реализации подобного рода стратегий необходимо стимулировать соответствующее поведение акторов протестной активности, обеспечивающее раскол реакционно настроенных социальных групп [13. С. 37-40].Таким образом, принимая во внимание указанные параметры стратегий противодействия угрозам политической стабильности в сети Интернет, наиболее эффективные из них должны характеризоваться:– предупредительными мерами воздействия на акторов протестной активности;– импортонезависимостью российского государства в производстве цифровых технологий;– регулированием локальных сегментов политического процесса;– контролем за нейросетями;– применением инструментов психологического воздействия на акторов политического протеста.Иными словами, практически эффективным стратегиям противодействия угрозам политической стабильности в сети Интернет должен быть свойственен комплексный характер, учитывающий не только специфику пространства их применения – онлайн-среды, но также современные технологические достижения и психологические особенности акторов протестной политической коммуникации. В случае непринятия во внимание какого-либо из указанных компонентов стратегии, под угрозу будет поставлена эффективность ее практического применения.

В свою очередь, к мерам превентивного характера, иными словами, позволяющим предотвратить возможность возникновения очагов протестной политической активности в сети Интернет, следует отнести конструирование условно-нейтральных средств массовой информации, формирующих, своего рода отвлекающую повестку, позволяющую сместить фокус внимания пользователей, негативно настроенных против действующей политической власти, либо реализуемого ею курса, на иные области социальной действительности. Наряду с этим, к указанным мерам представляется возможным отнести регулярное наблюдение за контентом сети Интернет, а также пространством социальных медиа, позволяющее предупредить вспышки протестной активности, либо, по крайней мере, их неконтролируемое разрастание. Наконец, российскому государству необходимо расширять производство импортозамещающих технологий, обеспечивающих невозможность применения против России цифровых платформ, содержащих в себе угрозы, первоначально известные исключительно стране-производителю. Регулирование локальных сегментов политического процесса должно базироваться, в первую очередь, на отслеживании политической активности лидеров общественного мнения на уровне руководителей регионов и муниципальных образований. Отсутствие в их риторике протестных настроений против действующей политической власти позволит исключить возможность их вовлечения в антиправительственные объединения в сети Интернет. Контроль за нейросетями, в первую очередь, должен базироваться на ограничении возможностей

использования искусственного интеллекта в тех областях политической жизни, где его применения может стать потенциальной угрозой. Кроме того, использование возможностей искусственного интеллекта должно стать недопустимым в случаях, где его алгоритмы способны скомпрометировать политические позиции действующей власти. Наконец, применение инструментов психологического воздействия на акторов политического протеста должно быть акцентировано преимущественно на лидерах указанных социальных групп. В этой связи, целесообразным представляется практическое использование манипулятивных технологий, обеспечивающих выявление неформальных лидеров объединений в онлайн-среде, являющихся реакционно настроенными в отношении действующей политической власти и реализуемого ею курса.Подводя итоги рассмотрению вопроса о стратегиях противодействия угрозам политической стабильности в сети Интернет, необходимо отметить, что разработка указанных стратегий является оправданным шагом в современных условиях, характеризующихся стремительным развитием цифровых технологий, а также переходом политического конфликта в онлайн-пространство.Вместе с тем, реализация российским государством в рамках стратегий противодействия угрозам политической стабильности в сети Интернет предупредительных действий в отношении акторов протестной активности, достижение им технологической импортонезависимости, регулирование локальных сегментов политического процесса, осуществление контроля за нейросетями, а также применение инструментов психологического воздействия на акторов политического протеста в комплексе обеспечивает эффективность их практического применения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А.** Цели и задачи России в специальной военной операции на Украине и в гибридной войне с коллективным Западом // Вопросы политологии. 2024. № 5.
2. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
3. **Апарин С.В., Суховерхова А.А., Григорян Д.К.** Цифровые войны: роль черного пиара // Вопросы национальных и федеративных отношений. 2025. № 1.
4. **Буданцев Э.В.** Информационная безопасность как фактор стратегического суверенитета на пространстве Большой Евразии // Евразийский Союз: вопросы международных отношений. 2024. № 6.
5. **Волох О.В., Костюков В.А.** Влияние средств массовой информации США на формирование общественного мнения в России // Вопросы политологии. 2023. № 11-1.
6. **Джибилова Е.Г., Побываев Н.С.** Анализ российского и зарубежного опыта применения ChatGPT и искусственного интеллекта в политике и социальной сфере // Социально-гуманитарные знания. 2024. № 1.

7. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
8. **Егорова М.Р.** Информационная война как угроза национальной безопасности страны в современном мире на примере конфликтов XXI века // Евразийский Союз: вопросы международных отношений. 2023. № 7.
9. **Иващенко З.С., Васильченко О.В., Григорян Д.К., Малявина А.Б.** Фейковые новости о ходе проведения Специальной военной операции как угроза национальной безопасности Российской Федерации // Евразийский Союз: вопросы международных отношений. 2024. № 9.
10. **Манойло А.В.** Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта / Материалы V Международной научно-практической конференции «Информационные технологии и безопасность». 2005. № 8.
11. **Маруев А.Ю.** Информационная безопасность России и основы организации информационного противоборства // Проблемный анализ и государственно-управленческое проектирование. 2010. Т. 3. № 1.
12. **Медведева В.К., Медведев Н.П.** Информационная политика государства: современные вызовы и направления совершенствования (Часть 1) // Вопросы политологии. 2025. № 1.
13. **Митюрина Н.Ю., Бобков Н.В.** Информационная составляющая экономической безопасности России // Информационная безопасность регионов. 2011. № 1 (8).
14. **Семченков А.С.** Противодействие современным угрозам политической стабильности в системе обеспечения национальной безопасности России: дисс. док. политич. наук. М., 2012.
15. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
16. **Степанов С.А., Иванова Е.А.** Социальные сети как поле информационных войн в современной политике // Вопросы политологии. 2023. № 11-2.
17. **Сулейманов Э.А.** Реализация информационной политики государства в современных условиях // Евразийский Союз: вопросы международных отношений. 2024. № 2.
18. **Уртаева Э.Б.** Геополитические аспекты информационных войн и их влияние на политические процессы // Вопросы политологии. 2024. № 3.
19. **Шавлохов А.К., Максименко Д.И.** Актуальные вопросы обеспечения информационной безопасности населения в условиях военных конфликтов: правовые аспекты // Региональное и муниципальное управление: вопросы политики, экономики и права. 2023. № 3.

S.V. NESHKOV
Candidate of political sciences,
director of the Center for cognitive defense,
assistant to the deputy of the State Duma of the Federal Assembly of the Russian Federation,
Moscow, Russia

STRATEGIES FOR COUNTERING THREATS TO POLITICAL STABILITY ON THE INTERNET

This article is devoted to strategies for countering threats to political stability on the Internet. The author focuses on the specifics of the development of political conflicts in the online environment at the present stage, and also identifies key elements of strategies for countering political conflicts in the virtual space, ensuring their practical effectiveness.

Key words: *strategy, politics, stability, Internet, social networks, conflict, neural networks, artificial intelligence.*