УДК 343
DOI 10.24412/3005-8023-2025-2-50-61

ЦИФРОВОЙ ЭКСТРЕМИЗМ: УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Кудратов Некруз Абдунабиевич, *начальник управления науки и инноваций Международного университета туризма и предпринимательства Таджикистана, д-р юрид. наук, профессор (Душанбе, Таджикистан);* ***Акилова Мукаддас Мирмухаммадовна,*** *ст. преподаватель каф. теории и истории государства и права ТГУПБП (Худжанд, Таджикистан)*

ЭКСТРЕМИЗМИ РАҚАМӢ: ТАҲДИД БА АМНИЯТИ МИЛЛӢ ВА РОҲҲОИ МУҚОВИМАТ

Кудратов Некруз Абдунабиевич, *сардори раёсати илм ва инноватсияи Донишгоҳи байналмилалии сайёҳӣ ва соҳибкории Тоҷикистон, доктори илмҳои ҳуқуқшиносӣ, профессор. (Душанбе, Тоҷикистон);* ***Акилова Муқаддас Мирмуҳаммадовна,*** *сармуаллими кафедраи назария ва таърихи давлат ва ҳуқуқи ДДҲБСТ (Хуҷанд, Тоҷикистон)*

DIGITAL EXTREMISM: A THREAT TO NATIONAL SECURITY AND WAYS TO COUNTERACTION

Kudratov Nekruz Abdunabievich, the *head of the department of science and innovations of the international University of tourism and entrepreneurship of Tajikistan, doctor of Law, professor. (Dushanbe, Tajikistan);* ***Akilova Mukaddas Mirmukhammadovna*** *senior lecturer of the department of theory and history of state and law under the TSULBP (Khujand, Tajikistan)* ***e-mail:*** *nek-kudratov@mail.ru*

Проанализировано понятие "цифровой экстремизм", который представляет собой одну из серьёзных угроз национальной безопасности Республики Таджикистан и всех стран мира. Установлено, что, несмотря на принятые меры, динамика совершения экстремистских и террористических преступлений в стране показывает значительное увеличение подобных случаев в последние годы. Подчёркивается необходимость разработки официального определения понятия "цифровой экстремизм" в национальном законодательстве и усиления правовых и технических механизмов противодействия названной угрозе. Кроме того, подробно рассмотрены основные формы проявления цифрового экстремизма: создание скрытых сетей, цифровая пропаганда, вербовка и кибератаки. Также предложена разработка новой Национальной стратегии противодействия цифровому экстремизму на основе глубокого анализа текущей ситуации.

Ключевые слова: *Таджикистан, национальная безопасность, информационная безопасность, цифровой экстремизм, кибератаки, цифровая пропаганда, национальное законодательство, противодействие цифровому экстремизму*

Мафҳуми "экстремизми рақамӣ" ҳамчун яке аз таҳдидҳои ҷиддӣ ба амнияти миллӣ дар Ҷумҳурии Тоҷикистон ва ҷаҳон таҳлил ва мавриди баррасӣ қарор гирифтааст. Муайян карда шудааст, ки бо вуҷуди тадбирҳои андешидашуда, динамикаи содиршавии ҷиноятҳои экстремистиву террористӣ дар кишвар дар солҳои охир тамоюл ба афзоиш дорад. Зарурати таҳияи таърифи расмии мафҳуми "экстремизми рақамӣ" дар қонунгузории миллӣ ва таҳкими механизмҳои ҳуқуқӣ ва техникии муқовимат бо ин таҳдид таъкид карда шудааст. Илова бар ин, ташкили шабакаҳои пинҳонӣ, таблиғоти рақамӣ, истихдом ва ҳамлаҳои киберӣ ҳамчун шаклҳои асосии зуҳури экстремизми рақамӣ муфассал тавсиф шудаанд. Ҳамчунин зарурати таҳияи стратегияи нави миллӣ барои муқовимат бо экстремизми рақамӣ бо такя ба таҳлили амиқи вазъи мавҷуда пешниҳод шудааст.

Калидвожаҳо: *Тоҷикистон, амнияти миллӣ, амнияти иттилоотӣ, экстремизми рақамӣ, ҳамлаҳои кибернетикӣ, қонунгузории миллӣ, муқовамат ба экстремизми рақамӣ*

The article analyzes the concept of "digital extremism", which is one of the serious threats to the national security of the Republic of Tajikistan and all countries in the world. It is established that, despite the measures taken, the dynamics of extremist and terrorist crimes in the country shows a significant increase in such cases in recent years. The need to develop an official definition of the concept of "digital extremism" in national legislation and to strengthen legal and technical mechanisms to counter this threat is emphasized. In addition, the main forms of digital extremism are examined in detail: the creation of hidden networks, digital propaganda, recruitment and cyber attacks. It is also proposed to develop a new National Strategy for Countering Digital Extremism based on a deep analysis of the current situation.

Key-words: *Tajikistan, national security, information security, digital extremism, cyber-attacks, digital propaganda, national legislation, counteraction to the digital extremism*

В Послании Президента Республики Таджикистан Эмомали Рахмона за 2023 год было подчёркнуто: «Сложная и тревожная обстановка в регионе и мире, в том числе ускоряющийся процесс перераспределения мира, быстрая милитаризация, холодная война, современные угрозы и вызовы — терроризм и экстремизм, контрабанда оружия, киберпреступность и другие формы транснациональной организованной преступности заставляют нас принимать дополнительные меры для обеспечения оборонной безопасности нашей страны» [10]. Современные угрозы, в том числе одна из форм экстремизма — цифровой экстремизм, представляют серьёзную опасность для национальной безопасности Таджикистана.

Исследователь С.С. Ятимов справедливо отмечает, что история человечества в целом — это не история мира. Это история войн, борьбы и конфликтов, которые на протяжении веков сопровождали жизнь людей, будучи одной из форм политики. Основная причина такой напряжённой ситуации, к сожалению, остаётся неизменной на протяжении веков — люди в основном говорят на одном языке. Этот язык можно назвать «языком интересов» [16]. Эти слова С.С. Ятимова указывают на глубокую природу человеческих конфликтов и противоречий, которые сопровождают общество и государство с древних времён до наших дней, что история человечества — это не только история мира, но и, в большей степени, история войн и борьбы. Этот процесс связан с тем, что люди в своих взаимоотношениях чаще говорят на языке интересов, а не на языке справедливости или взаимопонимания. Основные причины такой ситуации следующие: во-первых, экономические и политические интересы. На протяжении всей истории большинство войн и конфликтов возникало из-за природных ресурсов, территориальных захватов, влияния и власти. Древние империи – Рим, Персия, Египет, а также средневековые государства постоянно воевали за расширение территорий и политическое могущество. В современную эпоху экономические и геополитические интересы также способствуют возникновению конфликтов, яркими примерами являются войны в Сирии, Ираке, Афганистане, Йемене и конфликты за энергетические ресурсы. Во-вторых, это язык интересов и культурные столкновения. С.С. Ятимов справедливо отмечает, что люди чаще всего говорят на языке интересов. Это означает, что личные, групповые и государственные интересы часто ставятся выше человеческих ценностей и справедливости. Например, в международных отношениях большинство стран в первую очередь защищает национальные интересы независимо от того, как это может повлиять на глобальную стабильность и безопасность. В-третьих, это проявления человеческой природы и стремление к соперничеству. Язык интересов тесно связан с природой человека. Люди по своей природе стремятся к лучшему положению,

влиянию и власти. Это можно наблюдать не только в отношениях между государствами, но и в обществе, где группы, партии и организации борются за власть и влияние. В-четвёртых, это идеология и религиозные интересы. Помимо экономических и политических интересов, идеология и религиозные убеждения также часто становятся причиной конфликтов. В истории можно найти множество примеров этого, включая крестовые походы, религиозные войны в Европе и конфликты на религиозной почве на Ближнем Востоке. В-пятых, это технологическое развитие и разработка новых видов вооружений. Прогресс в военных технологиях и разработка новых видов оружия на каждом этапе истории способствовали усилению конфликтов. Каждое новое открытие в военной сфере, от луков и стрел до ядерного оружия, предоставляло новые возможности для ведения войн, делая конфликты ещё более разрушительными. В-шестых, это доступ к информации и политическая пропаганда. В современную эпоху средства массовой информации и социальные сети могут способствовать эскалации конфликтов, так как они быстро распространяют идеологическую пропаганду, ложную информацию и призывы к насилию.

Таким образом, взгляды С.С. Ятимова показывают, что войны и конфликты являются неотъемлемой частью человеческой истории, так как они часто связаны с личными, экономическими, политическими и культурными интересами. Язык интересов, который фактически лежит в основе международных и внутренних отношений, является основной причиной эскалации конфликтов на протяжении человеческой истории.

Проблема обеспечения информационной безопасности Республики Таджикистан в ходе развития информационно-коммуникационных технологий приобрела чрезвычайно важное значение. Её необходимость и значимость были отражены в Концепции информационной безопасности Республики Таджикистан, принятой ещё в 2003 году. Анализ этого важного политического документа показывает, что информационная безопасность действительно является центральным элементом национальной безопасности Таджикистана. В данном документе обоснованы цели, задачи, принципы и основные направления обеспечения информационной безопасности Республики Таджикистан. Также в документе отмечается, что информационная безопасность Республики Таджикистан представляет собой состояние защищённости национальных интересов страны в информационной сфере, которое включает комплекс взаимосвязанных интересов личности, общества и государства. В Концепции информационной безопасности Республики Таджикистан подчёркивается, что информационная сфера является важным элементом общественной жизни и оказывает значительное влияние на политическую, экономическую, оборонную и другие составляющие национальной безопасности Республики Таджикистан. Уровень и качество этих составляющих напрямую зависят от уровня обеспечения информационной безопасности. Концепция чётко определяет государственную политику Республики Таджикистан в области обеспечения информационной безопасности [17].

Безусловно, обеспечение информационной безопасности Республики Таджикистан является приоритетной задачей из-за роста информационных угроз, расширения цифровых технологий и увеличения масштабов киберпространства. Информационная безопасность как важнейший элемент национальной безопасности Таджикистана включает защиту информационных ресурсов, компьютерных сетей и информационных технологий. Этот процесс предполагает не только защиту конфиденциальности, целостности, доступности и безопасности государственных и личных данных, но и предотвращение кибератак, цифрового шпионажа и гибридных угроз.

В Таджикистане информационная безопасность регулируется комплексом законодательных и нормативных актов, включающих следующие основные элементы: защита критической информационной инфраструктуры, внедрение современных

технологий защиты информации, контроль за использованием цифровых технологий, создание эффективной системы управления рисками, повышение осведомлённости и цифровой грамотности населения, укрепление сотрудничества с международными партнёрами в области борьбы с киберпреступностью, а также усиление информационной безопасности электронного правительства и цифровых сервисов. Целью этих мер является создание устойчивой системы защиты информации от незаконного разглашения, изменения и уничтожения.

По состоянию на 2025 год в Республике Таджикистан по решениям Верховного Суда Республики Таджикистан запрещена деятельность 29 террористических и экстремистских групп и организаций. Однако, несмотря на принятые меры, динамика совершения экстремистских и террористических преступлений в Республике Таджикистан в период с 2010 по 2024 год показывает значительный рост в количественном и в качественном отношении [11]. Согласно статистическим данным, в 2010 году в Таджикистане было зарегистрировано десять случаев экстремистских преступлений, но в последующие годы их количество существенно увеличилось: в 2011 году — 28, в 2012 — 18, в 2013 — 38, в 2014 — 116, в 2015 — 345, в 2016 — 617, в 2017 — 506, в 2018 — 360, в 2019 — 634, в 2020 — 1091, в 2021 — 761, в 2022 — 991, в 2023 — 1228 и в 2024 — 1494 случая [6]. Эти данные свидетельствуют, что в последние годы интенсивность совершения экстремистских и террористических преступлений в стране значительно возросла [7]. Например, в 2024 году по сравнению с 2010 годом число таких преступлений увеличилось более чем в 149 раз, причём большинство из них связано с цифровыми технологиями.

Официальное определение понятия «цифровой экстремизм» в законодательстве Республики Таджикистан, в частности в Законе Республики Таджикистан «О противодействии экстремизму» [9], отсутствует. В этом законе даже не предусмотрено понятие «информационный экстремизм», что можно считать одним из его недостатков. Поэтому для разработки и определения понятия «цифровой экстремизм» требуется его доктринальное осмысление и правовая проработка.

С одной стороны, развитие информационных и коммуникационных технологий создало новые возможности для социального и экономического прогресса стран мира, с другой стороны — сформировало благоприятные условия для распространения опасных явлений, например, цифрового экстремизма. В современную эпоху цифровой экстремизм фактически превратился в транснациональное явление, которое объединяет традиционные формы радикализма с неограниченными возможностями Интернета. Анализ доктрины юридических наук (уголовное право, криминология, международное уголовное право и др.), политологии, социологии позволяет дать следующее определение цифрового экстремизма: «Цифровой экстремизм — это форма экстремистской деятельности, которая осуществляется с использованием цифровых инструментов, таких как социальные сети, мессенджеры, видеоплатформы и другие онлайн-ресурсы, с целью распространения радикальных идей, пропаганды насилия и привлечения новых сторонников».

По словам И. Эвона, экстремисты широко используют социальные сети как «стабильную и безопасную среду для радикализации молодёжи», где опасные идеологии распространяются простым и доступным языком, иногда под религиозными, политическими или социальными лозунгами [1, с. 278–286]. Определение этой среды как «стабильной и безопасной» И. Эвон выбрал не случайно, поскольку: 1) социальные сети не находятся под полным контролем; 2) радикалы могут действовать под вымышленными именами и анонимно; 3) экстремисты используют простой язык и эмоциональные лозунги, чтобы манипулировать чувствами молодёжи и склонять её к совершению экстремистских и террористических преступлений.

В каждом обществе всегда находятся люди (чаще всего молодёжь), которые переживают кризис, находятся в состоянии беспокойства, разочарования или ищут смысл жизни. Радикальная пропаганда в социальных сетях активно воздействует на эти чувства. Экстремистская идеологии внешне может казаться ответом на социальные проблемы или призывом к справедливости, в то время как на самом деле направлена на насилие, ненависть и радикализацию.

Цифровой экстремизм проявляется в различных формах и может меняться в зависимости от целей, методов и целевой аудитории экстремистов. Вот некоторые из основных форм цифрового экстремизма, которые чаще всего встречаются в Интернете и социальных сетях:

1. Цифровая экстремистская пропаганда — этот вид деятельности выражается в распространении изображений, видео, текстов и сообщений, пропагандирующих экстремистскую идеологию с использованием убедительных форматов подачи. Этот вид цифрового экстремизма особенно распространён в социальных сетях (Facebook, Instagram, TikTok) и на видеоплатформах (YouTube, Telegram). Основная цель такой пропаганды — воздействие на эмоции молодёжи, создание образов "героев" из радикалов и формирование групповой идентичности. Например, на видеоплатформе YouTube пропагандисты и экстремисты Муджибуррахмон Ансари, Абу Заир Дааи, Мухаммад Мадани, Абу Убайдулло Мутаваккил, Абу Мухаммад Хоблос, Закир Найк, Маулана Фируз, Мухаммадикбол Садриддин и многие другие создают страницы от своего имени или от имени организаций, деятельность которых запрещена в Таджикистане. Эти каналы могут насчитывать до 200 000 подписчиков, причём основное общение на таких каналах ведётся на таджикском языке, что позволяет предполагать, что значительная часть подписчиков — граждане Таджикистана или люди, владеющие таджикским языком.

2. Виртуальная радикализация — это процесс, в ходе которого человек постепенно принимает радикальные взгляды в онлайн-среде, пока не станет готовым к совершению экстремистских действий. Этот процесс может занимать месяцы или даже годы и часто включает просмотр пропагандистских материалов, участие в закрытых чатах и обсуждениях.

3. Вербовка — экстремистские группы используют чаты, форумы и игровые платформы (например, Discord, Steam) для установления контакта с молодыми людьми, ведут с ними переписку и постепенно вовлекают их в свои ряды. «Джамаат Ансорулло», «Группа-24», «Исламское государство», «Джабхат ан-Нусра», «Партия исламского возрождения Таджикистана» и «Национальный альянс Таджикистана» являются активными участниками таких экстремистских и террористических группировок. Только благодаря вербовке сторонников ИГИЛ более 2 500 граждан Таджикистана участвовали в вооружённых конфликтах в Сирии, Ираке и Афганистане [3; 4; 5; 6].

4. Создание скрытых сетей — экстремистские и террористические группы обычно используют зашифрованные приложения (например Telegram, Signal) для секретного общения, обмена планами и координации действий. Эти сети, как правило, закрыты для посторонних, доступ к ним возможен только после «проверки» или получения «доверия». Например, в период своей активности ИГИЛ широко использовало Telegram для объединения сторонников в разных странах и координации террористических операций. Telegram позволяет создавать группы до 200 000 участников и обеспечивает высокий уровень шифрования [13]. Организация «Аль-Каида» использует мессенджер Threema, который обеспечивает высокий уровень конфиденциальности и анонимности, для распространения пропаганды и оперативного планирования. Исследования, проведённые после терактов в Париже в 2015 году и в Москве («Крокус-сити») в 2024 году, показали, что

группы нападавших использовали для коммуникации и координации WhatsApp и Telegram [12]. Создание закрытых сетей позволяет экстремистам и террористам действовать практически незаметно, обмениваться информацией и готовить операции без риска разоблачения. Эти сети функционируют на основе передовых технологий шифрования и секретности, что делает их практически недоступными для внешнего контроля.

5. Кибератаки с идеологической мотивацией — некоторые экстремистские группы (например ИГИЛ) совершают цифровые атаки (DDoS, взломы, дефейсы сайтов) с политическими, религиозными или идеологическими целями. Эти атаки обычно направлены против государственных учреждений, военных сетей, СМИ или лиц, занимающих антирелигиозную или антиэкстремистскую позицию. Кибератаки на военные сети и оборудование могут подорвать обороноспособность страны, включая снижение возможностей связи, вмешательство в системы управления и контроля, а также нарушение работоспособности военной техники. Президент Республики Таджикистан Эмомали Рахмон в этом контексте подчёркивает, что для обеспечения оборонной безопасности страны необходимо принимать дополнительные меры: улучшать условия службы военнослужащих, подготавливать высококвалифицированные кадры и повышать уровень патриотизма солдат и офицеров.

6. Цифровые оскорбления и запугивание. Давление, оскорбления, угрозы и клевета в отношении общественных активистов, журналистов, преподавателей или даже студентов, которые выступают против экстремистских групп, стали одной из характерных форм поведения экстремистских и террористических группировок. Эти действия часто осуществляются через сообщения, комментарии и фейковые аккаунты.

Цифровые угрозы (или виртуальный шантаж) — это форма преступной деятельности, при которой злоумышленники используют цифровые технологии и Интернет для запугивания, вымогательства, шантажа или давления на жертв. Такие атаки могут быть направлены и на отдельных лиц, и на компании, организации или даже на государственные учреждения. Основные особенности цифровых угроз включают:

а) угрозу разглашения информации. Киберпреступники часто угрожают раскрыть конфиденциальную, личную или компрометирующую информацию, если их требования не будут выполнены;

б) финансовое вымогательство. Часто целью таких атак становится получение выкупа за неразглашение или уничтожение компрометирующей информации. Киберпреступники требуют выплаты в обмен на сохранение конфиденциальности данных;

в) атаки на личные данные. Киберугрозы могут включать угрозу раскрытия личных данных: фотографий, видео, переписки и другой чувствительной информации. Такие атаки представляют серьёзную угрозу для личной безопасности, репутации и информационной безопасности жертвы;

г) массовое психологическое давление. Экстремисты часто используют социальные сети для массовой травли и давления на активистов, политиков или граждан, выражающих антиидеологические позиции. Фейковые аккаунты, массовые рассылки и организованные кампании по травле — часть этой тактики.

Борьба с таким видом преступлений требует комплексного подхода, включающего обучение пользователей, использование современных технологий кибербезопасности и тесное взаимодействие с правоохранительными органами.

Цифровой экстремизм представляет серьёзную угрозу национальной безопасности, так как может стать причиной террористических актов на индивидуальном и социальном уровнях. Как отмечает Дж. Вейман: "Интернет предоставляет экстремистам не только платформу для агитации, но и инструмент для организации операций". В книге *"Терроризм в*

киберпространстве: следующее поколение" (Terrorism in Cyberspace: The Next Generation) он анализирует, как террористические организации адаптировались к цифровой среде и используют веб-сайты, социальные сети и скрытые сети (Darknet) для распространения своей идеологии и вербовки сторонников. Он подчёркивает, что Интернет предоставляет экстремистам прозрачность, глобальный охват и низкую стоимость распространения материалов, что делает его идеальной платформой для их деятельности [6].

В цифровой среде географические и юридические ограничения практически исчезают, что, по мнению Дж. Брауна, «превращает экстремизм в глобальную сеть без границ» [2, с. 45-58]. Этот аспект подчёркивает два ключевых фактора: а) отсутствие географических границ, т.к. Интернет представляет собой глобальную сеть, которая позволяет пользователям в реальном времени общаться с другими людьми независимо от их физического местонахождения. Это позволяет террористическим и экстремистским группам получать доступ к широкой аудитории, распространять заранее подготовленные пропагандистские материалы и привлекать сторонников со всего мира; б) сложности юридического контроля. В цифровой среде мониторинг и преследование экстремистских групп становятся значительно сложнее, чем в реальном мире. Многие из этих групп используют технологии шифрования, которые делают их коммуникации практически недоступными для правоохранительных органов. Приложения, например Telegram и WhatsApp, позволяют отправлять личные сообщения без риска идентификации, что существенно снижает эффективность правовых мер; в) скорость и глобальность распространения. Интернет позволяет экстремистским материалам распространяться с высокой скоростью и глобальным охватом. Это означает, что радикальное сообщение может быть доставлено тысячам людей всего за несколько секунд, чего невозможно достичь в реальном мире.

Таким образом, утверждение Дж. Брауна подчёркивает два ключевых аспекта: с одной стороны, глобальная сеть без границ позволяет экстремистским идеологиям распространяться широко и с высокой скоростью, а с другой стороны, она создаёт благоприятную среду для вербовки и укрепления сторонников, что делает традиционные методы противодействия менее эффективными.

В 2025 году завершится действие Стратегии противодействия экстремизму и терроризму в Республике Таджикистан на 2021-2025 годы, и мы уверены, что Правительство Республики Таджикистан разработает и внедрит новую стратегию с учётом факторов и условий, способствующих возникновению этих преступлений, особенно цифрового экстремизма. С учётом тревожной динамики роста в последние годы экстремистских и террористических преступлений, разработка новой стратегии должна основываться на глубоком анализе текущей ситуации и быть направлена не только на предотвращение экстремистских и террористических преступлений, но и на устранение социальных, экономических, культурных и идеологических факторов, способствующих распространению радикализма.

Для новой стратегии противодействия цифровому экстремизму могут быть предложены следующие рекомендации:

1. Необходимы инициативы по созданию новых правовых механизмов и по укреплению международного сотрудничества в области противодействия цифровому экстремизму. Для этого национальное законодательство должно быть адаптировано к новым технологическим вызовам, а также необходимо укреплять международные соглашения по борьбе с цифровым экстремизмом.

2. В рамках объявленного периода «Годы цифрового экономического развития и инноваций» (2025-2030) следует уделить особое внимание повышению цифровой

грамотности населения, принятию государственных программ, направленных на обучение методам выявления и противодействия экстремистской пропаганде в медиа и образовательных учреждениях.

3. Необходимо внедрить в деятельность ГКНБ, МВД и Генеральной прокуратуры Республики Таджикистан использование цифровых инструментов против экстремизма – искусственного интеллекта и криминологического анализа. Для этого следует разработать и внедрить алгоритмы, выявляющие опасные материалы, связанные с экстремизмом, терроризмом и другими преступлениями.

4. Проведение научных исследований и развитие криминологических подходов в области уголовной ответственности и противодействия экстремизму и терроризму. В Республике Таджикистан уже защищены две докторские и более десяти кандидатских диссертаций по вопросам уголовной ответственности за экстремизм и терроризм, однако многие из предложенных научных разработок не были реализованы на практике. Мы убеждены, что анализ этих диссертаций и практическая реализация их предложений могут существенно снизить уровень экстремистских проявлений.

Противодействие экстремизму в целом должно быть основано на науке, включая следующие ключевые направления:

а) рекомендации, представленные в диссертационных исследованиях (докторских и кандидатских) по вопросам уголовной ответственности и противодействия экстремизму и терроризму, должны быть внедрены в практику. Для этого необходимо установить тесное сотрудничество между научными учреждениями и правоохранительными органами (ГКНБ, МВД), чтобы результаты научных исследований могли эффективно применяться;

б) правительство Республики Таджикистан должно предусмотреть специальные меры для поддержки научных исследований в области противодействия экстремизму и терроризму. Это может включать гранты, финансовую поддержку, научные конкурсы и создание благоприятных условий для внедрения научных результатов;

в) проведение международных конференций и симпозиумов по вопросам цифровой криминологии и противодействия экстремизму и терроризму может способствовать обмену опытом, изучению новых методов исследований и разработке эффективных стратегий. Такие мероприятия могут проводиться с участием международных экспертов, представителей силовых структур и учёных;

г) для эффективной организации научных исследований в области противодействия экстремизму и терроризму необходимо создание, по крайней мере, Национального центра или научного Института криминологических исследований при ГКНБ и научных учреждениях (например, это Таджикский национальный университет, Академия МВД, Международный университет туризма и предпринимательства Таджикистана и другие). Этот центр должен заниматься анализом цифровых преступлений, изучением тактики и стратегии экстремистов в онлайн-среде, а также разработкой научных рекомендаций для предотвращения радикализации;

д) для повышения уровня знаний сотрудников правоохранительных органов, прокуроров, судей и преподавателей необходимо разработать и внедрить специальные курсы по цифровой криминологии, психологии экстремистов и методам противодействия экстремистской пропаганде. Такие учебные материалы должны быть адаптированы к конституционным основам национального государственного устройства.

Таким образом, в противодействии экстремизму имеют особое значение достижения науки. Научные исследования, посвященные изучению причин, условий и механизмов распространения экстремистской идеологии, позволяют разрабатывать эффективные стратегии для предотвращения этих угроз и борьбы с ними. Наука в этом процессе

выполняет двойную функцию: с одной стороны, она обеспечивает теоретическую основу для изучения экстремизма, а с другой – предлагает практические механизмы противодействия. Роль науки в противодействии экстремизму связана прежде всего со следующими моментами.

Во-первых, наука позволяет точно определять такие ключевые понятия, как «цифровой экстремизм» и другие связанные термины, анализировать формы их проявления и устанавливать основные показатели распространения [8]. Это включает использование больших данных (Big Data), искусственного интеллекта и сложных аналитических алгоритмов для идентификации экстремистского контента в цифровой среде. Например, такие платформы, как Meta (Facebook, Instagram) и YouTube, уже активно применяют автоматические системы распознавания и удаления экстремистского контента.

Во-вторых, наука играет ключевую роль в разработке технологий предотвращения и выявления опасного контента в цифровом пространстве. Этот процесс основан на применении искусственного интеллекта, аналитики больших данных и других современных технологий. Такие системы позволяют своевременно обнаруживать и блокировать экстремистские материалы, тем самым снижая риски радикализации.

В-третьих, наука может способствовать разработке эффективных механизмов вовлечения молодежи в социальные и политические процессы, снижая чувство отчуждения и безнадежности, которое часто становится причиной вовлечения молодых людей в экстремистские группы. Образовательные и воспитательные программы, направленные на повышение цифровой грамотности, развитие критического мышления и формирование гуманистических ценностей, могут существенно снизить уровень радикализации молодежи.

В-четвертых, научные исследования могут способствовать разработке комплексного законодательства и национальной стратегии по противодействию экстремизму. Например, исследования, проведенные в Таджикистане, посвященные экстремистским преступлениям, цифровым механизмам вербовки и пропаганды, могут стать основой для разработки новых законов и мер безопасности.

Таким образом, роль науки в противодействии экстремизму заключается в разработке теоретических основ, проведении эмпирических исследований и применении современных технологий, что создает благоприятные условия для защиты национальной и международной безопасности.

В этом контексте «С.С. Ятимов справедливо отмечает, что система, структура и функции обеспечения государственной безопасности могут успешно выполнять свои задачи в рамках действующего законодательства только в том случае, если к вопросам науки и образования будет применяться системный подход с обязательным учетом закономерностей развития общества и человеческого мышления» [14; 15].

5. Эффективное установление сотрудничества с глобальными платформами. Обеспечение сотрудничества с глобальными платформами Google, Meta (Facebook, Instagram, WhatsApp), TikTok, X (бывший Twitter) и другими является одним из ключевых направлений противодействия цифровому экстремизму. Такое сотрудничество не только делает борьбу с экстремистской пропагандой более эффективной, но и создаёт благоприятные условия для защиты национальной и международной безопасности. Многие страны, к примеру Германия (с законом NetzDG — Немецкий закон против ненависти и травли в Интернете) и Индия, законодательно обязывают технологические компании удалять опасный контент с их платформ в определенные сроки. Для Республики Таджикистан является своевременной мерой принятие аналогичного закона. Республика Таджикистан должна подписать с компаниями меморандумы о сотрудничестве, в которых будет закреплено обязательство платформ рассматривать опасные материалы по запросу

государственных органов, а также организовывать обучающие курсы для сотрудников силовых структур (например, как отправлять запросы на удаление контента или получение данных). Конечно, в каждой платформе действуют специальные программы с использованием искусственного интеллекта, чтобы экстремистский и террористический контент не попадал в сеть. Например, платформа Meta (Facebook, Instagram) использует Community Standards и специальные группы по противодействию hate speech и экстремизму. YouTube (принадлежащий Google) применяет искусственный интеллект для автоматического выявления и удаления экстремистских видео. Однако, несмотря на значительные усилия платформ в борьбе с экстремизмом и терроризмом, из-за огромного объема данных и сложности языков (например, таджикский или дари) возможность полного контроля остаётся ограниченной.

Вывод: противодействие цифровому экстремизму представляет собой сложный, многолетний и многосекторный процесс. Для его эффективного выявления и противодействия необходимо детально анализировать каждый аспект и обеспечивать профессиональный контроль на всех уровнях.

Проведённые исследования показывают, что цифровой экстремизм в современную эпоху стал серьёзной транснациональной угрозой, которая представляет собой риск для национальной безопасности Республики Таджикистан. Быстрое развитие информационных технологий и рост численности интернет-пользователей создают благоприятные условия для распространения экстремистской идеологии, виртуальной радикализации и цифрового вербовочного процесса.

Эффективное противодействие цифровому экстремизму должно включать активное правовое регулирование, цифровую грамотность, междисциплинарные научные исследования, использование искусственного интеллекта и криминологических методов анализа, а также международное сотрудничество с глобальными цифровыми платформами. В дополнение к этому, вовлечение гражданского общества и развитие цифровой криминологии может значительно снизить риск цифрового экстремизма и укрепить национальную стабильность.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. *Awan I. (2016). Cyber-Extremism: ISIS and the Power of Social Media. Society, 53(3), 278–286.*
2. *Brown J. Digital Radicalization: The Global Threat of Online Extremism. Global Security Review, 2020, 12(2), 45–58.*
3. *Farangis N. Life After Islamic State: Pardoned Tajik Militants Navigate Road To Reintegration. RFE/RL. – August 6, 2017.*
4. *Klausen J. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. Studies in Conflict & Terrorism, 2015, 38(1), 1–22*
5. *Richard B. Beyond the Caliphate: Foreign Fighters and the Threat of Returnees. Soufan Center. - October 2017. - June 2018/*
6. *Weimann, G. Terrorism in Cyberspace: The Next Generation. Columbia University Press, 2015. 329 p.*
7. *Кудратов, Н.А. Некоторые вопросы влияния образования на предупреждение экстремизма / Н.А. Кудратов // Вестник Таджикского государственного университета коммерции. – 2022. – № 3(42). – С. 313-325.*
8. *Кудратов, Н.А. Уголовно–правовая охрана основ конституционного строя и безопасности государства: проблемы доктрины, правоприменения и совершенствования законодательства: дисс… д-ра юрид. наук / Н.А. Кудратов. – Душанбе, 2021. – 539 с.*

9. *Қонуни Ҷумҳурии Тоҷикистон "Дар бораи муқовимат ба экстремизм". Аз 2 январи соли 2020, № 1655. [Электронный ресурwc]. – Режим доступа: https://mmk.tj/system/files/Legislation/1655_tj_0.pdf (дата обращения: 04.05.2025).*
10. *Паёми Президенти Ҷумҳурии Тоҷикистон муҳтарам Эмомалӣ Раҳмон «Дар бораи самтҳои асосии сиёсати дохилӣ ва хориҷии ҷумҳурӣ» [Электронный ресурс]. – Манбаи дастрасӣ: https://president.tj/event/missives/36370 (дата обращения: 04.05.2025).*
11. *Стратегияи муқовимат ба экстремизм ва терроризм дар Ҷумҳурии Тоҷикистон барои солҳои 2021-2025. [Электронный ресурс]. – Режим доступа: https://www.anticorruption.tj/images/PDF/ter-ek.pdf (дата обращения: 04.05.2025).*
12. *Телеграм заблокировал 78 каналов, связанных с ИГИЛ [Электронный ресурс]. – Режим доступа: https://www.tatar-inform.ru/news/telegram-zablokiroval-78-kanalov-svyazannyh-s-igil (дата обращения: 04.05.2025).*
13. *Телеграм. Роскомнадзор заблокировал 11 Telegram-каналов после теракта в «Крокусе» [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/6596494 (дата обращения: 04.05.2025).*
14. *Ятимов С.С. Илм ва амният / С.С. Ятимов // Международные отношения и безопасность. – 2022. – №. 1(1). – С. 9-23.*
15. *Ятимов С.С. Дунявият ва амният / С.С. Ятимов // Международные отношения и безопасность. – 2022. – №. 2(2). – С. 18-36.*
16. *Ятимов С.С. Эҳёи миллат - бақои давлат / С.С. Ятимов // Тоҷикистон ва ҷаҳони имрӯз. – 2024. – №. 4(88). – С. 14-33.*
17. *Ятимов С.С., Холиқов Ф.А. Амнияти иттилоотии Ҷумҳурии Тоҷикистон ва самтҳои асосии таъмини он / С.С. Ятимов // Идоракунии давлатӣ. – 2021. – №. 3(52). – С. 204-216.*

REFERENCES:

1. *Awan I. (2016). Cyber-Extremism: ISIS and the Power of Social Media. Society, 53(3), 278–286*
2. *Brown J. Digital Radicalization: The Global Threat of Online Extremism. Global Security Review, 2020, 12(2), 45–58.*
3. *Farangis N. Life After Islamic State: Pardoned Tajik Militants Navigate Road to Reintegration. RFE/RL. - August 6, 2017.*
4. *Klausen J. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. Studies in Conflict & Terrorism, 2015, 38(1), 1–22*
5. *Richard B. Beyond the Caliphate: Foreign Fighters and the Threat of Returnees. Soufan Center. - October 2017. - June 2018/*
6. *Weimann, G. Terrorism in Cyberspace: The Next Generation. Columbia University Press, 2015. 329 pp.*
7. *Kudratov N.A. Some Issues of the Influence of Education in the Prevention of Extremism // Bulletin of the Tajik State University of Commerce. - 2022. - No. 3 (42). - PP. 313-325.*
8. *Kudratov N.A. Criminal-Legal Protection of the Foundations of the Constitutional System and State Security: problems of doctrine, law enforcement and improvement of legislation: dissertation for the degree of Doctor of Law. - Dushanbe, 2021. - 539 pp.*
9. *Law of the Republic of Tajikistan "On Countering Extremism". From January 2, 2020, No. 1655 [Electronic resource]. – Source of access: https://mmk.tj/system/files/Legislation/1655_tj_0.pdf (date of appeal: 04.05.2025).*
10. *Message of the President of the Republic of Tajikistan, His Excellency Emomali Rahmon "On the Main Directions of the Domestic and Foreign Policy of the Republic" [Electronic resource]. – Source of access: https://president.tj/event/missives/36370 (date of appeal: 04.05.2025).*

11. *Strategy for Countering Extremism and Terrorism in the Republic of Tajikistan for 2021-2025 [Electronic resource]. – Source of access: https://www.anticorruption.tj/images/PDF/ter-ek.pdf (date of appeal: 04.05.2025).*

12. *Telegram blocked 78 channels linked to ISIS [Electronic resource]. – Source of access: https://www.tatar-inform.ru/news/telegram-zablokiroval-78-kanalov-svyazannyh-s-igil (date of appeal: 04.05.2025).*

13. *Telegram. Roskomnadzor blocked 11 Telegram channels after the terrorist attack in Crocus [Electronic resource]. – Source of access: https://www.kommersant.ru/doc/6596494 (date of appeal: 04.05.2025).*

14. *Yatimov S.S. Science and Security // International Relations and Security. – 2022. – No. 1(1). – PP. 9-23.*

15. *Yatimov S.S. Worldliness and Security // International Relations and Security. – 2022. – No. 2(2). – PP. 18-36.*

16. *Yatimov S.S. Revival of the Nation - the Survival of the State // Tajikistan and the Modern World. – 2024. – No. 4(88). – PP. 14-33.*

17. *Yatimov S.S., Kholikov F.A. Information Security of the Republic of Tajikistan and the Main Directions of Its Provision // State Administration. – 2021. – No. 3(52). – PP. 204-216.*