

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE

МРНТИ 11.15.24

DOI: <https://doi.org/10.51889/2959-6270.2026.95.3.016>

Е.К. Алияров<sup>1</sup> , Д.Ж. Жангузжекова<sup>1\*</sup> 

<sup>1</sup>Казахстанский центр гуманитарно-политической конъюнктуры

г. Алматы, Казахстан

\*e-mail: [dinara.zhanguzhekova@gmail.com](mailto:dinara.zhanguzhekova@gmail.com)

## ВОПРОСЫ ЭФФЕКТИВНОСТИ ГОСУДАРСТВЕННЫХ МЕР ПО ПРОТИВОДЕЙСТВИЮ ВЕРБАЛЬНОМУ ЭКСТРЕМИЗМУ В ИНТЕРНЕТ- ПРОСТРАНСТВЕ КАЗАХСТАНА

### Аннотация

Стремительное развитие информационно-коммуникационных технологий стало катализатором возникновения «вербального/информационного экстремизма», который представляет серьезную угрозу в системе обеспечения национальной безопасности института государства и общества. Как известно, наиболее актуальным и значимым аспектом в данном вопросе является тот факт, что главным потребителем цифровых платформ по всему миру являются молодые люди, которые соответственно подпадают под риски идеологической обработки и вербовки со стороны экстремистских групп. Следовательно, настоящее исследование направлено на анализ степени эффективности государственной политики реализации профилактических и противодействующих мер вербальному экстремизму среди молодежи и в целом населения Казахстана. Выявление и оценка проблем в данной сфере осуществляется посредством междисциплинарной методологической парадигмы, в эмпирическую часть которой включены представление правительственных статистических отчетов, аналитических докладов международных организаций, а также анализ технических блокировок и технологий обхода, и рассмотрение возможностей «миграции» цифровой радикализации между различными платформами. Так, в статье продемонстрирована деятельность государственных органов, приведшая к значительной блокировке сомнительных, с точки зрения государства, доменов и материалов. С позиции авторов, подобные подходы реагирования, вероятно, и приводят к положительным результатам, однако они не дают полной гарантии того, что к запрещенным сайтам не будет никакого доступа – их можно обойти с помощью указанных приложений, и одновременно сохранить анонимность. Существование одной лишь сдерживающей политики и ограничительных мер недостаточны в борьбе с экстремистской деятельностью в рамках обеспечения социально-политической и культурной стабильности в обществе. Следует переходить на более многогранную и комплексную государственную политику, где приоритеты должны быть расставлены в пользу повышения уровня образования, критического сознания, цифровой медиаграмотности и культурно-ценностных ориентиров в обществе.

**Ключевые слова:** вербальный экстремизм, Казахстан, государственные меры, молодежь, интернет-пространство, радикализация, контрпропаганда.

Е.К. Алияров<sup>1</sup>, Д.Ж. Жангузжекова<sup>1\*</sup>

<sup>1</sup>Қазақстан гуманитарлық-саяси конъюнктура орталығы

Алматы, Қазақстан

\* e-mail: [dinara.zhanguzhekova@gmail.com](mailto:dinara.zhanguzhekova@gmail.com)

## ҚАЗАҚСТАННЫҢ ИНТЕРНЕТ-КЕҢІСТІГІНДЕ ВЕРБАЛДЫ ЭКСТРЕМИЗМГЕ ҚАРСЫ ІС-ҚИМЫЛ ЖӨНІНДЕГІ МЕМЛЕКЕТТІК ШАРАЛАРДЫҢ ТИІМДІЛІГІ МӘСЕЛЕЛЕРІ

### *Аңдатпа*

Ақпараттық-коммуникациялық технологиялардың қарқынды дамуы мемлекет пен қоғам институтының ұлттық қауіпсіздігін қамтамасыз ету жүйесінде елеулі қауіп төндіретін "ауызша/ақпараттық экстремизмнің" пайда болуының катализаторына айналды. Өздеріңіз білетіндей, бұл мәселедегі ең өзекті және маңызды аспект-бүкіл әлем бойынша цифрлық платформалардың негізгі тұтынушысы-экстремистік топтардың идеологиялық өңдеу және жалдау тәуекелдеріне сәйкес келетін жастар. Демек, осы зерттеу жастар мен жалпы Қазақстан халқы арасында ауызша экстремизмнің алдын алу және оған қарсы іс-қимыл шараларын іске асырудың мемлекеттік саясатының тиімділік дәрежесін талдауға бағытталған. Осы саладағы проблемаларды анықтау және бағалау пәнаралық әдіснамалық парадигма арқылы жүзеге асырылады, оның эмпирикалық бөлігіне Үкіметтің статистикалық есептерін, халықаралық ұйымдардың аналитикалық есептерін ұсыну, цифрлық қосымшаларды айналып өтудің техникалық бұғаттаулары мен технологияларын талдау және әртүрлі платформалар арасындағы цифрлық радикалданудың "көші-қон" мүмкіндіктерін қарастыру кіреді. Мәселен, мақалада Мемлекет, домендер мен материалдар тұрғысынан күмәнді органдардың айтарлықтай бұғатталуына әкелген мемлекеттік органдардың қызметі көрсетілген. Авторлардың көзқарасы бойынша, мұндай әрекет ету тәсілдері оң нәтижелерге әкелуі мүмкін, бірақ олар тыйым салынған сайттарға кіруге болмайтындығына толық кепілдік бермейді – оларды аталған қосымшалар арқылы айналып өтіп, бір уақытта жасырын ұстауға болады. Қоғамдағы әлеуметтік-саяси және мәдени тұрақтылықты қамтамасыз ету шеңберінде экстремистік қызметке қарсы күресте тек тежеу саясаты мен шектеу шараларының болуы жеткіліксіз. Көп қырлы және кешенді мемлекеттік саясатқа көшу керек, онда басымдықтар білім деңгейін, сыни сананы, цифрлық медиа сауаттылықты және қоғамдағы мәдени-құндылық бағдарларын арттыру пайдасына қойылуы тиіс.

**Түйін сөздер:** ауызша экстремизм, Қазақстан, мемлекеттік шаралар, жастар, интернет-кеңістік, радикалдандыру, қарсы насихаттау.

*E. Aliyarov<sup>1</sup>, D. Zhanguzhekova<sup>1\*</sup>*

*<sup>1</sup>Kazakhstan Center for Humanitarian and Political Studies,  
Almaty, Kazakhstan*

*\* e-mail: [dinara.zhanguzhekova@gmail.com](mailto:dinara.zhanguzhekova@gmail.com)*

## ISSUES OF THE EFFECTIVENESS OF STATE MEASURES TO COUNTER VERBAL EXTREMISM IN KAZAKHSTAN'S INTERNET SPACE

### *Abstract*

The rapid development of information and communication technologies has become a catalyst for the emergence of "verbal/informational extremism", which poses a serious threat to the national security system of the institution of the state and society. As you know, the most relevant and significant aspect of this issue is the fact that the main consumers of digital platforms around the world are young people, who are therefore at risk of indoctrination and recruitment by extremist groups. Therefore, the present study is aimed at analyzing the degree of effectiveness of the state policy of implementing preventive and counteraction measures to verbal extremism among young people and the general population of Kazakhstan. The identification and assessment of problems in this area is carried out through an interdisciplinary methodological paradigm, the empirical part of which includes the presentation of government statistical reports, analytical reports from international organizations, as well as an analysis of technical blocking and circumvention technologies for digital applications, and consideration of the possibilities of "migration" of digital radicalization between different platforms. Thus, the article

demonstrates the activities of government agencies, which led to significant blocking of dubious domains and materials from the point of view of the state. From the authors' point of view, such response approaches probably lead to positive results, but they do not provide a complete guarantee that there will be no access to prohibited sites – they can be circumvented using these applications and at the same time maintain anonymity. The existence of restrictive policies and restrictive measures alone is insufficient to combat extremist activity within the framework of ensuring socio-political and cultural stability in society. It is necessary to switch to a more multifaceted and comprehensive public policy, where priorities should be set in favor of improving the level of education, critical awareness, digital media literacy and cultural and value orientations in society.

**Keywords:** verbal extremism, Kazakhstan, government measures, youth, Internet space, radicalization, counter-propaganda.

### **Введение**

Современная эпоха характеризуется повсеместным внедрением информационно-коммуникационных технологий в качестве краеугольного камня человеческого существования, выходящего за рамки традиционных границ и переосмысливающего межличностное общение, политический дискурс и социокультурные рамки. Цифровые платформы и интерфейсы превратились в основное связующее звено между человеком и объективным миром, фундаментально оптимизирующее системную функциональность и рациональную эффективность в различных сферах жизни общества. В рамках этой цифровой парадигмы глобальная сеть играет двойственную и беспрецедентную роль самого влиятельного канала связи в мире, обладающего исключительной способностью распространять как конструктивные идеи развития, так и глубоко дестабилизирующие и разрушительные информационные потоки. Согласно мнению специалистов, «глобальная информатизация и развитие Казнета, с одной стороны, и неготовность государства и бизнеса к этому с другой стороны, привели к тому, что информационно-коммуникационная инфраструктура страны и национальные информационные ресурсы оказались самыми уязвимыми объектами воздействия со стороны недружественных государств, террористических организаций, криминальных групп, отдельных злоумышленников и специально созданного компрометирующего материала» (Vechkinzova et al., 2019).

Актуальность данного исследования подчеркивается беспрецедентным ростом мировой интернет-аудитории – по заявлению ООН, в 2025 г. интернетом пользуются уже больше половины человечества – 6 млрд. пользователей (“V mire naschitali...”, 2025). В том же отчете ООН отмечается высокая степень вовлеченности молодежи 15-24 лет – 82% из них находятся в режиме онлайн. Следовательно, преобладающая часть повседневной сознательной жизни современной молодежи неразрывно связана с цифровым подключением, что значительно повышает риск того, что податливые когнитивные структуры будут подвержены воздействию злокачественных или деструктивных информационных потоков. Взаимосвязь между молодежной демографией и информационным экстремизмом характеризуется симбиотической синергией, прежде всего потому, что молодое поколение представляет собой основную и наиболее активную базу потребителей современной инфраструктуры массовых коммуникаций. В рамках этой парадигмы быстрое развитие телекоммуникационных технологий превратилось в стратегическое убежище для экстремистской мобилизации, пропаганды и вербовки, что фактически сводит на нет необходимость в физической межличностной близости. Используя виртуальные каналы, включая цифровые манифесты, мультимедийные артефакты и онлайн-дискурс в режиме реального времени, радикальные организации теперь могут оказывать глубокое социально-психологическое влияние и способствовать идеологической синхронизации удаленно, достигая своих оперативных целей посредством изолированного манипулирования цифровой псевдосредой. Исследователи отмечают, что «экстремистский характер злоупотребления правом проявляется в информационной сфере тогда, когда институциональные субъекты реализуют свои субъективные права на производство, распространение и доступ к информации, осуществляя при этом воздействие, ставящее целью изменение личностных установок,

идеологии, принципов, мировоззрения, приводящее к соответствующему индивидуальному или групповому поведению, а также созданию общественного мнения, выгодного воздействующей стороне... эта деятельность провоцирует этнополитическую, социально-экономическую, институционально-правовую и духовно-нравственную нестабильность, способствует ослаблению национальной государственности, порождает сепаратистские настроения, религиозную и иную нетерпимость и т.п.» (Upornikov, 2007).

Целью исследования является оценка эффективности государственных мер по противодействию информационному экстремизму среди молодежи Казахстана и анализ конкретных механизмов цифровой радикализации. Исследование основано на гипотезе о том, что преимущественная стратегия госполитики Казахстана в рамках технической блокировки ограничена в эффективной реализации данной сферы вследствие постоянно изменчивого характера примененных тактик и технологий экстремистских акторов, а также ввиду возможности сохранения их анонимности.

*Обзор научной литературы.* Тематика исследования является объектом для изучения многих социогуманитарных наук. Теоретическая основа для понимания типологических основ и неотъемлемых характеристик экстремизма заложена в серии фундаментальных классических исследований. Интеллектуальная значимость в этой области принадлежит основополагающим работам Э. Хоффера (Hoffer, 1951), Х. Арендт (Arendt, 1951) и Э. Фромма (Fromm, 1973), чьи философские и политические взгляды структурно дополнены строгими таксономическими рамками, разработанными Д. Рапопортом (Rapoport, 2004), Р. Гриффином (Griffin, 2012) и Дж.Б. Бауэром (Bowyer, 1979). Параллельно с этими глобальными академическими традициями отечественный исследовательский ландшафт в Казахстане накопил значительный объем знаний об угрозах радикализации. Региональное научное повествование формируется, в частности, благодаря авторитетному вкладу К. Бурханова и Д. Сатпаева (Burkhanov et al., 2000), наряду с существенными запросами М. Лаумулина (Laumulin, 2019), А. Сабдина, А. Гусаровой (Gusarova, 2019), А. Чеботарева (Chebotarev, 2016), Е. Карина (Karin, 2014), А. Решетняка (Reshetnyak, 2016), Г. Жусуповой (Zhusupova, 2009), С. Бейсембаева и Д. Шариповой (Beissembayev, 2019), (Sharipova & Beissembayev, 2021).

Фундаментальный научный вклад в изучение сложной социально-политической динамики молодежной демографии и сопутствующих рисков ее вовлечения в экстремистскую мобилизацию представлен новаторскими исследованиями К. Мангейма (Mannheim, 1943) и Ш. Эйзенштадта (Eisenshtadt, 2017). Эта теоретическая связь еще больше подкрепляется важными аналитическими разработками Р. Томпсона (Thompson, 2012), П. Ньюмана (Neumann, 2016) и Э.Бриггса (Briggs, 2011), чьи коллективные исследования выявляют системные уязвимости и психологические предпосылки, способствующие переходу от социального отчуждения к радикализированной деятельности.

В рамках научного дискурса, посвященного системным уязвимостям и экзистенциальным опасностям информационной эры, обширный массив теоретической литературы обеспечивает концептуальную основу для определения природы этих цифровых явлений. Основополагающие взгляды на сложность и системные нарушения изложены в фундаментальных исследованиях Э.Лоренца (Lorenz, 1996) и Дж. Глейка (Gleick, 1987), которые структурно дополнены критическими оценками информационной войны П. Вирилио (Virilio, 2002) и У. Липпмана (Lippmann, 1922), а также теорией сетевого общества М. Кастельса (Castells, 1998). Психологических и манипулятивных аспектов коммуникативной сферы дополнительно освещены авторитетным вкладом Х. Ингрэма (Ingram, 2014), Э. Бернейса (Bernays, 1928). Особое значение имеет постулат Липпмана о «псевдосреде» – когнитивном посреднике, через который индивиды воспринимают объективную реальность и взаимодействуют с ней; в рамках этой парадигмы деятельность человека в основном опосредована стереотипными стимулами, генерируемыми этим искусственным информационным слоем (Lippmann, 1922).

Параллельно казахстанское академическое сообщество разработало всеобъемлющее локальное представление об этих цифровых угрозах. Социологические и политические

последствия для республики тщательно изучены в коллективном исследовании Ж.К. Букановой, Ж.К. Каримовой, Л.М. Амреевой и Л.Ю. Зайниевой (Bukanova et al., 2014), а также в специальных исследованиях С.И. Каракушева и К.Б. Токкожина (Karakushev et al., 2016), посвященных вопросам безопасности. Кроме того, правовые и технологические проблемы интернет-пространства рассматриваются в работах Э.С. Сапаровой, Е.Т. Омиржанова (Saparova & Omirzhanov, 2016), Л. Татариновой (Tatarinova, 2019) и Д. Заурбекова (Zaurbekov, 2021). Современные аналитические взгляды на цифровой дискурс и социальную динамику также представлены Ш. Мусиралиевой, М. Болатбек (Mussiraliyeva et al., 2024) и др. М. Сакенова особо подчеркивает важную роль глобальных сетей в содействии идеологической мобилизации и вербовке молодежи, которая определяет цифровую среду как основной канал радикализации: «наиболее уязвимые слои населения, подверженные данной идеологии – это молодежь. Радикально настроенная молодежь снабжена всей необходимой литературой, им доступны все информационные каналы, их учителя благополучно получают образование в Египте, Саудовской Аравии, Пакистане. Именно среди молодежи все чаще затрагиваются сложные вопросы исламского права и исламского вероубеждения, в том числе обсуждение вопроса о произнесении “аминь” вслух или про себя, вопрос о поднятии рук перед и после руку, празднование Мавлида, и т.п. Сегодня салафитами, в том числе экстремистским течением такфиритов, используется всем известный интернет. Всемирная паутина вам не только растолкует истины религии, но и расскажет о том, как вести “джихад”. После чего молодые люди просто уходят из домов, бросая родителей и семьи, для того чтобы “служить” религии в своем специфическом понимании. Позже через месяцы, а то и года, родители внезапно узнают, что пропавший ребенок – на учебе, только это не привычные для нас университеты, а “спецкурсы” по тому, как “бороться” с “неверными”» (“Agentstvo po delam religii ...”, 2013).

### **Методология исследования**

Методологическая основа данного исследования базируется на всеобъемлющей междисциплинарной парадигме, сочетающей концептуальный набор инструментов политологии, социологии и социально-правовых исследований с передовыми технологическими оценками. Этот многомерный эпистемологический подход специально разработан для того, чтобы облегчить тщательную оценку стратегических инициатив правительства, уделяя особое внимание их эффективности в смягчении последствий и предотвращении распространения вербального экстремизма. Объединяя эти разнообразные аналитические инструменты, исследование направлено на анализ эффективности национальных профилактических мер, переходя от изолированной юридической или технической критики к целостной оценке государственной политики по борьбе с радикализацией в цифровую эпоху. Учитывая то, что современный экстремизм стал новой формой международной и национальной информационной безопасности, авторы сочли логичным и обоснованным применение качественного исследовательского подхода, ориентированного на системный анализ существующих проблем в данной сфере. Системность в методологическом инструментарии предполагает, что вербальный экстремизм рассматривается не только как техническая проблема, а в качестве деструктивной социально-политической силы, которая целенаправленно использует возможности «компьютерного переворота» с целью влияния и на сознание и идеологию современной молодежи.

Настоящее исследование носит, прежде всего, оценочный характер и ориентировано на оценку степени эффективности профилактических и технических мер правительства в отношении интернет-пространства, включая методы блокировок веб-ресурсов.

Для того, чтобы всецело обеспечить комплексную оценку вопроса, в исследовательской работе применяется гибридная методология количественного и качественного анализа, куда входят официальные государственные отчеты и доклады, оценка современных интернет-технологий, а также анализ дискурса. Первичная источниковая база состоит из официальной правительственной статистики и заключительных аналитических докладов Государственной

программы по противодействию религиозному экстремизму и терроризму в РК, а также текущих данных по наблюдению функционирования информационной системы «Кибернадзор». Изучая данные, которые представлены Комитетом национальной безопасности Республики Казахстан, — о блокировке более 620 тысяч экстремистских материалов и 38 тысяч доменов, в исследовательской работе определяется исходная информация для выявления и измерения государственной регуляторной деятельности.

Основополагающим элементом методологического инструментария исследования послужил технологическая оценка механизмов и подходов обхода предпринятых правительством мер блокировок посредством таких виртуальных частных приложений и сетей, как VPN и (TOR). Подобный анализ необходим для раскрытия ограничений и возможностей традиционных механизмов государственной профилактики и контроля в свете применения технологий обхода технических блокировок. В работе анализируется политика «миграции» экстремистского контента между социальными сетями и платформами — это, к примеру, переход с Facebook и YouTube на более и менее зашифрованные мессенджеры, такие как Telegram и TamTam. Такие ключевые изменения рассматриваются в качестве основных показателей пределов государственного контроля. Этому этапу исследования характерно применение качественного тематического анализа конкретных кейсов, связанных, например, со сбоем в работе различных стратегических служб обмена сообщениями по всей стране в 2018 г., с целью оценки реакции гражданского общества и IT-групп на проводимые правительством «технические работы».

И, наконец, в настоящем исследовании применяется компаративистский метод, который позволяет сопоставить определенную степень зависимости государства от реактивных и агрессивных технических мер жизненной необходимости осуществления идеологической контрпропаганды.

Определяя и оценивая актуальную «псевдосреду», сформированную экстремистскими сообществами в информационном пространстве, изложенная методология исследования стремится представить обоснование перехода от преимущественно ограничительных мер и стратегий государства к комплексной, многогранной политике, включая учет культурно-ценностных аспектов, медиаграмотность и использование высококачественного видеоконтента. Хронологический охват данного исследования охватывает 2013-2026 гг., что позволяет масштабно и всесторонне объяснить ту степень адаптации государственных мер к глобальным цифровым потокам, которая на сегодня связана со всеми системами международного пространства.

Следует также упомянуть, что все исследовательские процедуры проводились в соответствии с этическими нормами и стандартами социальных исследований с применением общедоступных официальных отчетов и аналитических докладов, а также с обеспечением анонимности акторов в применимой цифровой среде.

### **Результаты исследования**

Усиление внимания исполнительной власти к радикальным идеям, распространяемым по цифровым каналам связи, достигло поворотного момента с официальной ратификацией Государственной программы по противодействию религиозному экстремизму и терроризму в Республике Казахстан на 2013-2017 гг. Эта стратегическая инициатива ознаменовала переход к более строгому нормативному надзору за национальным информационным пространством. В заключительном аналитическом обзоре, подготовленном Комитетом национальной безопасности по завершении проекта, содержался всесторонний оценочный отчет о масштабах государственного вмешательства, документально подтверждающий, что «...в целях ограждения пользователей Интернет и социальных сетей от влияния пропаганды терроризма проводится мониторинг информационного пространства на предмет соблюдения законодательства РК. В интернете и социальных сетях заблокировано более 620 тыс. материалов (2015 – 150 тыс., 2016 – 700 тыс.) с пропагандой терроризма и экстремизма» (Исабаева, 2020).

Согласно оценкам последних данных, государственная система «Кибернадзор» выявила 38 тысяч запрещенных сайтов, которые были заблокированы в дальнейшем (“Bolee 38 tysyach saitov...”, 2025). Результаты анализа государственной политики в борьбе с распространением и пропагандой экстремистских идей, а также с вербальной вербовкой, демонстрируют, что техническая блокировка интернет-ресурсов зачастую не приводят к полному прекращению сетей распространения; они успешно функционируют в специализированных каналах интернет-пространства – к ним имеется определенный доступ, несмотря на запреты и ограничения, предпринятые государственными органами. Такие системные браузеры, как Virtual Private Network (VPN) и The Onion Router (TOR), позволяют справиться с данной задачей, а наиболее «мотивированные» и знающие, или столкнувшиеся ранее с блокировками, слои населения умело могут противостоять таким техническим барьерам. Важно отметить, что применение данных защитных системных платформ само по себе не представляет уголовное правонарушение. Это утверждение имеет особый правовой статус и было подкреплено резолюцией Совета по правам человека Организации Объединенных Наций в 2015 г. (“OON priznala anonimnost ...”, 2015).

Функциональная задача VPN состоит в конструировании так называемой туннелированной защиты цифрового пространства – оно заменяет стандартные протоколы прямого подключения доменов. В обычных сетевых случаях попытки пользователей войти в тот или иной заблокированный правительством запрещенный веб-сайт сразу же перехватываются, а провайдер немедленно подобные попытки регистрирует. Правоохранительные органы соответствующих юрисдикций имеют доступ к подобным транзакциям несанкционированного входа местных пользователей. Но сетевой браузер VPN в большинстве своем нарушает эту возможность отслеживать за трафиком пользователей, поскольку оно выступает в качестве посредника и перенаправляет его веб-домен на другие идентификаторы. Суть парадигмы VPN состоит в том, чтобы разработать безопасное сквозное шифрование и всесторонне исказить исходный географический цифровой идентификатор входящего пользователя. В случаях, когда маскируется IP-адрес, к примеру, исходящий адрес из Казахстана заменяется удаленным идентификатором под иностранной юрисдикцией, например, Германии, данный браузер формирует замкнутую связь передачи данных. Стало быть, VPN всецело способствует созданию щита, как от государственных органов надзора, так и от поставщиков коммуникационных услуг на характер активности веб-пользователя, его просматриваемых сайтов и каналов, загрузок, полностью обеспечивая непрозрачность от внешнего наблюдения.

Особого внимания и аналитического разбора требует функциональная деятельность системного браузера The Onion Router (TOR), который отличается многоуровневым техническим содержанием. Изначально данная платформа была разработана в Соединенных Штатах в качестве секретной технологии обеспечения конфиденциальности пересылаемых информационных материалов вооруженных сил; далее этот инструмент претерпел значительные изменения и стал достоянием общества. Как только военные усовершенствовали систему безопасности на базе VPN, приложение TOR официально был объявлен как легальный программный способ входа в глобальную сеть в режиме анонимности, и как защитный способ несанкционированного контроля со стороны правительств, военных, и других акторов.

Помимо того, что TOR в функционально-содержательном плане схож с VPN, он в отличие от VPN имеет уникальную техническую способность объединять децентрализованные домены, что способствует созданию параллельной цифровой системы, которую часто называют «интернет в интернете». Фундаментальная проблема для институционального надзора заключается в том, что эти скрытые сервисы недоступны. Они доступны исключительно с помощью специализированного программного обеспечения, что делает их невидимыми для обычных поисковых систем и стандартных протоколов просмотра. Следовательно, эта децентрализованная инфраструктура остается в значительной степени неподвластной контролю какой-либо национальной юрисдикции. Как подчеркивают современные ИТ-специалисты, устойчивый и распределенный характер сети TOR делает любые попытки государства по всеобъемлющему систематическому приостановлению работы технически неосуществимыми (Çalışkan et al., 2015).

Сеть TOR содержит огромное количество специализированных децентрализованных хранилищ, которые представляют собой серьезную системную угрозу национальной безопасности. Благодаря относительно несложным навигационным процедурам участники могут получить доступ к обширным объемам вредоносных данных и ресурсов. Несмотря на то, что правоохранительные органы имеют определенные технические возможности, которые нужны для раскрытия зашифрованных посредством браузеров VPN и TOR лиц и участников, но выстроенные в их системах технические ограничения в полной мере не обеспечивают раскрытия многих факторов.

Помимо указанных браузеров, цифровой коммуникационный сегмент преобразился и усложнился добавлением в него сетевых платформ быстрого обмена сообщениями – мессенджерами. В частности, для казахстанского общества стали наиболее популярными такие мессенджеры, как WhatsApp и Telegram, руководство которых с большой долей вероятности заявляют об их надежности. Следовательно, категория надежности играет весомую и положительную роль в контексте масштабного распространения радикальных идей, а также представляет собой основу материально-технического и финансового оснащения экстремистских и террористических ячеек.

Telegram в определенной степени является лидером среди информационных коммуникационных технологий благодаря усложненной системе шифрования и защиты личных данных. По официальным заявлениям Службы государственной безопасности Бельгии в течение 2017-2018 гг., экстремисты и террористы Исламского Государства постепенно перешли от более популярных социальных сетей и видео-платформ, как Facebook, Instagram, Twitter и YouTube, внедрившие серьезную систему отслеживания и модерации постов, к наиболее скрытой платформе Telegram для успешного распространения и пропаганды своих идей (“Teroristy rasprobovali Telegram...”, 2018). Данная социальная сеть обрела широкую популярность среди боевиков, прежде всего, за счет принципиального подхода основателя Павла Дурова к защите личных данных пользователей. Несмотря на то, что в 2017 г. его компания внедрила в систему протоколы для ограничения некоторых каналов, инициированные меры не были столь эффективными и оптимальными с точки зрения обеспечения информационной безопасности (“VKontakte sostavila...”, 2017). Учитывая слабые стороны ограничительных мер, экстремистские и террористические группировки расширили и увеличили количество своих цифровых мультязычных каналов до 1000 разнообразных форматов – это видео и аудио материалы, фото и рисунки с высоким разрешением, документальные фильмы, периодические издания и т.д. (“Telegram nashel...”, 2017).

Наиболее серьезный прогресс в информационном сетевом сегменте был обозначен в ноябре 2019 г., когда руководство Telegram проводило «чистку», отключив более 5 тысяч каналов, связанных с Исламским государством. Деятельность правоохранительных органов стала важнейшим фактором массовой цифровой миграции – экстремистские группировки переходили на мессенджер под названием TamTam, цифровую платформу под руководством Mail.ru. Оперативность и эффективность этих переходов проявилась во время Лондонского теракта в ноябре 2019 г., когда официальные лица ИГ появились в этом мессенджере за 2 минуты раньше, чем эта информация была распространена через Telegram (“Teroristy ushli iz Telegram...”, 2019). Несмотря на то, что впоследствии в Telegram было удалено около 50 каналов радикального характера, данные коммуникационные узлы были благополучно восстановлены на TamTam в течение одних суток.

В марте 2018 г. в Казахстане наблюдались масштабные перебои с подключением к интернету. Власти объясняли причину данных перебоев «техническими моментами» (“Sboi v rabote Telegram...”, 2018), которые ориентированы на уничтожение незаконных материалов со стороны «Демократического выбора Казахстана» – организации, объявленной правительством экстремистской. Однако это регулирующее вмешательство столкнулось со значительным противодействием со стороны гражданского общества, представителей средств массовой информации и IT-сообщества. Наряду с этим, результаты исследования показывают о возможности использования

обходов с помощью VPN, что позволяет сохранять полную функциональность платформ, несмотря на попытки их официальной блокировки.

### Обсуждение

Принимая во внимание результаты исследования, следует отметить, что государственная администрация остро осознает тот факт, что распространение сложных средств обхода ограничений в корне подрывает целостность национальных стратегических инициатив, направленных на нейтрализацию запрещенного контента. Несмотря на то, что статья 21 недавно ратифицированной Конституции Республики Казахстан прямо закрепляет «право на неприкосновенность частной жизни, личную и семейную тайну, защиту персональных данных от их незаконного сбора, обработки, хранения и использования, в том числе с применением цифровых технологий, гарантируется законом» (“Constitution of the Republic...”, 2026), де-юре сохраняются серьезные разногласия по поводу защиты персональных данных в цифровой среде, и присутствует фактическое несоответствие в его практическом применении. Отечественная цифровая среда характеризуется нормативно-правовой базой, позволяющей вводить ограничения в интернете по административным, судебным или дискреционным каналам, однако он страдает от институционального отсутствия прозрачных механизмов восстановления контента или публичного раскрытия информации о доменах с ограниченным доступом. Эта системная неопределенность свидетельствует пример с судебным запретом премиум VPN-сервиса «IPVanish.com» в марте 2018 года (“VPN-servis zablokiroval...”, 2018). Оправдывая эту интервенционистскую позицию, министр информации и коммуникации пояснил, что «требования об ограничении доступа к интернет-ресурсу были включены в исковые заявления МИК, которое было подано в суды Астаны и Алматы, в связи с тем, что VPN-сервис используется для обхода технических возможностей операторов связи, применяемых для нераспространения в стране незаконных материалов» (“VPN-servis zablokiroval...”, 2018).

В то время как институциональное намерение государства оградить граждан от экстремистских высказываний в основе своей рационально, оперативные механизмы, используемые в настоящее время для достижения этой цели, все чаще имеют характер ограниченной эффективности. Более того, усиливающиеся запретные действия государства в отношении определенных веб-доменов и браузера VPN вызвали серьезное осуждение со стороны мирового правозащитного сообщества, так как данные меры рассматриваются в качестве посягательства на естественные права человека, прописанные и утвержденные ООН и другими международными правовыми организациями.

Ввиду изложенных многоаспектных вопросов авторами предлагается делать акцент на комплексное культивирование ценностно-идеологических установок и норм в казахстанском социуме, в частности на уязвимых молодых людей и детей. Данная задача требует критического восприятия двух базовых аспектов – концептуально-методологической основы передачи информации, а также качества содержания информации и информационных потоков.

Как известно, передача онлайн-информации осуществляется через медиа посредством различных форматов – это аналитические, новостные тексты, визуальные артефакты, аудио-и-видео материалы. В иерархии ИКТ видео-форматы играют особую аналитическую роль благодаря своему уникальному содержанию, где сбалансированно и гармонично встраиваются слуховые и визуальные аспекты, что усиливает психологический эффект и вовлечение необходимой аудитории. Серьезное преимущество видео-форматов подтверждается результатами исследований зарубежных и отечественных авторов. Так, согласно оценкам Института изучения журналистики Reuters, уже 2016 году мировая информационная сеть стала свидетелем непомерного роста видео-контентов (Karogelorous et al., 2016). За кратчайшие сроки эта практика становится совершенной нормой для субъектов, касающихся традиционной журналистики, специализированных информационных агентств и служб, а также отдельных участников, деятельность которых связана с быстрым распространением информации в интернет-

пространстве. Масштабное внедрение высококачественных смартфонов, которые оснащены дисплеями с высокой четкостью и понятным, интересным интерфейсом, позволило сделать более демократизированным и повсеместным процесс производства видео-контентов.

Этот сдвиг парадигмы был еще более ускорен систематической оптимизацией инфраструктуры мобильных сетей и последующим снижением тарифов на передачу данных. Крупнейшие архитектуры социальных сетей, включая Facebook, Twitter и ВКонтакте, стратегически использовали эти технологические достижения; например, к 2015 году количество просмотров видео на Facebook выросло на беспрецедентные 75%, достигнув стратегической отметки в 8 млрд. ежедневных просмотров (Karogelopoulos et al., 2016).

При рассмотрении социокультурного аспекта национальной жизнестойкости крайне важно культивировать глубокое уважение к основополагающим культурным нормам и ценностям, не впадая при этом в регрессивный традиционализм. В то время как уникальные культурные особенности казахского народа должны оставаться неотъемлемой частью национальной идентичности в условиях неизбежного давления глобальной интеграции и межкультурного синтеза, существует острая необходимость преодолеть архаичные когнитивные рамки в бытовой, социальной и политической сферах. Этот переход к модернизированным интеллектуальным парадигмам, по сути, является длительным процессом; однако требования нынешней обстановки в области безопасности требуют немедленных идеологических результатов. Следует признать, что экстремистские деятели используют радикализированную интерпретацию веры в качестве обобщающего показателя всей человеческой деятельности. Следовательно, стратегический приоритет должен быть отдан усилению дихотомии между свободой личности, определяемой личной свободой и приверженностью правовым системам, ориентированным на человека, и догматическим подчинением, которого требуют радикальные взгляды. Этот аналитический контраст не менее важен в контексте института семьи, где современные эгалитарные модели отношений должны сознательно противопоставляться регрессивным и патриархальным структурам, типичным для религиозно-экстремистских сред.

### **Заключение**

Современная информационная экосистема республики, отражающая общемировые тенденции, в настоящее время переживает период глубоких структурных метаморфоз. Эта системная эволюция обусловлена сложной конвергенцией многогранных социально-политических и экономических факторов, неразрывно связанных со стремительным развитием цифровых платформ и социальных сетей. В крайне короткие сроки цифровые медиа ресурсы стали главными преобразователями Вселенной, способствуя трансформации классических мировоззрений, а традиционные социокультурные паттерны практически неузнаваемыми. Согласно Окинавской хартии Глобального информационного общества, «...информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, образования и трудовой деятельности, а также организации взаимодействия правительства и гражданского общества. Информационно-коммуникационные технологии быстро становятся жизненно важным стимулом развития мировой экономики» (“Okinawa Charter...”, 2000). Рассматривая современное развитие национальных государств, следует подчеркнуть, что оно в значительной мере выходит за рамки территориальной целостности, экономического, социального развития – оно во многом требует серьезной защиты и заботы культурно-духовного составляющего. Но данный важный нематериальный элемент национальной безопасности зачастую подвергается глубоким и системным угрозам, рискам. Всеохватывающий «компьютерный переворот» не только модернизирует уровень технологического развития человечества, но и способствует значительному изменению человеческого сознания, ее идейных основ и концептуальных парадигм. Объективно считать, что республика по-прежнему остро нуждается в защите ее фундаментальных нормативно-ценностных установок в контексте усиливающейся цифровой системы.

Для технологически развитых государств, которые постоянно совершенствуют сложные архитектуры для защиты информации и тайного проникновения данных, Республика рискует стать прозрачной мишенью для стратегического внешнего воздействия. В данном отношении значительной угрозой выступает вербальный экстремизм и его последствия на граждан Казахстана, в частности на неподготовленную молодежь и детей, которые выступают главным потребителем интернет-услуг. Более того, следует подчеркнуть, что общество имеет существенный опыт в использовании таких приложений и браузеров во время Январских событий.

Обобщение вышеупомянутых наблюдений подчеркивает институциональный императив разработки надежных методов работы в сфере образования, науки и просвещения – технические запреты и блокировки со стороны правительства не являются достаточной мерой по борьбе с информационным экстремизмом. Достижение этой цели требует, прежде всего, тщательной кодификации нормативно-правовых стандартов, дополненной установлением основополагающих принципов, обеспечивающих их строгое и бескомпромиссное применение. Эти стратегические механизмы должны служить основополагающими элементами современной архитектуры национальной безопасности Казахстана и основой его долгосрочной государственной политики.

### **Финансирование**

Авторы заявляют, что для проведения исследования и/или публикации данной статьи была получена финансовая поддержка. Статья подготовлена в рамках программно-целевого финансирования Комитета науки Министерства науки и высшего образования Республики Казахстан (BR27195711 «Социально-политические процессы в Казахстане (1980-2020): опыт демократизации и становление Справедливого государства»).

### **Конфликт интересов**

Авторы заявляют, что исследование проводилось в отсутствие каких-либо коммерческих или финансовых отношений, которые могли бы быть истолкованы как потенциальный конфликт интересов.

### **Вклад авторов**

ЕА: написание – первоначальный проект, концептуализация, формальный анализ, привлечение финансирования. ДЖ: написание и редактирование, методология, контроль за продвижением статьи.

### **References:**

Agentstvo po delam religii RK: Kto takie salafity i kak s nimi borot'sya? [Agency for Religious Affairs of the Republic of Kazakhstan: who are Salafists and how to deal with them?] (2013, September 23). *Zakon.kz*. Retrieved June 13, 2026, from [https://online.zakon.kz/Document/?doc\\_id=31447175#pos=3;-81](https://online.zakon.kz/Document/?doc_id=31447175#pos=3;-81)

Arendt, H. (1951). *The origins of totalitarianism*. Harcourt, Brace & Co.

Beissembayev, S. (2019). Aspekty gosudarstvennoi politiki v oblasti predotvrashcheniya ekstremizma v Kazakhstane [Aspects of state policy in preventing extremism in Kazakhstan]. *Bulletin of L.N. Gumilyov Eurasian National University*, 128(3), 155-163. <https://doi.org/10.32523/2616-6895-2019-128-3-155-16>

Bernays, E. L. (1928). *Propaganda*. Horace Liveright.

Bolee 38 tysyach saitov zablokirovali v Kazakhstane [More than 38 thousand websites have been blocked in Kazakhstan] (2025, November 24). *Ratel.kz*. Retrieved June 13, 2026, from [https://ratel.kz/outlook/bolee\\_38\\_tysyach\\_sajtov\\_zablokirovali\\_v\\_kazahstane](https://ratel.kz/outlook/bolee_38_tysyach_sajtov_zablokirovali_v_kazahstane)

Bowyer, B.J. (1979). *Terror out of Zion: Irgun Zvai Leumi, LEHI, and the Palestine underground, 1929-1949*. Academy Press.

Briggs, E. (2011). *The Munich massacre: A new history*. University of Sydney.

Bukanova, Zh.K., Karimova, Zh.K., Amreeva, L.M., & Zainieva, L.Yu., et al. (2014). Natsionalnyi doklad «Molodezh Kazakhstana – 2014» [National report “Youth of Kazakhstan – 2014”]. NITs “Molodezh”.

Burkhanov, K., Karin, E., Satpayev, D., & Davydova, I. (2000). *Ekstremizm v Tsentralnoi Azii* [Extremism in Central Asia]. Institut Rossii i Kitaya.

Castells, M. (1998). *The information age: Economy, society and culture*. Blackwell.

Chebotarev, A. (2016, May 16). Ekstremizm v Kazakhstane: Sovremennoe sostoyanie i voprosy protivodeistviya [Extremism in Kazakhstan: Current state and issues of counteraction]. *CABAR.asia*. Retrieved May 24, 2026, from <https://cabar.asia/ru/andrej-chebotarev-ekstremizm-v-kazahstane-sovremennoe-sostoyanie-i-voprosy-protivodejstviya/>

Constitution of the Republic of Kazakhstan. (2026, June 15). *Adilet*. Retrieved June 30, 2026, from <https://adilet.zan.kz/rus/docs/K2600000000>

Eisenshtadt, Sh.N. (2017). *From generation to generation: Age groups and social structure*. Taylor & Francis.

Fromm, E. (1973). *The anatomy of human destructiveness*. Holt, Rinehart and Winston.

Gleick, J. (1987). *Chaos: Making a new science*. Viking.

Griffin, R. (2012). *Terrorist's creed: Fanatical violence and the human need for meaning*. Palgrave Macmillan.

Gusarova, A. (2019, November 22). Osobennosti protivodeistviya nasilstvennomu ekstremizmu i terrorizmu v Kazakhstane [Features of countering violent extremism and terrorism in Kazakhstan]. *CABAR.asia*. Retrieved May 24, 2026, from <https://cabar.asia/ru/osobennosti-protivodejstviya-nasilstvennomu-ekstremizmu-i-terrorizmu-v-kazahstane/>

Hoffer, E. (1951). *The true believer: Thoughts on the nature of mass movements*. Harper & Brothers.

Ingram, H.J. (2014). *The charismatic leadership phenomenon in radical and militant Islamism*. Routledge.

Isabayeva, S.B. (2020). *Obespechenie kiberbezopasnosti Kazakhstana v usloviyakh globalnoi tsifrovizatsii* [Ensuring cybersecurity in Kazakhstan in the context of global digitalization] [Doctoral dissertation]. Nur-Sultan.

Karakushev, S.I., Tokkozhin, K.B., & Tnymov, A.M. (2016). *Pravovye i organizatsionnye osnovy protivodeistviya molodezhnomu ekstremizmu (problemy teorii i praktiki)* [Legal and organizational foundations for countering youth extremism: Problems of theory and practice]. Aktobe Legal Institute of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Bukenbayev.

Karin, E. (2014). *Soldaty khalifata: Mify i realnost* [Soldiers of the caliphate: Myths and reality]. VMG Consultancy.

Kalogeropoulos, A., Cherubini, F., & Newman, N. (2016). *The future of online news video*. Reuters Institute for the Study of Journalism. <https://doi.org/10.60625/risj-ftg2-zc61>

Laumulin, M. (2019). Evolyutsiya vospriyatiya terroristicheskoi i ekstremistskoi ugrozy [Evolution of perceptions of the terrorist and extremist threat]. In Z.K. Shaukenova (Ed.), *Profilaktika ekstremizma. Uspekhi i trudnosti* [Prevention of extremism: Successes and difficulties], 141-147. Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan.

Lippmann, W. (1922). *Public opinion*. Harcourt, Brace and Company.

Lorenz, E. (1996). *The essence of chaos*. University of Washington Press.

Mannheim, K. (1943). *Diagnosis of our time: Wartime essays of a sociologist*. Kegan Paul, Trench, Trubner & Co.

Mussiraliyeva, Sh., Bolatbek, M., & Baispay, G. (2024). Investigating long short-term memory approach for extremist messages detection in Kazakh language. *Expert Systems with Applications*, 1-19. <https://doi.org/10.1111/exsy.13595>

Neumann, P.R. (2016). *Radicalized: New jihadists and the threat to the West*. Blackstone Publishing.

OON priznala anonimnost v internete pravom cheloveka [The UN has recognized anonymity on the Internet as a human right] (2015, August 25). *Gazeta.ru*. Retrieved May 18, 2026, from [https://m.gazeta.ru/tech/news/2015/08/25/n\\_7509455.shtml](https://m.gazeta.ru/tech/news/2015/08/25/n_7509455.shtml)

Okinawa Charter on Global Information Society. (2000, July 21). *Kremlin.ru*. Retrieved June 25, 2026, from <http://www.kremlin.ru/supplement/3170>

Rapoport, D.C. (2004). The four waves of modern terrorism. In A. K. Cronin & J. M. Ludes (Eds.), *Attacking terrorism: Elements of a grand strategy*, Georgetown University Press, 46-73.

Reshetnyak, A.V. (2016). *Terrorizm i religiozniy ekstremizm v Tsentralnoi Azii: Problemy vospriyatiya. Keis Kazakhstana i Kyrgyzstana* [Terrorism and religious extremism in Central Asia: Problems of perception. The case of Kazakhstan and Kyrgyzstan]. Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan.

Saparova, E.S., & Omirzhanov, E.T. (2016). Religious extremism and terrorism in internet-space: the current challenges and Kazakhstan experience of counteraction. *International Relations and International Law Journal*, 73(1), 145-147. <https://bulletin-ir-law.kaznu.kz/index.php/1-mo/article/view/427>

Sboi v rabote Telegram v Kazakhstane obyasnili zapretom na dvizhenie DVK [Disruptions in the work of Telegram in Kazakhstan were explained by the ban on the movement of DCK.] (2018, March 20). *Sputnik Kazakhstan*. Retrieved May 27, 2026, from <https://ru.sputniknews.kz/society/20180320/4992341/telegram-sboy-prichina-dvk-zapret.html>

Sharipova, D., & Beissembayev, S. (2021). Causes of violent extremism in Central Asia: The case of Kazakhstan. *Studies in Conflict & Terrorism*, 46(9), 1-23. <https://doi.org/10.1080/1057610X.2021.1872163>

Tatarinova, L. (2019). Problemy opredeleniya pravovoi prirody informatsionnogo terrorizma [Problems of defining the legal nature of information terrorism]. *International Relations and International Law Journal*, 84(4), 70-75. <https://bulletin-ir-law.kaznu.kz/index.php/1-mo/article/view/961>

Telegram nashel u sebya v dva raza bolshe IGIL, chem polgoda nazad [Telegram has found twice as many ISIS members as it did six months ago] (2017, April 4). *Roem.ru*. Retrieved May 27, 2026, from <https://roem.ru/04-04-2017/246777/telegram-vs-isis/>

Teroristy rasprobovali Telegram dlya propagandy [Terrorists tried Telegram for propaganda] (2018, December 2). *Lenta.ru*. Retrieved May 27, 2026, from [https://lenta.ru/news/2018/12/02/isis\\_propaganda/](https://lenta.ru/news/2018/12/02/isis_propaganda/)

Teroristy ushli iz Telegram v TamTam [The terrorists left Telegram for TamTam] (2019, December 3). *iGuides*. Retrieved May 27, 2026, from [https://www.iguides.ru/main/security/teroristy\\_ushli\\_iz\\_telegram\\_v\\_tamtam/](https://www.iguides.ru/main/security/teroristy_ushli_iz_telegram_v_tamtam/)

Thompson, R.L. (2012). Friction: How radicalization happens to them and us. *Journal of Strategic Security*, 4(4), 195-196. <https://doi.org/10.5038/1944-0472.4.4.10>

Upornikov, R.V. (2007). *Politiko-pravovye tekhnologii protivodeistviya informatsionnomu ekstremizmu v Rossii* [Political and legal technologies for countering information extremism in Russia] [Abstract of doctoral dissertation in law]. Rostov-on-Don.

V mire naschitali bolee 6 mlrd polzovatelei interneta – otchet Digital 2026 [There are more than 6 billion Internet users in the world – Digital 2026 report] (2025, January 26). *MIGnews.ua*. Retrieved May 12, 2026, from <https://mignews.ua/news/technology/v-mire-uzhe-bolee-6-mlrd-polzovatelej-interneta-lidiruyut-kitaj-i-indiya.html> Vechkinzova, E.A., Petrenko, E.S., Raimbekova, G.A., & Gelashvili, N.N. (2019). Issledovanie razvitiya informatsionnoi sredy Respubliki Kazakhstan [Study of the development of the information environment of the Republic of Kazakhstan]. *Voprosy innovatsionnoi ekonomiki*, 9(4), 1263-1278.

Virilio, P. (2002). *Informatsionnaya bomba: Strategiya obmana* [The information bomb: Strategy of deception]. Gnozis.

VPN-servis zablokiroval sud v Kazakhstane [VPN service blocked by court in Kazakhstan] (2018, March 7). *Zakon.kz*. Retrieved May 28, 2026, from <https://www.zakon.kz/redaktsiia-zakonkz/4907805-ypn-servis-zablokiroval-sud-v-kazahstane.html>

Vkontakte sostavila podrobnuyu instruktsiyu po obkhodu blokirovok [VKontakte has compiled detailed instructions on how to bypass the locks] (2017, May 17). *ZONA.media*. Retrieved May 27, 2026, from <https://zona.media/news/2017/05/17/vk>

Zaurbekov, D.A. (2021). Tekhnologii manipulyatsii obshchestvennym soznaniem v internet-prostranstve [Technologies of manipulating public consciousness in cyberspace]. In *Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Tsifrovaya zhurnalistika i informatsionnaya bezopasnost: Mirovoi opyt i natsionalnye strategii»* [Proceedings of the International Scientific-Practical Conference “Digital Journalism and Information Security: World Experience and National Strategies”], 9-15. International Information Technologies University.

Zhusupova, G.B. (2009). Otdelnye kharakteristiki ekstremistskikh proyavlenii v molodezhnoi srede [Selected characteristics of extremist manifestations among youth]. In *Preduprezhdenie i borba s korruptsiei v svete ukrepleniya zakonnosti v ugolovno-ispolnitelnoi sisteme* [Prevention and combating corruption in the context of strengthening legality in the penal system]: *Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Proceedings of the International Scientific-Practical Conference], 248-251. Kostanai.

Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). *Technical and legal overview of the Tor anonymity network*. NATO Cooperative Cyber Defence Centre of Excellence.