МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра политических наук

«Государственная политика противодействия экстремизму в социальных сетях»

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ ДИССЕРТАЦИОННОЙ РАБОТЫ

Студента 2 курса 264 группы
направления (специальности) 41.04.04 «Политология»
юридического факультета
Гоман Александра Павловича

Научный руководитель

_____	_____	С.В Дубровская
должность, уч. степень, уч. звание	дата, подпись	инициалы, фамилия

Заведующий кафедрой

_____	_____	А.А Вилков
должность, уч. степень, уч. звание	дата, подпись	инициалы, фамилия

Саратов 2025 г.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность выбранной темы. Экстремизм в онлайн-среде является одной из наиболее актуальных проблем современного общества. Быстрое развитие информационно-коммуникационных технологий привело к тому, что экстремистские организации и отдельные радикально настроенные лица получили доступ к широким возможностям распространения своей идеологии через интернет. Социальные сети, видеохостинги, мессенджеры и тематические форумы стали ключевыми платформами, используемыми экстремистами для вербовки сторонников, координации деятельности и пропаганды деструктивных идей. В связи с этим возникает необходимость детального изучения особенностей интернет-экстремизма, его разновидностей, а также государственных мер по противодействию данной угрозе.

Для Российской Федерации, учитывая масштаб цифровизации и активное вовлечение молодежи в сетевые коммуникации, задача противодействия экстремизму в социальных сетях приобретает не просто актуальное, но приоритетное значение. При этом переход от декларативных мер к конкретным показателям эффективности, обозначенный в новой редакции Стратегии, требует осмысления и научного анализа.

Цель исследования. Проанализировать специфику форм, механизмов распространения экстремизма в интернет-пространстве (социальные сети). Дать оценку эффективности существующих мер противодействия на государственном уровне.

Для достижения указанной цели в рамках исследования необходимо решить следующие ***задачи***:

1. Изучить теоретические основы экстремизма, его понятие, виды и особенности в сети Интернет.

2. Проанализировать роль основных социальных сетей в распространении экстремистской идеологии.

3. Исследовать масштабы проявлений экстремизма в интернет-пространстве России.

4. Выявить ключевые проблемы и вызовы, с которыми сталкиваются государственные органы при реализации мер по противодействию экстремизму в социальных сетях.

5. Оценить перспективы развития государственных стратегий и предложить возможные пути совершенствования мер противодействия интернет-экстремизму.

Материалом исследования стали научные статьи, монографии, доклады международных организаций, статистические данные о масштабах интернет-экстремизма, а также судебные решения по делам, связанным с распространением экстремистского контента в социальных сетях.

Структура работы определена задачами исследования и логикой раскрытия темы. Работа состоит из введения, двух глав, заключения, списка литературы и приложений. В первой главе рассматриваются теоретико-концептуальный анализ понятия экстремизма его виды и особенности, а также роль социальных сетей в распространении экстремистской идеологии. Во второй главе рассматриваются условия эффективности государственных мер противодействия экстремизму в социальных сетях. В рамках второй главы проводится анализ масштабов проявлений экстремизма в интернете России, выявляются проблемы и вызовы при реализации государственных стратегий противодействия экстремизму в социальных сетях и рассматриваются возможные перспективы развития государственных мер противодействия экстремизму.

Научная новизна работы заключается в разработке целостной модели анализа и противодействия интернет-экстремизму в социальных сетях, основанной на синтезе правовых, технологических и социокультурных компонентов. Системно охарактеризованы формы и каналы распространения экстремистского контента в онлайн-среде с акцентом на особенности алгоритмической персонализации и вовлекающих механизмов социальных

сетей. Обоснована необходимость перехода от фрагментарных правовых и технических мер к комплексной стратегии, включающей правовое регулирование, цифровую просветительскую политику и социальное партнёрство. Выдвинуты предложения по совершенствованию государственной политики, основанные на результатах контент-анализа, экспертной оценки и сопоставлении с международной практикой.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы, сформулированы ее цель и задачи, научная новизна, практическая значимость и основные положения, выносимые на защиту.

Первая глава посвящена теоретико-концептуальному анализу понятия экстремизма, его видов и особенностей, а также выявлении роли социальных сетей в распространении экстремистской идеологии.

Важно отметить, что проведённый анализ позволил установить, что экстремизм в онлайн-среде представляет собой сложное и многогранное явление, отличающееся высокой степенью динамичности и адаптивности к современным условиям цифрового взаимодействия. В ходе исследования было выявлено, что интернет-пространство предоставляет экстремистским группам широкие возможности для распространения своих идей, мобилизации сторонников и координации действий, что обусловлено спецификой виртуальной коммуникации, её доступностью, анонимностью и скоростью распространения информации.

Современные экстремистские движения активно используют социальные сети, форумы, мессенджеры и видеохостинги для продвижения своей идеологии, рекрутинга и пропаганды.

Особенности интернет-экстремизма заключаются в том, что он выходит за рамки традиционных форм насильственного радикализма и включает в себя информационно-психологическое воздействие, манипуляцию общественным мнением, распространение дезинформации и

конструирование альтернативной реальности. Виды интернет-экстремизма разнообразны и включают религиозный, политический, этнический, националистический и другие формы радикализма, что требует дифференцированного подхода к их анализу и противодействию.

Роль социальных сетей в распространении экстремистской идеологии заключается в их способности объединять единомышленников, обеспечивать доступ к радикальному контенту и стимулировать вовлечённость пользователей в экстремистскую деятельность.

Особую угрозу представляет алгоритмическая персонализация контента, способствующая созданию информационных пузырей и радикализации аудитории. В этой связи социальные сети становятся не только площадками для коммуникации, но и инструментами, влияющими на формирование взглядов и убеждений пользователей.

Анализ масштабов проявления экстремизма в интернет-пространстве России показывает, что с развитием цифровых технологий количество случаев выявления экстремистской активности в сети увеличивается, а методы распространения радикальной идеологии становятся всё более изощрёнными. Государственные органы сталкиваются с рядом проблем в процессе противодействия интернет-экстремизму, включая техническую сложность идентификации нарушителей, трудности правоприменения в транснациональной среде, а также балансирование между защитой прав граждан на свободу выражения мнений и необходимостью обеспечения национальной безопасности.

Перспективы развития государственных стратегий в области противодействия интернет-экстремизму предполагают совершенствование законодательства, усиление сотрудничества с технологическими компаниями, развитие алгоритмических методов выявления и блокировки экстремистского контента, а также повышение уровня цифровой грамотности населения. Важным направлением является разработка комплексных мер профилактики, включающих образовательные программы, направленные на

формирование критического мышления и устойчивости к деструктивному информационному воздействию. Успешная реализация указанных мер требует координации усилий государственных институтов, международных организаций, гражданского общества и цифровых платформ.

Проведённый анализ показал, что социальные сети играют ключевую роль в распространении экстремистской идеологии за счёт специфики их функционирования: алгоритмической персонализации контента, слабой модерации, доступности групповой коммуникации и возможностей вербовки. Социальные платформы активно используются как инструмент радикализации, в том числе через закрытые сообщества, тематические паблики и комментарии к публикациям. Особенно опасным является использование визуального контента (мемов, видео) и так называемой «языковой игры» — скрытой терминологии, понятной только внутри радикальных сообществ. Таким образом, социальные сети не только транслируют, но и активно формируют экстремистские установки у пользователей.

Во второй главе проводится анализ масштабов проявлений экстремизма в интернете России, выявляются проблемы и вызовы при реализации государственных стратегий противодействия экстремизму в социальных сетях и рассматриваются возможные перспективы развития государственных мер противодействия экстремизму.

В ходе анализа масштабов проявления экстремистской активности в российских социальных сетях установлен рост угроз, обусловленных как глобальными технологическими трендами, так и внутренними социальными факторами. Государственные меры, направленные на противодействие этому явлению, уже продемонстрировали определенную результативность, однако сохраняется целый ряд проблем. В числе наиболее острых:

- фрагментарность правового регулирования;
- техническая неоснащенность некоторых государственных структур;
- недостаточная вовлеченность гражданского общества;

- слабая координация между различными субъектами профилактики.

Перспективы развития государственных мер противодействия экстремизму в социальных сетях связаны с комплексным подходом, основанным на сочетании правовых, организационных и технических механизмов. Одним из важнейших направлений в этой сфере становится повышение информированности населения о признаках экстремизма, а также создание эффективной системы взаимодействия граждан с органами государственной власти [5, с. 73].

Распространение информации о том, как идентифицировать экстремистскую деятельность, формирование у граждан устойчивой негативной установки к экстремистским идеологиям и поощрение их участия в выявлении подозрительных публикаций и аккаунтов может значительно повысить эффективность борьбы с экстремизмом в онлайн-пространстве. Такие меры позволяют не только предупреждать преступления, но и формировать у общества общее неприятие идеологии ненависти, агрессии и радикализма.

Важное место в системе противодействия занимает блокировка доступа к экстремистским сайтам и иным информационным ресурсам. Для реализации этого направления на практике требуется активное использование программных решений, фильтрации контента, машинного обучения и алгоритмов искусственного интеллекта, позволяющих эффективно выявлять и блокировать экстремистские материалы. Наряду с этим государственные органы обязаны обеспечивать развитие и продвижение социально-полезного контента, альтернативного экстремистской пропаганде. Создание и популяризация позитивной повестки, основанной на ценностях толерантности, гуманизма, взаимного уважения, способствует ослаблению влияния деструктивных идеологий на молодежную аудиторию.

Перспективным направлением является организация просветительских мероприятий для различных возрастных и социальных групп, особенно школьников и студентов. Такие инициативы должны быть направлены на

формирование правовой культуры, развитие критического мышления, понимание природы экстремизма и его последствий. Особое значение имеет сотрудничество с общественными и молодежными организациями, которые могут эффективно транслировать антитеррористическую и антиэкстремистскую повестку в своем информационном пространстве. Вовлечение гражданского общества в противодействие экстремизму в социальных сетях способствует формированию горизонтальных связей, обмену опытом и расширению спектра мероприятий, направленных на профилактику и предупреждение угроз.

Не менее актуальной задачей является разработка и распространение контраргументов, направленных на деконструкцию экстремистских нарративов. Такие контраргументы должны быть построены на основе глубокого анализа идеологических установок и риторики экстремистских групп, с учетом психологических, социокультурных и лингвистических особенностей целевой аудитории. Разработка таких стратегий требует участия квалифицированных специалистов в области лингвистики, психологии, политологии и социологии [5, с. 73].

Кроме того, перспективным направлением является создание безопасных онлайн-пространств, в которых пользователи могли бы открыто обсуждать угрозы экстремизма, делиться опытом и получать поддержку. Такие площадки могут быть организованы в виде форумов, чатов, просветительских каналов и специализированных образовательных ресурсов. Важно, чтобы подобные пространства были модераторски защищены от вмешательства со стороны экстремистских элементов и использовались в том числе как инструменты раннего выявления опасных тенденций и потребностей в профилактическом вмешательстве.

С технической точки зрения, развитие методов автоматического мониторинга и анализа данных представляет собой одно из ключевых направлений государственной политики. Алгоритмы машинного обучения, технологии обработки естественного языка, методы контент-анализа и

инструменты мониторинга социальных сетей дают возможность быстро выявлять и реагировать на признаки экстремистской активности. Такие технологии способны анализировать текст, изображения, видео, распознавать экстремистские символы, ключевые фразы и подозрительную активность. Интеграция этих решений в общенациональную систему противодействия экстремизму значительно расширяет возможности оперативного реагирования правоохранительных органов.

Организационно данные меры должны быть обеспечены созданием устойчивой структуры мониторинга, включающей команды специалистов, разработку стратегий и процедур реагирования, системы отчетности и контроля эффективности. Необходимо формирование единой национальной платформы мониторинга, сочетающей автоматические и ручные методы анализа, а также обеспечение взаимодействия с операторами связи, провайдерами и платформами социальных сетей. В этом контексте особое значение приобретает обучение сотрудников органов внутренних дел навыкам выявления, анализа и документирования экстремистского контента в цифровой среде [5, с. 75].

Для точного определения экстремистского характера информации используются специализированные методы, включая лингвистическую экспертизу, анализ визуального и текстового контента, а также поведенческих моделей пользователей. Лингвистический анализ позволяет выявлять риторические приемы, типичную лексику, синтаксические конструкции, отражающие экстремистскую идеологию. Такой подход помогает не только установить сам факт распространения экстремистского контента, но и определить его адресность и потенциальное воздействие на конкретные группы пользователей.

Практика документирования преступлений экстремистской направленности в интернете требует учета ряда специфических факторов. Это, в частности:

1. Оперативность получения данных, характер среды (цифровой формат).

2. Возможность утраты информации.

3. Необходимость постоянного привлечения компетентных специалистов.

Важно учитывать и технические аспекты – доступ к оборудованию и инфокоммуникационным объектам операторов связи, которые часто становятся ключевыми источниками оперативно значимых данных. Выстраивание эффективной системы взаимодействия с провайдерами и платформами социальных сетей позволяет своевременно получать и анализировать данные, необходимые для возбуждения дел и привлечения к ответственности лиц, причастных к распространению экстремистских идей.

Таким образом, перспективы развития мер по противодействию экстремизму в социальных сетях заключаются в комплексной цифровой трансформации соответствующих направлений государственной политики. Эффективное сочетание технических решений, организационных процедур, просветительских стратегий и механизмов гражданского участия формирует устойчивую основу для минимизации угроз, связанных с экстремизмом в информационном пространстве.

Для повышения эффективности противодействия экстремистской деятельности в социальных сетях и цифровой среде в целом необходимо реализовать комплекс системных мер, направленных как на оперативное выявление и пресечение противоправных действий, так и на профилактику вовлечения граждан, особенно молодежи, в экстремистские сообщества.

Важной задачей остается формирование единой национальной базы экстремистских материалов, включающей в себя фото- и видеоматериалы, текстовый контент и прочие формы цифровых данных. Такая база позволит существенно сократить время реагирования на угрозы и повысить эффективность анализа и блокировки опасного контента. Данная инициатива требует четкого нормативного закрепления, а также создания защищенной

информационной инфраструктуры, обеспечивающей оперативный доступ к информации для уполномоченных органов.

Следует также расширить зону мониторинга за счет включения в наблюдение различных онлайн-форумов и сайтов, являющиеся русскоязычными аналогами уже запрещенных в стране зарубежных платформ Reddit и 4chan [5, с. 76].

Эти ресурсы нередко становятся площадками для распространения маргинальных и радикальных идей, особенно в анонимном формате, что значительно осложняет выявление и привлечение к ответственности правонарушителей. Систематическое отслеживание таких площадок с последующим аналитическим сопровождением позволит выявлять очаги зарождения экстремистской риторики и оперативно реагировать на них.

Важнейшим направлением развития противодействия киберэкстремизму является создание специализированной государственной службы или целевой группы, состоящей из экспертов в области:

- информационных технологий;
- кибербезопасности;
- правоохранительной деятельности.

Такой орган должен обладать высоким уровнем технической оснащенности, независимым кадровым составом и доступом к современным методам цифрового анализа.

Важной задачей станет не только нейтрализация уже действующих субъектов экстремистской активности, но и выявление лиц из так называемой "группы риска", то есть потенциальных потребителей и распространителей радикального контента. Работа такой службы должна основываться на принципах межведомственного взаимодействия и постоянной координации с федеральными органами исполнительной власти, интернет-провайдерами, цифровыми корпорациями, а также представителями гражданского общества.

Противодействие экстремизму в социальных сетях невозможно представить без привлечения к этой деятельности научного, образовательного, культурного и религиозного сообщества. Представители этих сфер обладают значительным авторитетом в своей аудитории и могут эффективно выполнять задачи по просвещению, профилактике и выработке устойчивого неприятия радикальных идей. Их участие в разработке стратегий информационного противодействия экстремизму и последовательной реализации этих программ способно оказать долговременное воздействие на снижение уровня вовлеченности граждан в экстремистскую среду.

Особую актуальность приобретает развитие международного сотрудничества в данной области. Сложность экстремистских сетей, их децентрализованный характер и постоянное использование трансграничных технологий требует активного обмена данными между правоохранительными органами разных стран, унификации правовых подходов и использования зарубежного опыта в части выявления и нейтрализации экстремистского контента в сети.

Необходимо также признать существующие проблемы технического и кадрового характера, с которыми сталкиваются органы внутренних дел. Современные радикальные движения в интернете:

- обладают высоким уровнем цифровой грамотности;
- используют новейшие технологические решения;
- активно противодействуют методам оперативно-розыскной деятельности.

Это обстоятельство требует постоянного обновления технических средств, повышения уровня профессиональной подготовки сотрудников, разработки инновационных методов мониторинга и анализа сетевых угроз. Важно, чтобы работа по противодействию киберэкстремизму велась не эпизодически, а на постоянной основе с четким планированием, адекватным

ресурсным обеспечением и широкой координацией между всеми заинтересованными субъектами.

Таким образом, перспективы развития государственной политики в сфере противодействия экстремизму в социальных сетях связаны прежде всего с модернизацией и институционализацией имеющихся механизмов, созданием новых высокотехнологичных структур, а также включением в эту деятельность более широкого круга акторов, включая представителей общества и международных партнеров. Эффективность государственной политики будет напрямую зависеть от способности адаптироваться к динамично изменяющейся цифровой среде, разрабатывать долгосрочные меры профилактики и обеспечивать высокую степень институционального доверия со стороны общества.

ЗАКЛЮЧЕНИЕ

Во-первых, теоретический анализ экстремизма в онлайн-среде подтвердил, что интернет-экстремизм представляет собой качественно новое явление, отличающееся высокой адаптивностью, анонимностью и трансграничностью. Были выделены его основные виды (политический, религиозный, националистический, молодежный) и механизмы распространения, включая алгоритмическую персонализацию контента и создание "информационных пузырей".

Во-вторых, подтвердилась ключевая роль социальных сетей в распространении экстремистской идеологии. Платформы, такие как ВКонтакте, Telegram и TikTok, используются для вербовки, координации действий и пропаганды, выявлено, что каждая из платформ обладает своими рисками: от прямой агитации и вербовки до манипулятивного контента, замаскированного под развлекательный или социальный, а их алгоритмы непреднамеренно усиливают радикализацию пользователей.

В-третьих, статистика МВД свидетельствует о росте преступлений экстремистской направленности в цифровой среде, особенно среди

молодежи. Наблюдается увеличение числа случаев использования интернета для координации экстремистской деятельности, что подчеркивает необходимость усиления мониторинга и регулирования. Государственные меры, такие как блокировка ресурсов и удаление контента, показывают определенную эффективность, но сталкиваются с проблемами оперативности и адаптивности экстремистских групп, что говорит о необходимости перехода от реактивных к превентивным мерам.

В-четвертых, в ходе исследования выяснилось, что основными проблемами государственных стратегий являются фрагментарность правового регулирования, техническая сложность выявления контента, недостаточная координация между ведомствами и ограниченность юрисдикции в отношении зарубежных платформ.

В ходе размышления о перспективах развития стратегии противодействия экстремизму был проведён сравнительный анализ редакций Стратегии национальной политики противодействия экстремизму 2014 и 2023 годов. В ходе которого мы смогли установить, что в обновлённой версии сделан акцент на профилактику, межведомственное сотрудничество, развитие цифровых инструментов и ориентацию на конкретные результаты. Вместе с тем, предлагаются меры совершенствования, включая повышение прозрачности механизмов блокировки контента, внедрение алгоритмов на основе ИИ, а также правовое закрепление понятий, применимых к сетевому экстремизму, что позволило выявить ключевые векторы эволюции государственной политики в данной сфере

Выявленные проблемы — от недостатков нормативной базы до технологического отставания и ограниченного участия гражданского общества — сдерживают эффективность противодействия. В то же время положительный опыт внедрения некоторых правовых и организационных решений демонстрирует потенциал дальнейшего развития в этом направлении. Для эффективного противодействия требуется комплексный подход, сочетающий правовые меры, технические решения,

просветительские инициативы и участие общества. Перспективными являются усилия, направленные на повышение правовой и цифровой грамотности населения, создание альтернативных форм коммуникации и укрепление механизмов взаимодействия между гражданами и государственными структурами.

Особое значение приобретает внедрение алгоритмов машинного обучения и технологий анализа цифрового контента для своевременного выявления угроз. Одновременно важно развивать механизмы модерации и профилактики, в том числе с использованием лингвистической и психологической экспертизы, чтобы оперативно определять и нейтрализовать проявления экстремистской активности.

Таким образом, борьба с интернет-экстремизмом требует не только технических и правовых усилий, но и выстраивания устойчивой системы общественного иммунитета к идеологиям насилия, ненависти и радикализма. Только на основе скоординированных действий различных субъектов — от государства до пользователей социальных сетей — возможно обеспечить долгосрочную эффективность противодействия экстремизму в цифровом пространстве.