Выписка из Рекомендаций по противодействию идеологии терроризма
в информационном пространстве в условиях проведения
специальной военной операции на Украине

В современных условиях информационное пространство становится важнейшей ареной для распространения идеологии терроризма, которая представляет собой одну из главных угроз безопасности общества и государства. Террористические организации активно используют цифровые платформы для вербовки, пропаганды, координации действий и распространения дезинформации. Сеть Интернет является одним из основных источников экстремизма и терроризма как одно из средств коммуникации, используемых для пропаганды деструктивной идеологии, привлечения новых членов в ряды экстремистских и террористических организаций, а также организации и координации совершения преступлений.

Особую озабоченность вызывает активное использование террористическими структурами генеративных моделей искусственного интеллекта (далее – ИИ) и технологий синтетических медиа. Современные дипфейки, модели клонирования голоса, имитация переписки и автоматизированная генерация «новостных» материалов позволяют создавать эффект подлинности, значительно усложняя работу по верификации данных. Такие технологии применяются для подмены официальных сообщений, создания провокационных видеоматериалов, распространения ложных свидетельств «очевидцев» и формирования эмоционального давления на аудиторию.

Основные механизмы информационного воздействия остаются устойчивыми, однако их технический уровень растёт. Среди наиболее распространённых инструментов: намеренная дезинформация с опорой на авторитетность поддельные источников; генеративные дипфейки высокого качества; подмена официальных документов и имитация сообщений от органов власти; эксплуатация эффекта первичного восприятия; массовое тиражирование контента через боты и автоматизированные системы.

Совместное действие этих инструментов формирует замкнутый цикл, в котором сложность технологий сочетается с низкой медиаграмотностью отдельных групп аудитории. Особенно уязвима молодёжь – наиболее активные пользователи цифровой среды, чаще сталкивающиеся с манипулятивным контентом.

В связи с этим ключевыми задачами на ближайший год становятся:

укрепление цифровой гигиены граждан, развитие привычек безопасного поведения в сети;

повышение медиаграмотности, включая умение распознавать манипуляции, дипфейки и псевдоновости;

внедрение современных практик работы с данными, включая обучение алгоритмической прозрачности и критическому восприятию информации;

масштабирование профилактических мер, направленных на раннее выявление вовлекающих воздействий и снижение восприимчивости к радикальные идеям;

развитие механизмов мониторинга информационных угроз, связанных с использованием ИИ, и совершенствование межведомственного взаимодействий в этой сфере.

Настоящие рекомендации направлены на создание устойчивой системы противодействия идеологии терроризма в цифровой среде, учитывающей современные технологические вызовы и необходимость формирования у граждан навыков ответственного и безопасного поведения онлайн.

Особое внимание предлагается уделить следующим направлениям работы:

1. *Производство и распространение антитеррористического контента.*

1.1. Создание просветительского контента (обеспечивать высокое качество просветительского контента, ориентированного на нивелирование вербовочных и идеологических механизмов радикализации; учитывать реальные условия, в которых ведётся информационная работа).

1.2. Координация с профильными структурами (учитывать и трансформировать в практики рекомендации Национального антитеррористического комитета (№ 11/п/3-1856, ноябрь 2022 г.) и региональных антитеррористических комиссий; обеспечить обмен шаблонами, чек-листами и примерными сценариями для социальных сетей и образовательных программ.

1.3. Интеграция в популярный контент (организовать долгосрочное взаимодействие с локальными и региональными медийными лидерами (включая блогеров, Telegram- каналы, паблики).

1.4. Формализовать сотрудничество с некоммерческими организациями, профильными институтами (институты развития интернета, образовательные центры, поисковые и патриотические организации) через меморандумы и реестры лучших практик:

АНО «Институт развития интернета» (social-ads-feedback@iri.center);

АНО «Диалог Регионы» (через Центр управления регионом г. Санкт-Петербург);

ФГБУ «Дом народов России» (https://domnarodov.ru);

Федеральный проект «Без срока давности» (https://безсрокадавности.рф);

ООГПО «Российское общество «Знание» (https://znanierussia.ru);

ООД «Поисковое Движение России» (https://rf-poisk.ru).

2. *Проведение информационно-разъяснительных мероприятий с населением.*

2.1. Расшифровка методов внешнего влияния (в материалах для населения и школ чётко разъяснять современные методы информационно-психологических операций (включая кейсы по фейкам, манипуляциям, вербовке), демонстрировать алгоритмы воздействия и способы защиты).

2.2. Каналы сообщения о деструктиве (пропагандировать использование единой электронной приёмной и форм обратной связи Роскомнадзора/централизованных реестров для направления материалов и блокировок; обеспечить инструкции для граждан и образовательных организаций по заполнению форм (URL, скрин-архивы).

2.3. Медиаграмотность и кибергигиена (внедрять обязательные модули медиаграмотности и кибергигиены в программы для школьников и студентов (практики проверки источников, распознавания дипфейков, правила поведения в тематических чатах); использовать игровые механики и адаптивные курсы (платформы-симуляторы, педагогические игры, в том числе через расширение функционала уже имеющихся решений, таких как «Урок цифры»).

2.4. Дипфейки и ИИ-риски (включить отдельную секцию по распознаванию дипфейков и управлению ИИ-рисками: методы проверки (метаданные, обратный поиск по кадрам, инструменты верификации), алгоритмы реагирования при обнаружении потенциально опасных материалов).

2.5. Юридическая осведомленность (информировать о правовых последствиях совершения преступлений, связанных с диверсиями, передачей сведений иностранным разведкам и иными действиями, подпадающими под уголовную ответственность; доводить практические инструкции о порядке действий при обнаружении призывов к преступлениям.

2.6. Работа с семьями и педагогами (обучать педагогов и родителей распознавать признаки вовлечения и направлять по маршрутам поддержки; формировать «родительские гайды» и чек-листы).

3. *Мониторинг информационного пространства и поддержка кибердружин.*

3.1. Гибридный мониторинг (развернуть национальную методику мониторинга интернет-пространства, сочетающие автоматические инструменты (ИИ – классификация, фильтрация по признакам) и обученные региональные команды (добровольцы, специалисты); отдельные правила для выявления и эскалации контента, угрожающего объектам инфраструктуры).

3.2. Защита персонала и волонтеров (обеспечить психологическую поддержку, периодическую ротацию и доступ к квалифицированной помощи для тех, кто постоянно задействован в мониторинге (кибердружины и волонтёры).

3.3. Обучение работе с ИИ-инструментами (совместно с профильными подразделениями разработать курсы и практикумы по работе добровольцев и операторов с ИИ-наборов инструментов (тегирование, верификация, приоритезация сигналов).

3.4. Процедуры передачи материалов в правоохранительные органы (установить регламент направлений деструктивного контента в правоохранительные органы, Роскомнадзор, Росмолодежь и региональные антитеррористические комиссии через единые формы, включая: сроки реакции, каналы обратной связи:

https://rkn.gov.ru/treatments/ask-question (общая форма для материалов из средств массовой информации, сети Интернет и другие);

https://eais.rkn.gov.ru/feedback (только для материалов из сети Интернет);

https://fadm.gov.ru/feedback/contact-agency (общая форма).

3.5. Учет результатов мониторингов в образовании (включать результаты мониторингов среди студенчества в план профилактической работы учебных заведений для раннего выявления факторов радикализации и корректировки учебных программ).

4. *Продвижение героических образов и позитивных повествований* (поддерживать и масштабировать проекты по увековечиванию памяти участников современных конфликтов (муралы, мемориальные объекты), в том числе с участием молодёжи; сочетать художественную среду и образовательные мероприятия для формирования устойчивых позитивных нарративов).

5. *Реализация мероприятий в сфере государственной политики для детей и молодежи, способствующих формированию социально ответственной личности.*

5.1. Контент для детей и молодежи (создавать и распространять контент, продвигающий традиционные и гражданские ценности, в адаптированных форматах для разных возрастных групп; внедрять механизмы сертификации «детского» контента для крупных платформ).

5.2. Участие в патриотических и волонтерских проектах (обеспечить системны возможности вовлечения детей и молодежи в патриотические и общественно-полезные программы (включая туризм, волонтёрство, проекты «малой родины»).

5.3. Выявление и поддержка талантов (развивать инфраструктуру для выявления талантов, предоставления грантов и площадок для самореализации (молодежные центры, конкурсы проектов).

5.4. Доступность дополнительного образования (увеличить доступность дополнительного образования, в том числе по цифровым навыкам, медиаграмотности и кибербезопасности; поощрять партнерства с платформами и вузами).

7. *Технологические и правовые меры для платформ* (наличие «детских/подростковых режимы» (с отдельной логикой рекомендаций и ограниченным функционалом);

прозрачность алгоритмов рекомендаций для несовершеннолетних; информирование родителей о «детских» тарифах.

Интеграция предложенных мер позволит обеспечить сбалансированную стратегию: сочетание проактивного производства качественного просветительского контента, современных технических ограничений на платформах, обучения и медиаграмотности, оперативного мониторинга.