Научная статья / Research article

# Противодействие Российской Федерации и Республики Казахстан информационному терроризму

**Ю. Н. Лагуткина**

*Российский университет дружбы народов, Москва, Россия*
*E-mail:lagnas@bk.ru*

**Ж. И. Мадалимбеков**

*Российский университет дружбы народов, Москва, Россия*
*E-mail:jaaandos@inbox.ru*

**Д. К. Омарова**

*Российский университет дружбы народов, Москва, Россия*
*E-mail:omarova.1999@mail.ru*

**Аннотация**. В статье рассматривается вопрос противодействия стран РФ и РК с информационным терроризмом, представлены проблемы реализации информационной безопасности и перспективы ее развития в целом, а также в период пандемии. Глубокое научное понимание сущности информационного терроризма, выявление его причин и порождающих его условий, а также научный анализ трансформации его видов и форм с учетом его адаптации к меняющейся геополитической ситуации в мире должны оказать решающую помощь в борьбе с этим вызовом. Активное применение мировой паутины террористическими и экстремистскими группировками в качестве инструмента для достижения своих целей приходится на XXI век. Сегодня главная задача состоит в том, чтобы лишить терроризм его социально-политической почвы. В данной работе были проанализированы социокультурные и религиозные факторы в контексте исторического развития, а также, проведен системный анализ, позволяющий выявить возможные пути решения в борьбе с информационным терроризмом, кибератаками и киберугрозами. Также проведен сравнительный анализ состояния структур кибербезопасности России и Казахстана и способов урегулирования этих проблем. Данная работа включает в себя исследование нормативно-правовых актов двух государств, насколько их законодательства отвечают современным реалиям и какие инструменты включены в них, с целью противодействия и борьбы информационному терроризму. Большое внимание оба государства уделяют безопасности в интернет-пространстве на локальном, региональном и глобальном уровнях. Россия и Казахстан принимают активное участие в многостороннем диалоге по противодействию терроризму и экстремизму, поддерживают глобальные инициативы и коллективные усилия по этому вопросу. В ходе проделанной работы, была выявлена необходимость расширить знания о возможных киберугрозах и способах борьбы с ними, а также поиск «точек соприкосновения» двух стран в обеспечении защищенной информационной среды. Терроризм представляет собой серьёзную угрозу всему мировому сообществу, а использование информационных ресурсов и цифровых технологий позволяет террористам пропагандировать деструктивную деятельность и завладевать умами, как представителей молодого поколения, так и старшего. В связи с этим противодействие информационному терроризму в государствах-членах СНГ, Российской Федерации и Республики Казахстан, в последние десятилетия выходит на передовую, способствует формированию правовой базы и построению тесного сотрудничества в противодействии вышеупомянутой угрозы.

**Ключевые слова:** информационный терроризм, кибертерроризм, информационная война, кибератаки, киберугрозы, кибербезопасность, информационная безопасность, информационное оружие.

**Для цитирования:** Лагуткина Ю. Н., Мадалимбеков Ж. И., Омарова Д. К. Противодействие стран Российской Федерации и Республики Казахстан информационному терроризму // Постсоветские исследования. 2022;8(5):847-860.

# Counteraction of the Russian Federation and the Republic of Kazakhstan to information terrorism

**Yuliya N. Lagutkina, Zhandos I. Madalimbekov, Dinara K. Omarova**

*Peoples' Friendship University of Russia, Moscow, Russia*
*lagnas@bk.ru, jaaandos@inbox.ru, omarova.1999@mail.ru*

**Abstract**. The article deals with the issue of counteraction of the countries of the Russian Federation and the Republic of Kazakhstan with information terrorism, presents the problems of implementing information security and the prospects for its development in general, as well as during the pandemic. A deep scientific understanding of the essence of information terrorism, identification of its causes and conditions that give rise to it, as well as a scientific analysis of the transformation of its types and forms, taking into account its adaptation to the changing geopolitical situation in the world, should provide decisive assistance in combating this challenge. The active use of the World Wide Web by terrorist and extremist groups as a tool to achieve their goals falls on the 21st century. Today, the main task is to deprive terrorism of its socio-political soil. In this paper, sociocultural and religious factors were analyzed in the context of historical development, and a system analysis was carried out to identify possible solutions in the fight against information terrorism, cyber-attacks and cyber threats. A comparative analysis of the state of the cybersecurity structures of Russia and Kazakhstan and ways to resolve these problems was also carried out. This work includes a study of the legal acts of the two states, how much their legislation meets modern realities and what tools are included in them, in order to counteract and combat information terrorism. Both states pay great attention to security in the Internet space at the local, regional and global levels. Russia and Kazakhstan take an active part in the multilateral dialogue on countering terrorism and extremism, and support global initiatives and collective efforts on this issue. In the course of the work done, the need was identified to expand knowledge about possible cyber threats and ways to deal with them, as well as the search for "common ground" between the two countries in providing a secure information environment. Terrorism is a serious threat to the entire world community, and the use of information resources and digital technologies allows terrorists to promote destructive activities and take over the minds of both the younger generation and the older one. In this regard, the counteraction to information terrorism in the CIS member states, the Russian Federation and the Republic of Kazakhstan, has come to the fore in recent decades, contributes to the formation of a legal framework and building close cooperation in countering the aforementioned threat.

**Keywords:** information terrorism, cyberterrorism, information war, cyber-attacks, cyber threats, cyber security, information security, information weapons.

**For citation:** Yuliya N. Lagutkina, Zhandos I. Madalimbekov, Dinara K. Omarova. Counteraction of the countries of the Russian Federation and the Republic of Kazakhstan to information terrorism // Post-Soviet studies. 2022;4(5): Postsovetskie issledovaniya = Post-Soviet Studies. 2022;8(5):847-860 (In Russ.).

В наши дни приходится признать, что терроризм уже стал неизбежным фактором международных отношений, являясь одним из самых разрушительных вызовов человечеству. Тактика насилия, как следует из ее характеристики, крайне неизбирательна при выявлении целей, что неизбежно приводит к гибели тех, кто не является непосредственным объектом террористической атаки. И все же их гибель не случайна – в данном случае невинные жертвы среди мирного населения невольно выступают инструментом политического давления на правящую элиту страны,

являющаяся основным объектом теракта. Иными словами, не имея возможности устранить членов правящей элиты какого-либо государства, террористы выбирают в качестве мишеней наименее защищенную категорию населения, используя теракты и гибель простых людей в качестве актов устрашения руководства страны. Часто информационный терроризм выступает как международное преступление, подрывающее существующую систему политических связей разных стран и посягающее на общечеловеческую мораль. При этом в большинстве случаев страдают люди, не имеющие никакого отношения к процессам формирования глобального правопорядка. Информационный терроризм характеризуется большим географическим охватом, отсутствием явно очерченных границ, наличием связи и взаимодействия с международными террористическими центрами и организациями, гибкой и разветвленной организационной структурой. Широко используются технологические достижения в области IT-технологий: информационно-пропагандистская работа ведется террористами с предельной эффективностью. Такая работа включает в себя подбор и подготовку сторонников, активных функционеров и бойцов с целью их практического использования в кризисных зонах. При этом ценность таких рекрутов остается для террористов на самом низком уровне – после их использования их место всегда можно будет заменить вновь прибывающими рекрутами.

Информационная война может вестись как в больших масштабах, так и в рамках полноценных военных действий, таких как сетевая или кибервойна, или как одиночный способ ведения боевых действий. Насильственное навязывание посторонних целей и интересов наглядно показывает, что информационная война – это настоящая война с применением технологий. В этой информационной войне, начиная со СМИ, почты и любого другого вида распространения информации, вступают в действие военные инструменты. Потому что правдивая и прямая информация выгодна только дистрибьютору. Сегодня информационное воздействие происходит постоянно. Оперативное обслуживание и распространение информационной системы в несколько раз увеличило мощность информационного оружия. Дополнительным эффектом стала открытость общества, так как в открытом обществе поток информации намного больше, чем в закрытом. Цель информационной войны - воздействовать на врагов так, чтобы они не знали об этом воздействии.

К концу XX в. процесс бурного развития и внедрения новых информационных технологий, получивший название «информационной революции», стал закономерным этапом экономического и научно-технического прогресса, необходимым условием дальнейшего развития общества. Естественно, с такой же интенсивностью участились случаи использования информационных средств в деструктивных целях: против отдельных лиц, групп и, наконец, против силовых структур, экономики и вооруженных сил. В результате изменились понятия конфликта, войны и оружия, а также границы между войной и миром, военные и гражданские технологии слились воедино. Нападающая сторона получила реальную возможность разорить противника, не проникая на его территорию, победить без собственных потерь. Новые вредоносные и опасные информационные операции требуют постоянного контроля и глубокого всестороннего анализа в целях обеспечения как национальной безопасности стран России и Казахстана, так и международной безопасности. Разработка, производство, распространение и использование информационных технологий в военных целях не регулируется международным правом. На современном этапе такое положение не позволяет говорить о возможности применения хорошо разработанных теорий на практике. В России и Казахстане теоретическая база в этой области формируется на основе прецедента: от практики к теории. Таким образом, необходим постоянный мониторинг и детальное разностороннее изучение случаев нарушения информационной безопасности с целью

создания базовой теории, применения ее на практике и дальнейшего совершенствования.

Существуют множество исторических примеров, когда нововведения в технике приводили к коренным изменениям в характере информационной составляющей войны. Проблема кибератак является одним из наиболее значимых, но недостаточно изученных и описанных примеров использования вредоносных методов в сфере информационных технологий. Киберманипуляции можно рассматривать не просто как киберпреступление, а как кибервойна с применением кибероружия. Эти прецеденты стали достоянием общественности и привели к важным последствиям, повлиявшим на дальнейший ход событий. В годы войн кибертехнологии дополнялись и не уступали по своему воздействию не только политическим и экономическим санкциям, но и военным мерам.

Изучение информационного терроризма поможет России и Казахстану не только расширить знания о возможных киберугрозах и способах борьбы с ними, но и найти «точки соприкосновения» в подходах обеих стран к обеспечению защищенной информационной среды с целью более эффективной защиты интересов двух стран на международном уровне. Превращение информационной безопасности в одну из заданных тем стратегического диалога Москвы и Нур-Султана поможет адаптировать «стратегическое партнерство» к реалиям современного мира. Задача изучения проблем обеспечения информационной безопасности личности и общества обозначена в качестве одного из приоритетных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации и Республики Казахстан. Это обосновывается тем, что в настоящее время информационные операции, осуществляемые насильственными средствами воздействия на соответствующее поле противника для достижения стратегических целей нападающего, являются наиболее общественно опасным видом противоборства. Политическое и психологическое влияние одних государств на другие зародилось на раннем этапе истории человечества в виде отдельных дезинформационных операций противника. Такое воздействие претерпело значительные изменения в процессе развития и стало постоянным фактором внешнеполитической, диверсионной информационно-психологической деятельности, осуществляемой не только в боевой, но и в мирной фазе кризисов и конфликтов. В конце XX – начале XXI вв., этот новый вид ведения войны стал доминирующей политикой во многих государствах.

Наиболее важное теоретико-методологическое значение для данного исследования имеет системный анализ, который позволяет выявить возможные пути решения государств в борьбе с информационным терроризмом, кибератаками и киберугрозами. Данный анализ позволит более тщательно рассмотреть сотрудничество обеих стран в сфере информационной безопасности.

Метод сравнительного анализа позволил сопоставить оценки и позиции антитеррористических центров в сфере киберпространства, тем самым, выявить эффективность работы против киберугроз.

На сегодняшний день среди глобальных проблем терроризм особенно отличается. Его отличие заключается в том, что в XXI в. он перешел и захватил новую сферу, тем самым появился новый вид терроризма – информационный терроризм или же кибертерроризм.

В XXI в. терроризм не стал ограничиваться на территории одного государства, вместо этого, террористическая деятельность начала переходить на территории других государств, регионов и континентов, при этом следует, отметить, что террористические группировки имеют между собой тесную взаимосвязь. Соединяющим звеном террористических групп выступает всеми известные ИКТ, интернет, социальные сети и т.д. Российская

Федерация является одним из активных субъектов международных отношений, который противодействует всем формам экстремизма и терроризма. Сегодня, как и в остальных государствах, так и на территории России террористические организации совершают свои злодеяния с помощью ИКТ.

Отмечается, что Россия относится к списку государств, которые больше всего испытывают на себя кибератаки. По данным экспертов, заманчивыми областями для кибертеррористов являются ядерная, финансовая, энергетическая, военная области и логистика [Малик 2020: 170–171]

Активное применение мировой паутины террористическими и экстремистскими группировками в качестве инструмента для достижения своих целей в РФ приходится на начало XXI в.

Для борьбы с кибертерроризмом на государственном уровне Россия имеет множество нормативно-правовых актов. К основным нормативно-правовым актам можно отнести:

— «Концепция противодействия терроризму в Российской Федерации» от 2009 г.;

— Федеральный закон «О противодействии терроризму» от 2006 г.;

— Закон «Об информации, информационных технологиях и о защите информации» от 2006 г.;

— «Доктрина информационной безопасности Российской Федерации» от 2016 г.;

— Указ Президента России 2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»;

— «Концептуальные взгляды на деятельность Вооруженных сил РФ в информационном пространстве» от 2011 г.;

— Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 2017 г. и т.п.

Среди всех нормативно-правовых актов особенно отличается так называемый «Закон Яровой»[1] [2], который был принят 13 мая 2016 года. Особенность данного документа заключается в том, что он является первым законом, дающий возможность вмешиваться в Интернет, иными словами, борется с информационным терроризмом в мировой паутине [Барсегян, Кернер 2020: 317–318].

Однако несмотря на существование нормативных актов ежегодно увеличивается количество преступлений, которые относятся к информационному терроризму. К примеру, всего за период 2005–2006 гг. в России было совершено более 2 млн кибератак на официальные сайты и информационные данные государственных органов [Еделев 2005]. Стоит отметить, что в период январь-июнь 2006 г. было совершено 752 террористических актов [Прокопьева 2017: 32-33]. Согласно данным Генеральной Прокуратуры Российской Федерации, в 2009 г. было совершено 654 террористических атак [Аношкина 2020]. В 2012 г. российскими спецслужбами было ликвидировано более 500 сайтов на просторах интернета, которые имели отношения к экстремизму и терроризму. Также в том году был пойман участник радикальной исламской партии «Хизб-ут-Тахрир аль-Исламий», который занимался распространением экстремизма в мировой паутине. [Усилинский 2014: 7–8]. В 2016 году в РФ кибертерроризм так расширился, что две трети преступных деяний имели экстремистский характер, а также каждое девятое правонарушение являлось террористическим актам, который был

[1] Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». URL: http://www.kremlin.ru/acts/bank/41113 (дата обращения: 14.06.2022)

[2] Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». URL: http://www.kremlin.ru/acts/bank/41108 (дата обращения: 14.06.2022)

реализован посредством интернета. Данные Генеральной Прокуратуры РФ показали, что за 2018 г. количество подобных атак составляло 1679, за 2019 г. – 1806, из которых 844 расследовано [1].

Исходя из данных, в России терроризм в период 2003–2006 гг. находился на высшей точке. После данного периода произошло снижение до 2014 г. Но начиная с 2014 г. терроризм восстановился с новыми формами и держаться на одном темпе до сегодняшнего дня [Дементьева, Моргоева, Нестеров 2022: 229–230].

Некоторые эксперты отмечают, что со временем происходит уменьшение доли правонарушений, связанных с кибертерроризмом, по сравнению к террористическим актам в целом. Несмотря на то, что доля кибертеррористических преступлений в 2018 г. составляла 48%, в 2019 г. 44% и в 2020 г. 32%, с каждым годом увеличивается количество террористических преступлений, связанных с использованием ИКТ [2].

Во время пандемии угроза информационного терроризма еще больше увеличилась. Пандемия кардинально изменила жизни людей. До пандемии были люди, которые не пользовались мировой паутиной, сегодня пандемия заставила людей пользоваться интернетом, ИКТ, социальными сетями, люди начали больше времени тратить в просторах интернета. Таким образом, у террористов появилась возможность незаметно пропагандировать свою деятельность и получить доступ к персональным данным или иным важным ресурсам. По состоянию на октябрь 2020 г. МВД России заявило, что в 2020 г. продолжает расти преступности в мировой паутине и оказывает отрицательное воздействие на уровень преступности в стране. В Министерстве отметили, что в 2020 г. показатель киберпреступлений вырос на 75,1% по сравнению с 2019 г [3]. По данным МВД за первые четыре месяца 2021 г. количество кибератак увеличилось на 31,5%[4]. Почти две трети из них совершаются с использованием сети Интернет, свыше трети – с помощью средств мобильной связи. Несмотря на это в декабре 2021 г. информационный центр Национального антитеррористического комитета (НАК) сообщили, что в 2021 г. государственные спецслужбы и правоохранительные органы не допустили совершения ни одного теракта в стране[5]. Казалось, что после пандемии темп информационных преступлений сохранится, но данные за первые четыре месяца 2022 г. показали уменьшение число преступлений, с применением ИКТ, было зарегистрировано на 11,4% меньше[6].

Необходимо отметить, что информационный терроризм является угрозой для всего мирового сообщества, учитывая этот факт Российская Федерация в сотрудничестве с другими государствами и международными организациями предпринимает всевозможные усилия для борьбы с этой угрозой. В прошлом году на

[1] Генеральная Прокуратура Российской Федерации. Главное управление правовой статистики информационных технологий. Состояние преступности в России // Сборник подготовлен на основании формы федерального статистического наблюдения № 4-ЕГС. — За январь-декабрь 2016–2019 гг.

[2] Статистика генеральной прокуратуры РФ. Приведенная статистика охватывает более широкий спектр статей Уголовного кодекса РФ: ст. 205 ч.1, 205 ч.2, 205 ч.3, 205.1 ч.1, 205.1 ч.2, 205.1 ч.3, 205.1 ч.4, 205.2 ч.1, 205.2 ч.2, 205.3, 205.4 ч.1, 205.4 ч.2, 205.5 ч.1, 205.5 ч.2, 205.6, 206 ч.1, 206 ч.2, 206 ч.3, 206 ч.4, 207 ч.1, 207 ч.2, 207 ч.3, 207.4, 208 ч.1, 208 ч.2, 361 ч.1, 362.1 ч.2, 361 ч.3. URL: http://crimestat.ru/ (дата обращения: 12.05.2022)

[3] Краткая характеристика состояния преступности в Российской Федерации за январь — октябрь 2020 г. URL: https://xn--b1aew.xn--p1ai/reports/item/21933965/ (дата обращения: 5.06.2022)

[4] Министерство внутренних дел Российской Федерации. Краткая характеристика состояния преступности в Российской Федерации за январь-апрель 2021 года. URL: https://мвд.рф/reports/item/24644450/ (дата обращения: 13.06.2022)

[5] В НАК сообщили, что в России в 2021 году не допущено совершения ни одного теракта // «ТАСС»// URL: https://tass.ru/obschestvo/13193919 (дата обращения: 13.06.2022)

[6] Министерство внутренних дел Российской Федерации. МВД России публикует данные о состоянии преступности по итогам четырех месяцев 2022 года. URL: https://мвд.рф/news/item/30236038/ (дата обращения: 13.06.2022)

саммите ШОС Россия поддержала предложение глав государств Республики Кыргызстана и Республики Узбекистана о запуске совещания руководителей профильных министерств и возобновлении встречи министров внутренних дел и общественной безопасности для противодействия кибертерроризму и отметила, что в последние годы увеличивается риски информационного терроризма [Черняева, Журавлёва 2022: 540–541].

Термин информационный терроризм или кибертерроризм в нормативно-правовых актах РФ не существует. Невозможно сказать, что информационный терроризм совсем отсутствует в правовых нормах России. К примеру, кибертерроризм используется в пунктах, касающиеся подготовки профессионалов для борьбы против терроризма[1]. С одной стороны кажется, что отсутствие таких терминов в нормативно-правовых актах РФ не препятствует противодействию кибертерроризму, так как эксперты отмечают, что проблема заключается в правоохранительных органах, ибо они допускают ошибок и не доводят дело до конца, с другой стороны, законодательное закрепление термина дало бы новые возможности для противодействия информационному терроризму.

Для противодействия кибертерроризму в 2013 г. был издан Указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», этот Указ расширил полномочия Федеральной службы безопасности Российской Федерации по формированию на государственном уровне структуры выявления, уничтожения и предотвращения последствий информационных нападений на российские информационные источники, ИКТ, которые расположены в Российской Федерации и заграничных учреждениях Российской Федерации[2]. А также РФ в двусторонних отношениях и в рамках международных организаций выступает против информационному терроризму. Очевидным примером послужит заключения «Соглашения между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» в 2009 году, в котором одной из основных целей договора стало обеспечение информационной безопасности участников ШОС и создание информационной атмосферы для благополучного сотрудничество во всех сферах. Также в данном соглашении отмечалось, что информационный терроризм является опасностью для международной безопасности [Питинова 2018: 32–33]. В рамках ШОС страны организации рассматривают вопросы, связанные с безопасностью и борьбой с терроризмом [Рахимов 2019]. Опираясь на формат ШОС, государствам-участникам значительно легче бороться с исламским экстремизмом, сепаратизмом и терроризмом [Рахимов 2020]. В рамках СНГ в 2000 г. для противодействия террористических и экстремистских актов был создан Антитеррористический центр. Сегодня данный центр находится в активном сотрудничестве органами государств-членов Содружества согласовывает и содействует в противодействии терроризму[3].

Сегодня в России отсутствует основополагающий нормативно-правовой акт, который включает в себя все пути противодействия кибертерроризму. Вместо

[1] Концепция противодействия терроризму в Российской Федерации от 05.10.2009. URL: https://docs.cntd.ru/document/902180267 (дата обращения: 15.05.2022)

[2] Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Российская газета. 2013. URL: https://docs.cntd.ru/document/902392496 (дата обращения: 20.05.2022)

[3] Решение совета глав государств СНГ от 21 июня 2000 года «О создании Антитеррористического центра государств - участников Содружества Независимых Государств» // Официальный сайт АТЦ СНГ. URL: https://www.cisatc.org/132/166/188 (дата обращения: 27.05.2022)

этого существует ряд законодательных документов (Стратегии национальной безопасности Российской Федерации, Доктрина информационной безопасности, проект Концепции стратегии кибербезопасности и т. д.), а также документы, которые сдерживают и препятствуют законам и поправкам.

Некоторые ученые предполагают, что приведение в единую форму Российских и зарубежных законодательных актов может привести к тесному взаимодействию спецслужб и положительному противодействию терроризму, а также дает возможность увеличит процент защищенности в просторах интернета и в самих государствах [Декола, Магомедова, Петрашко 2020: 329–330].

Стоит отметит, что таких средств недостаточно для достижения положительных результатов в информационным пространстве. Информационный терроризм, как отмечалось выше, в современным мире является острым вопросом и угрозой национальной безопасности для всех государств, не только для РФ. С каждым годом вопрос о проявлениях кибертерроризма увеличивается и становится важной проблемой.

Республика Казахстан с момента приобретения независимости (1991 г.) ставит во главу угла безопасность. В более широком смысле здесь подразумевается не только территориальная безопасность, но и безопасность во всех сферах жизнедеятельности казахстанских граждан. Большое внимание правительство уделяет безопасности в интернет-пространстве на локальном, региональном и глобальном уровнях. Казахстан активно участвует в глобальном диалоге по противодействию терроризму и экстремизму. Немалое внимание в стране уделяется противодействую терроризма в интернет-пространстве. Республика Казахстан также является непосредственным участником контртеррористической деятельности в рамках организаций ОДКБ, ШОС, СВМДА, Антитеррористического центра СНГ, в сотрудничестве с ОБСЕ активно проводит мероприятия обучающего характера, заседания, конференции и тренинги регионального и международного уровня, направленные на противодействие экстремизму и терроризму[1].

В настоящее время достигнута степень полного взаимодоверия стран-участников ШОС по вопросам политики и военной сферы, дальнейшие усилия будут направлены на совместную борьбу с третьими силами, а именно: укрепление международного сотрудничества в сфере информационной безопасности и борьбу с интернет-терроризмом, пресечение финансирования терроризма с целью прекращения распространения оружия. Таким образом, основными вопросами сотрудничества государств-участников ШОС являются укрепление международного сотрудничества в области безопасности и борьба с третьими силами [Рахимов 2019].

Казахстан, решительно осуждая насилие во всех формах его проявления, в том числе террористические действия, а также действия направленные на угрозу безопасности и попытку дестабилизации ситуации в стране, поддерживает глобальные инициативы и коллективные усилия всего мирового сообщества по борьбе с вышеперечисленными явлениями. Республика Казахстан неукоснительно выполняет требования глобальной антитеррористической стратегии СБ ООН (2006 г.) и ежегодно в Национальном докладе отчитывается в Контртеррористический Комитет ООН о проделанной работе в рамках борьбы с терроризмом[2]. Для усиления работы по противодействию терроризму, Казахстан присоединился к четырнадцати международным универсальным инструментам по борьбе с терроризмом. Что касается кибертерроризма и

[1] Официальный сайт МИД РК: https://www.gov.kz/memleket/entities/mfa/press/article/details/589?lang=ru (дата обращения: 05.06.2022)

[2] Глобальная контртеррористическая стратегия ООН: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/90/PDF/N0550490.pdf?OpenElement (дата обращения: 06.06.2022)

киберпреступности, резолюция 53/70, принятая в декабре 1998 г. Генеральной Ассамблеей ООН и касающаяся киберпреступности, кибертерроризма и кибервойны призывает государства-члены информировать Генерального секретаря ООН касательно мер принимаемых для информационной безопасности стран участниц данной организации[1]. Соглашаясь с правилами принятой резолюции, Республика Казахстан отчитывается о проделанной работе и принятых мерах для обеспечения и поддержания информационной безопасности.

В последние несколько десятилетий с развитием цифровых технологий, терроризм приобрел новые формы, одной из которых является развитие и распространение терроризма в интернет-пространстве. Так называемый кибертерроризм в последнее время немало опасен, чем традиционный. На сегодняшний день очень много различных определений понятию кибертерроризм. По одному из определений под кибертерроризмом понимается «общее наименование компьютерных правонарушений (взломы файлов, похищение секретов и денег со счетов банков), а также компьютерное хулиганство (введение вирусов и т.п.)»[2]. На самом деле, кибертерроризм очень опасен тем, что имеет большое количество сфер влияния посредством интернет-сообществ, пабликов, сайтов и порталов, носящих замаскированный деструктивный характер и разрушающее влияние. Открытого призыва к террористическим действиям сейчас почти нет, зато кибертеррористы настолько профессионально действуют в мировой паутине, что так называемые «жертвы», подвергшиеся действию и влиянию террористов, как правило, зачастую молодое поколение, не осознают, на какие действия они идут и к чему их принудят. Еще одним фактором, способствующим развитию кибертерроризма, помимо цифровых технологий относятся всеобъемлющие процессы глобализации, неизбежного процесса, в который вовлечены все страны и континенты.

Ни для кого не секрет, что с каждым годом глобализация всё сильнее влияет на все стороны жизни гражданина любой страны и её влияние проявляется не только в обмене культурными и материальными ценностями. Военные конфликты и нерешенные территориальные вопросы, смертоносные пандемии, природные катаклизмы и международная преступность сегодня имеет широкий информационный охват [Турсынбекова 2014]. В период любого из вышеперечисленных вызовов современности терроризм видоизменяясь в любую из форм (религиозный, экономический, геополитический, этнорелизиозный и т.д.) легко проявляется и как «невидимый зверь» руководствуясь подорванной ситуацией в стране, регионе или мире начинает масштабное влияние в виде информационных атак, создания деструктивных сайтов и рассылок, вербовки в социальных сетях и сообществах. Для подобного рода обширности своего влияния террористические группировки, получая от определенных лиц и организаций необходимое финансирование, обучение логике, математике, психологии, психосоматике, логистике, криптографии, освоение ИКТ, программного обеспечения, математико-экономических методов, развивают свою организационную основу, подвергают разрушительному влиянию большие массы.

Правительство Республики Казахстан, осознавая всю опасность, губительное влияние и ужасающие последствия от широкомасштабного кибертерроризма, взяв за основу принцип обеспечения безопасности, поручило создать программу «Киберщит Казахстана», в которую были заложены: анализ текущей ситуации, мировой опыт, цели, задачи, результаты и период реализации, а также основные принципы и подходы противодействия

[1] АДР РК. О некоторых методах противодействия кибертерроризму в интернет-пространстве. 10.10.2015. https://yvision.kz/post/577387 (Дата обращения: 06.06.2022)

[2] Толковый словарь Ефремовой Т.Ф. https://dic.academic.ru/dic.nsf/efremova/275669/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%82%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC (дата обращения: 06.06.2022)

информационному терроризму[1]. Во втором полугодии текущего года с учетом проделанной работы и новых реалий будет принята новая редакция концепции «Киберщит Казахстана-2», реализация которой предусмотрена до 2027 г. В новой концепции будут отражены основные направления, охватывающие усиление административной ответственность за утечку личных данных, использование отечественных и регулирование иностранных медиа-платформ на территории страны. В обновленном документе будут отражены вызовы и угрозы кибербезопасности с учетом мирового опыта борьбы с кибертерроризмом. Стоит отметить, что осведомленность населения по вопросам кибербезопасности в 2021 г. составила 75%. Для противодействия информационному терроризму, был принят ряд мер, направленных на повышение информационной грамотности у населения, а также на 2021–2022 гг. увеличено количество образовательных грантов до 2632 по профессии «информационная безопасность»[2].

Помимо концепции кибербезопасности, в рамках противодействия кибетерроризму, в 2014 г. был принят уголовный кодекс, особенностью которого стало включение целого ряда составов уголовных правонарушений в сфере информатизации и связи[3]. В общем, Республике Казахстан принято порядка 30 других проектов и законодательных актов, нацеленных на борьбу и противодействие информационному терроризму. Особое внимание уделяется работе с местными и иностранными СМИ, ведется контроль официальных законодательных сайтов, проводится мониторинг работы спецслужб страны. Особое внимание в киберпространстве на территории Казахстана уделяется учебным платформам, образовательным сайтам и обучающим порталам. Спецслужбы, ответственные за поддержание кибербезопасности тщательно следят за тем, чтобы данные учащихся находились под защитой, а сами учащиеся не были подвержены кибератакам, а также сомнительным «урокам о религии», за которыми могут скрываться террористы, орудующие в онлайн-пространстве.

В период пандемии коронавируса и перехода на дистанционный формат работы и обучения, резко возросла нагрузка на цифровую инфраструктуру республики [Лебедева, Кузнецов 2021]. К этому казахстанские системы оказались не готовы, в результате возникли проблемы с доступом к некоторым государственным интернет-ресурсам. С начала 2020 г. в Казахстане зафиксировано порядка 200 кибератак[4]. С целью профилактики кибератак и противодействия киберпреступности, в стране ужесточилось отслеживание переписки сомнительных пользователей сети, а также, по данным Комитета Национальной Безопасности, телефонные разговоры граждан могут быть записаны, если в разговоре звучат так называемые слова-маркеры, такие как: бомба, атака, террор и другие.

Из интервью с К. Бекназаровым, сотрудником КНБ РК, а также полковником в отставке, стало известно, что в 2021 году предотвращен экономический ущерб более чем на 300 миллиардов тенге, еще 63 миллиарда было возвращено в государственный бюджет. По другому направлению, контрразведке ведется обширная системная работа с обеспечением информационной безопасности граждан. «Наша контрразведка смогла за последние

[1] Официальный сайт Концепции кибербезопасности «Киберщит Казахстана»: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 08.06.2022)

[2] Курсив. В 2022 году будет принята новая редакция концепции «Киберщит Казахстана». 31.03.2022. URL: https://kz.kursiv.media/2022-03-31/v-2022-godu-budet-prinyata-novaya-redakciya-koncepcii-kibershhit-kazahstana/

[3] Digital report. Обзор законодательства Республики Казахстан: Борьба с киберпреступностью. 29.07.2016. URL: https://digital.report/zakonodatelstvo-kazahstana-borba-s-kiberprestupnostju/ (дата обращения: 08.06.2022)

[4] 200 миллионов кибератак зафиксировали с начала года в РК. 07.12.2020. URL: https://24.kz/ru/news/social/item/440938-200-millionov-kiberatak-zafiksirovali-s-nachala-goda-v-rk (дата обращения: 09.06.2022)

три года выявить и разоблачить 21 агента иностранных спецслужб. Сегодня Комитет национальной безопасности выступает как равноправный партнер в сообществе спецслужб мира», - отмечает К. Бекназаров[1]. Киберпреступность сегодня представляет собой настоящую опасность для всех пользователей сети Интернет. Для того, чтобы уберечь себя от кибертеррористов, IT-эксперты не рекомендуют незнакомым людям сообщать о себе персновальную информацию, которая содержит дату рождения, индивидуальный идентификационный номер, номер удостоверения личности, а также пароли и коды от банковских карт и денежных счетов. В стране ежегодно проводятся мероприятия, повышающие уровень грамотности населения и улучшение мер по борьбе с преступностью в интернете. Отмечая успехи казахстанских киберспециалистов по борьбе с информационным терроризмом и киберпреступностью, 2019 году Казахстан стал членом организационного комитета CAMP (Cybersecurity Alliance for Mutual Progress). Данный комитет находится и действует в Южной Корее. В его состав входят 60 организаций из 46 стран. Члены CAMP имеют возможность обмениваться учебными программами и информацией по вопросам кибербезопасности, которые становятся все более сложными и затрагивают все больше пользователей и организаций по всему миру. В период с 14 по 20 сентября 2020 г. прошла Пятая ежегодная конференция членов Cybersecurity Alliance for Mutual Progress (CAMP, Альянс по кибербезопасности для взаимного прогресса), где странами-участниками обсуждались вопросы информационной безопасности и разбирались наиболее значимые события инцидентов ИБ за 2019–2020 гг. От лица Казахстана выступил директор департамента Государственной технической службы Медет Искаков, который в своем выступлении поделился опытом Казахстана в борьбе с кибератаками в период пандемии. Выступление спикера было признано лучшим в номинации «Best Speaker» из 47 стран-участниц CAMP[2].

На сегодняшний день деятельность по противодействию кибертерроризму требует системного и комплексного подхода взаимодействия всех правоохранительных органов страны [Барсегян, Кернер 2020]. Анализируя международный и государственный опыт по противодействию кибертерроризму, наиболее эффективными мерами в данном вопросе является совершенствование правовой базы и дальнейшая активизация разъяснительной и идеологической работы, особенно в молодежной среде [Минязева Т.Ф. 2018].

Важно понимать, что обеспечение кибербезопасности – это не проект, который можно реализовать и в скором времени отложить в дальний ящик. Это в первую очередь выстраивание новых и изменение существующих процессов в жизненном цикле организации с учетом определенных правил и рекомендаций по обеспечению информационной безопасности [Абазов 2018]. Все сферы, в том числе образование и предпринимательство должны определить достаточный уровень безопасности, и чем в случае атаки должны быть готовыми рискнуть. Исходя из этого решения, формируется объем работ и бюджет на их реализацию.

Подводя к заключению, информационный терроризм, несомненно, является одной из глобальных проблем. А значит, подход к поискам ответа на этот вызов должен отражать это обстоятельство. Это относится к единому пониманию проблемы, тщательному изучению и анализу теоретических вопросов этого вида насилия. Все это может служить основой совершенствования и гармонизации государственных и международно-правовых актов, и особенно комплексных программ борьбы с терроризмом, совместного планирования и осуществления

[1] Ахметова А. Бекназаров К. Тотальная слежка давно осталась в прошлом.14.05.2021. URL: https://online.zakon.kz/Document/?doc_id=30505670&pos=3;-80#pos=3;-80 (дата обращения: 09.06.2022)

[2] Егеубаев Ж. Кибербезопасность в Казахстане – что сегодня актуально? 26.03.2021. URL: https://mobilaser.kz/kiberbezopasnost-v-kazahstane-chto-segodnya-aktualno/technologies/ (дата обращения: 09.06.2022)

предупредительных, оперативно-розыскных, политических, экономических и судебных мероприятий. К сожалению, сегодня такое сотрудничество серьезно осложнено политическими противоречиями между странами, а то и вовсе прекращено в результате односторонних решений, принимаемых некоторыми странами, особенно по политическим мотивам. Глубокое научное понимание сущности терроризма, выявление его причин и порождающих его условий, а также научный анализ трансформации его видов и форм с учетом его адаптации к меняющейся геополитической ситуации в мире должны оказать решающую помощь к этому вызову [Дакка, Дмитриева 2020]. На сегодняшний момент, главная задача, на наш взгляд, состоит в том, чтобы лишить терроризм его социально-политической почвы, на которой он растет, во многом благодаря незнанию его потенциала.

В настоящее время определяющим фактором является обеспечение надежного и безопасного функционирования информационных систем, противодействие различным формам информационного воздействия. Информационная безопасность является неотъемлемой и все более важной частью процесса обеспечения стратегической стабильности. Сегодня понятие информационной безопасности охватывает все сферы жизни общества. Информационную оборону можно рассматривать как комплекс тесно связанных задач в области международной этики, права и организации управления, разработки технических средств, программирования и математики. В Российской Федерации и Республике Казахстан, развитию законодательства в этой сфере предшествует принятие политических и доктринальных документов, формулирующих основные задачи и пути их решения. Государства защищают свои национальные интересы в информационной сфере общим балансом интересов на уровне личности, общества и государств.

## СПИСОК ЛИТЕРАТУРЫ

*Абазов К.М.* Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями. Вопросы безопасности. Общество с ограниченной ответственностью "НБ-Медиа". – 2018. С. 7.

*Аношкина А. А*. Информационный терроризм как угроза национальной безопасности / Молодой ученый. – 2020.— № 20 (310). — С. 245–247.

*Барсегян А.А., Кернер Е.А.* Проблема цифровизации терроризма на пространстве СНГ// Постсоветские исследования. Автономная некоммерческая организация Центр исследований постсоветских стран. – 2020. Т. 3. С. 319.

*Дакка А., Дмитриева М*. Роль Центральной Азии в российско-индийском сотрудничестве в области энергетики. Вестник МГИМО-Университета. – 2020. – №13(6). С.208-227.

*Декола И.В., Магомедова А.Д., Петрашко Б.Э.* Проблема обеспечения кибербезопасности в Белоруссии, России и Украине. Постсоветские исследования. – 2020. Т.3. № 4. С. 323–335.

*Дементьева О. Е., Моргоева Д. Э., Нестеров А. В.* Терроризм в Российской Федерации в 2002–2020 гг. Постсоветские исследования. – 2022.– Т. 5. – № 2. С. 220–231.

*Еделев А. Л.* Борьба с экстремизмом: вопросы теории и практики. М.— 200 с. АУ МВД России, 2005.

*Лебедева М. М., Кузнецов Д. А.* Глобальное управление в вопросах противодействия биогенным угрозам. Вестник МГИМО-Университета – 2021. №14(2). – С.7-21.

*Малик Е. Н.* Кибертерроризм как мировая угроза: вызовы и меры борьбы // Вестник Прикамского социального института. 2020. № 1 (85). С. 169–173.

*Минязева Т.Ф.*, Психологическая диагностика человека при решении вопросов профилактики терроризма. Евразийская адвокатура. – 2018 – Т.1. С. 77–82

*Питинова А. С.* Актуальные вопросы противодействия кибертерроризму / Право: история, теория, практика: материалы VI Междунар. науч. конф. – 2018.— С. 31–34.

*Прокопьева В. А.* Политика противодействия кибертерроризму в современной России / Выпускная квалификационная работа. 2017.

*Рахимов К.Х.* Шанхайская организация сотрудничества в системе обеспечения евразийской региональной, международной и глобальной безопасности (международно-правовое измерение) // Постсоветские исследования. 2020. – Том 3. №2. С.124-135.

*Рахимов К.Х.* Правовое регулирование противодействия терроризму и экстремизму в государствах Шанхайской организации сотрудничества // Евразийский юридический журнал. №2 (129) 2019. С. 67–70.

*Турсынбекова С.* О роли органов прокуратуры в противодействии терроризму в интернет-пространстве. Материалы международной научно-практической конференции «Терроризм и Интернет». –2014.

*Усилинский Ф. А.* Кибертерроризм в России: его свойства и особенности. Право и кибербезопасность. – 2014. – № 1. С. 6–11.

*Черняева С. В., Журавлёва Е. В.* Роль ШОС в контексте «афганской проблемы». Постсоветские исследования. – 2022. Т. 5. № 5. С. 531–544.

## REFERENCES

*Abazov K.M.* The problem of the use of modern information and communication technologies by international terrorist organizations. Security questions. Limited Liability Company "NB-Media". - 2018. P. 7.

*Anoshkina A. A.* Information terrorism as a threat to national security / Young scientist. - 2020. - No. 20 (310). - S. 245-247.

*Barseghyan A.A., Kerner E.A.* The problem of digitalization of terrorism in the CIS space // Post-Soviet Studies. Autonomous non-profit organization Center for Post-Soviet Studies. – 2020. V. 3. S. 319.

*Dhaka A., Dmitrieva M.* The role of Central Asia in Russian-Indian cooperation in the field of energy. Bulletin of MGIMO-University. - 2020. - No. 13(6). pp.208-227.

*Decola I.V., Magomedova A.D., Petrashko B.E.* The problem of ensuring cybersecurity in Belarus, Russia and Ukraine. Post-Soviet Studies. – 2020. V.3. No. 4. S. 323-335.

*Dementieva O. E., Morgoeva D. E., Nesterov A. V.* Terrorism in the Russian Federation in 2002–2020. Post-Soviet Studies. - 2022. - V. 5. - No. 2. S. 220-231.

*Edelev A. L.* Fighting extremism: questions of theory and practice. M. - 200 p. AU MIA of Russia, 2005.

*Lebedeva M. M., Kuznetsov D. A.* Global management in countering biogenic threats. Bulletin of MGIMO-University - 2021. No. 14(2). - P.7-21.

*Malik E. N.* Cyberterrorism as a global threat: challenges and measures to combat // Bulletin of the Kama Social Institute. 2020. No. 1 (85). pp. 169-173.

*Minyazeva T.F.*, Psychological diagnostics of a person in solving issues of prevention of terrorism. Eurasian Advocacy. – 2018 – Vol.1. pp. 77-82

*Pitinova A. S.* Topical issues of counteracting cyberterrorism / Law: history, theory, practice: materials of the VI Intern. scientific conf. - 2018. - S. 31-34.

*Prokopieva V. A.* The policy of counteracting cyberterrorism in modern Russia / Final qualification work. 2017.

*Rakhimov K.Kh*. Shanghai Cooperation Organization in the System of Ensuring Eurasian Regional, International and Global Security (International Legal Dimension) // Post-Soviet Studies. 2020. - Volume 3. No. 2. pp.124-135.

*Rakhimov K.Kh.* Legal regulation of countering terrorism and extremism in the states of the Shanghai Cooperation Organization // Eurasian Law Journal. No. 2 (129) 2019. P. 67-70.

*Tursynbekova S.* On the role of the prosecutor's office in countering terrorism in the Internet space. Materials of the international scientific-practical conference "Terrorism and the Internet". – 2014.

*Usilinsky F. A.* Cyberterrorism in Russia: its properties and features. Law and cybersecurity. - 2014. - No. 1. S. 6-11.

*Chernyaeva S. V., Zhuravleva E. V.* The role of the SCO in the context of the “Afghan problem”. Post-Soviet Studies. – 2022. V. 5. No. 5. S. 531-544.

**ИНФОРМАЦИЯ ОБ АВТОРАХ/INFORMATION ABOUT THE AUTHORS**

**Лагуткина Юлия Николаевна** – Магистр в области «Международных отношений» Российского университета дружбы народов. Москва, Россия. E-mail: lagnas@bk.ru

**Yuliya N. Lagutkina** – Master in International RelationsDepartment of RUDN University. Moscow, Russia. E-mail: lagnas@bk.ru

**Мадалимбеков Жандос Исроилбекович** – Магистр в области «Международных отношений» Российского университета дружбы народов. Москва, Россия. Москва, Россия. E-mail: jaaandos@inbox.ru

**Zhandos I. Madalimbekov** – Master in International RelationsDepartment of RUDN University. Moscow, Russia. E-mail: jaaandos@inbox.ru

**Омарова Динара Куанбековна** – Магистр в области «Международных отношений» Российского университета дружбы народов. Москва, Россия. Москва, Россия. E-mail: omarova.1999@mail.ru

**Dinara K. Omarova** – Master in International RelationsDepartment of RUDN University. Moscow, Russia. E-mail: omarova.1999@mail.ru