

Секция «24.14 Технологии искусственного интеллекта в современной политике»

Эскалация киберугроз и оборонительный потенциал ИИ: новый контур безопасности.

Научный руководитель – Пятибратов Иван Сергеевич

Киева Анастасия Николаевна

Студент (бакалавр)

Финансовый университет, Факультет социальных наук и массовых коммуникаций,
Москва, Россия

E-mail: anassttassia@yandex.ru

В современном государственном управлении наблюдается переход от ситуативного к непрерывному стратегическому процессу формирования общественного мнения и контроля над информационным пространством. Спектр задач политических коммуникаций существенно расширился, охватывая как внутренние цели, такие как популяризация национальных проектов и государственных инициатив, так и внешние – формирование благоприятного международного имиджа и консолидация социума на основе фундаментальных ценностей. В условиях фрагментации внимания аудитории и беспрецедентной скорости распространения информации в цифровой среде традиционные подходы к организации подобных кампаний демонстрируют снижение эффективности.

Искусственный интеллект (ИИ) выступает в качестве катализатора трансформации политических коммуникаций, обеспечивая их адаптивность, высокую степень таргетированности и максимальное воздействие на целевую аудиторию. Посредством глубинного анализа данных, извлекаемых из социальных сетей, медиапространства и иных цифровых следов, ИИ позволяет осуществлять идентификацию ключевых социальных групп, строить их детализированные психографические и поведенческие профили, а также прогнозировать их реакцию на различные нарративы. Данный подход гарантирует точечное информационное воздействие и оптимальное распределение ресурсов независимо от масштаба и характера проводимой кампании.

Более того, искусственный интеллект способствует формированию "эхо-камер", усиливая естественную склонность людей к "мотивированному мышлению", поиску подтверждений своим убеждениям и игнорированию противоречащей информации. Социальные сети и ИИ-алгоритмы активно используют это, создавая персонализированные "информационные пузыри". В таких пузырях каждое подтверждение взглядов вызывает положительные эмоции, укрепляя существующие убеждения и снижая открытость к другим мнениям [1].

Кроме того, ИИ может манипулировать пользователями, используя когнитивные искажения. Например, "эффект якоря" устанавливает первоначальную информацию как точку отсчета, а "эффект фрейминга" влияет на восприятие смысла в зависимости от подачи информации [2].

Также ИИ применяется политтехнологами не только для создания ложного контента, но и для размывания реальности с целью раскола общества. Так, согласно Politico, США рассматривают возможность организации кампаний по дезинформации населения Гренландии с помощью ИИ для формирования положительного общественного мнения о вопросе присоединения острова к США путём референдума [3].

Если подобные кампании нацелены на достижение конкретных геополитических целей, то использование технологий ИИ больше не ограничено одной лишь сферой информационного воздействия. Технология становится универсальным инструментом ведения войны

— от фабрикации общественного мнения до непосредственного участия в боевых операциях. Так, согласно Reuters, Применение Пентагоном искусственного интеллекта Anthropic, в частности инструментов Claude во время атаки на Иран вызывает ряд вопросов, особенно в свете недавних событий. За день до операции США объявили Anthropic угрозой для цепочки поставок, что фактически приравнивает ее к угрозе национальной безопасности, а президент Трамп даже дал указание прекратить сотрудничество с компанией. Несмотря на это, военные использовали ее технологии. Reuters не смог установить точный характер использования ИИ в данной операции. Известно, что Anthropic активно сотрудничает с разведывательным сообществом и вооруженными силами, и благодаря партнерству с Amazon она стала первой ИИ-компанией, допущенной к работе с секретной информацией [4].

Таким образом, искусственный интеллект является универсальным инструментом, который может быть использован как для проведения информационных атак, так и для ведения боевых действий. Злоумышленники применяют ИИ для автоматизации своих операций, что позволяет им осуществлять более сложные и масштабные кибератаки с минимальным человеческим участием. Данная тенденция к автоматизации и увеличению масштабов киберугроз со стороны противников ставит перед системами национальной и информационной безопасности беспрецедентный вызов. Логичным и неизбежным ответом на него является внедрение технологий ИИ в оборонительные стратегии.

Источники и литература

- 1) Пьянов М.П. Эхо-камера как инструмент политического консалтинга в цифровой среде: новые формы сегментации электората // Право и политика. 2025. № 12. URL: <https://cyberleninka.ru/article/n/eho-kamera-kak-instrument-politicheskogo-konsaltinga-v-tsifrovoy-srede-novye-formy-segmentatsii-elektorata> (дата обращения: 08.03.2026).
- 2) Рябова И. «Якоря» и «рамки»: как «эффект привязки» и фрейминг влияют на принятие решений // ECONS.ONLINE. 10.02.2023. URL: <https://econs.online/articles/coffee-break/yakorya-i-ramki-kak-effekt-privyazki-i-freyming-vliyayut-na-prinyatie-resheniya/> (дата обращения: 08.03.2026).
- 3) Cheslow D. Trump wants Greenlanders to join the US. His comments are making that harder // Politico. 14.01.2026. URL: <https://www.politico.com/news/2026/01/14/trump-greenland-residents-independence-00726696> (дата обращения: 08.03.2026).
- 4) Seetharaman D., Stone M. US uses Anthropic AI, B-2 bombers and suicide drones in Iran strikes // Reuters. 01.03.2026. URL: <https://www.reuters.com/business/aerospace-defense/us-deploys-suicide-drones-tomahawk-missiles-iran-strikes-2026-03-01/> (дата обращения: 08.03.2026).