Научная статья / Research article

Противодействие кибертерроризму в Беларуси, Казахстане и Азербайджане

Д. С. Тарасов[1], Е. А. Солодухина[2], В. Е. Марченкова[3], В. В. Скориков[4]

[1, 2, 3, 4] *Российский университет дружбы народов им. П. Лумумбы, Москва, Россия*
[1] *E-mail: 1032211937@rudn.ru*
[2] *E-mail: 1132223119@rudn.ru*
[3] *E-mail: 1032220375@rudn.ru*
[4] *E-mail: 1132223091@rudn.ru*

Аннотация. Кибертерроризм становится все более актуальной и серьезной угрозой для национальной безопасности многих стран в мире. Этот вид терроризма может нанести серьезный ущерб государственным институтам, критической инфраструктуре, финансовой системе и частным компаниям. Беларусь, Казахстан и Азербайджан являются важными государствами в Евразии, которые сталкиваются с различными угрозами и вызовами на своих территориях. Одной из таких угроз является кибертерроризм, который может иметь серьезные последствия для экономики, политики и общественной безопасности. В данной статье проведён анализ угроз, которые представляет кибертерроризм для каждой из этих стран, описаны меры, которые принимают данные страны для противодействия данной угрозе, представлен анализ эффективности этих мер. Также авторы сравнили различные подходы к противодействию кибертерроризму в каждой из этих стран, определили ключевые проблемы и вызовы, с которыми они сталкиваются, и рассмотрели вопрос о том, какие международные соглашения и инициативы могут помочь Беларуси, Казахстану и Азербайджану улучшить свои возможности по борьбе с кибертерроризмом.

Ключевые слова: киберпространство, кибертерроризм, киберпреступность, цифровая безопасность, Беларусь, Казахстан, Азербайджан.

Для цитирования: Тарасов Д. С., Солодухина Е. А., Марченкова В. Е., Скориков В. В. Противодействие кибертерроризму в Беларуси, Казахстане и Азербайджане // Постсоветские исследования. 2023;5(6):531-539.

Countering Cyberterrorism in Belarus, Kazakhstan and Azerbaijan

Daniil S. Tarasov[1], Yelizaveta A. Solodukhina[2], Valeria E. Marchenkova[3], Vladislav V. Skorikov[4]

[1, 2, 3, 4] *RUDN University named after P. Lumumba, Moscow, Russia*
[1] *E-mail: 1032211937@rudn.ru*
[2] *E-mail: 1132223119@rudn.ru*
[3] *E-mail: 1032220375@rudn.ru*
[4] *E-mail: 1132223091@rudn.ru*

Keywords: cyberspace, cyber terrorism, cybercrime, digital security, Belarus, Kazakhstan, Azerbaijan.

For citation: Daniil S. Tarasov, Yelizaveta A. Solodukhina, Valeria E. Marchenkova, Vladislav V. Skorikov Counteraction of cyberterrorism in Belarus, Kazakhstan and Azerbaijan // Postsovetskie issledovaniya = Post-Soviet Studies. 2023;5(6):531-539.

Кибертерроризм — это использование информационных технологий для проведения террористических действий. Как правило, это включает в себя хакерские атаки на компьютерные системы, сети и инфраструктуру, кражу конфиденциальной информации, распространение вирусов и других вредоносных программ, а также использование социальных сетей и интернета для навязывания своей идеологии

и привлечения новых сторонников [Буткевич 2018: 17].

Кибертерроризм может представлять серьезную угрозу для национальной безопасности по нескольким причинам. Во-первых, страны имеют критическую информационную инфраструктуру, такую как электроэнергетика, транспортные сети, финансовые системы и т.д., которые могут быть атакованы кибертеррористами. Атаки на такие системы могут привести к нарушению их работы и значительным экономическим потерям. Во-вторых, кибертерроризм может использоваться для вмешательства в политические процессы и выборы в странах. Кибератаки на системы государственного управления и электронного голосования могут привести к фальсификации результатов выборов, что может угрожать демократическим институтам и процессам. В-третьих, кибертерроризм может быть использован для дестабилизации общественного порядка и нарушения общественной безопасности в этих странах. Например, хакерские атаки на сайты правительственных органов или средств массовой информации могут вызвать панику и неуверенность среди населения [Мухамеджанова 2021: 50]. Наконец, кибертерроризм может быть использован для поддержки других форм терроризма, включая террористические группы, которые используют интернет для распространения своей идеологии, навязывания своих взглядов и привлечения новых сторонников. Такие действия могут привести к угрозе миру и безопасности не только в этих странах, но и во всем мире. В связи с этим, защита от кибертерроризма является критически важным элементом национальной безопасности и требует совместных усилий правительств, частного сектора и международного сообщества [Колин 2022: 46]

Понимание уровня угрозы, методов и технологий, используемых кибертеррористами, а также изучение мер и практик противодействия этой угрозе является крайне важным для Беларуси, Казахстана и Азербайджана. Кроме того, кибертерроризм является глобальной проблемой, которая требует совместных усилий и координации международных сообществ и стран в борьбе против нее [Колин 2021: 74]. Кроме того, с развитием технологий и увеличением количества устройств, подключенных к интернету, кибертерроризм становится все более угрожающим. Многие эксперты утверждают, что в ближайшие годы количество кибератак только возрастет, что делает необходимым принятие соответствующих мер по защите информационной инфраструктуры. Изучение опыта и мер, принятых в Беларуси, Казахстане и Азербайджане в борьбе с этой угрозой, может дать ценные уроки и рекомендации другим странам, столкнувшимся с аналогичными вызовами.

В Беларуси, Казахстане и Азербайджане кибертерроризм представляет ряд угроз для национальной безопасности и экономики. Например, в Казахстане в 2018 г. был зафиксирован кибератака на сайты государственных органов, энергетических компаний и медицинских учреждений[1]. Атака была проведена группой хакеров, которые украли конфиденциальные данные и требовали выкуп. Данный случай показал уязвимость казахстанских государственных систем и необходимость улучшения киберзащиты.

Глобальный индекс кибербезопасности (GCI) является надежным справочником, который измеряет приверженность стран кибербезопасности на глобальном уровне – для повышения осведомленности о важности и различных аспектах этой проблемы. В 2020 г. в рейтинге Global Cybersecurity Index Казахстан занял 31-е место, Азербайджан - 40-е место, а Беларусь - 89-е место[2]. Также существует Национальный индекс кибербезопасности (National Cybersecurity Index) - это глобальный оперативный индекс, который измеряет готовность стран к

[1] Кибератаки в Казахстане: с 2018 года зафиксировано более 2 млрд // Inbusiness.kz. 23.10.2019. URL: https://inbusiness.kz/ru/last/v-kazahstane-zafiksirovali-bolee-2-mlrd-kiberatak-s-2018-goda

[2] Global Cybersecurity Index 2020 // International Telecommunication Union. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

предотвращению киберугроз и управлению киберинцидентами. NCSI также является базой данных с общедоступными доказательственными материалами и инструментом для наращивания национального потенциала в области кибербезопасности. В рамках данного рейтинга Казахстан, Азербайджан и Беларусь занимают 76, 52, 67 места соответственно[1].

В Азербайджане кибертерроризм представляет угрозу для финансовой системы и критической инфраструктуры, такой как гидроэлектростанции, нефтепроводы и газопроводы. В 2018г. в стране была зафиксирована серия кибератак на банки, что привело к финансовым потерям, а также к лок-ауту в этом же году, когда половина страны осталась без света из-за аварии на Мингячевирской ГЭС. Кроме того, было обнаружено, что хакеры из Ирана попытались атаковать системы нефтяной компании SOCAR[2].

В Беларуси кибертерроризм также представляет угрозу для критической инфраструктуры, включая системы энергоснабжения и транспортные сети. В 2020г. была зафиксирована серия кибератак на белорусскую энергосистему, которые могли привести к отключению электричества во всей стране[3]. Кроме того, была проведена кибератака на белорусский телеканал, которая привела к сбою в работе телевизионного вещания.

Таким образом, кибертерроризм представляет серьезную угрозу для национальной безопасности Беларуси, Казахстана и Азербайджана. Для борьбы с этими угрозами необходимо улучшение киберзащиты и принятие мер на уровне правительств и частного сектора.

Кибертерроризм - это сложный и многогранный феномен, требующий комплексного подхода для его понимания и борьбы с ним. В 2019г. было выпущено исследование на тему Кибербезопасности в Казахстане. В работе подчеркивается, что национальные стратегии безопасности должны быть сбалансированы с глобальной стратегией по борьбе с кибертерроризмом, а также отмечаются основные уязвимости казахстанской критической инфраструктуры, такие как энергетические системы и банковский сектор. Авторы делают особый акцент на том, что в стране отсутствует стратегия в сфере кибербезопасности, которая определила бы траекторию стратегического плана. В части рекомендаций авторы приходят к выводам, что Казахстану необходимо проводить работы по повышению компьютерной грамотности населения, а также рассмотреть возможность привлечения зарубежных экспертов или усилить подготовку отечественных кадров в данной области [Зейнельгабдин, Исабаева 2019: 47].

Анализ нормативно-правовых документов по противодействию кибертерроризму в Беларуси, Казахстане и Азербайджане и государственных акторов, участвующих в реализации кибербезопасности страны, показывает, что каждая из этих стран имеет свою систему законодательства и подведомственные уполномоченные органы, целью которых является борьба с киберугрозами.

В Беларуси законодательство в области кибербезопасности включает в себя ряд законов и правовых актов, таких как Закон "Об информации, информационных технологиях и защите информации"[4], Закон "О борьбе с терроризмом"[5], а также Концепция информационной безопасности[6]. В 2020г. в Беларуси было создано Главное управление по противодействию киберпреступности при Министерстве

[1] National Cybersecurity Index. URL: https://ncsi.ega.ee/ncsi-index/?order=-ncsi

[2] Проблемы кибербезопасности в Азербайджане и пути их решения // Азербайджанский взгляд. 12.04.2023. URL: https://vzglyad.az/news/226567.html

[3] Минсвязи Белоруссии сообщило о полном восстановлении доступа к интернету // ТАСС. 12.08.2020. URL: https://tass.ru/obschestvo/9183075

[4] Закон Республики Беларусь от 10 ноября 2008г. № 455-З «Об информации, информатизации и защите информации»,

[5] Закон Республики Беларусь от 3 января 2002г. № 77-З "О борьбе с терроризмом"

[6] Концепция информационной безопасности Беларуси от 18 марта 2019г. URL: https://estu.1prof.by/napravlenie_raboti/informacionnaya-rabota/koncepciya-informacionnoj-bezopasnosti-respubliki-belarus/

внутренних дел, которое осуществляет оперативно-розыскную деятельность в сфере кибербезопасности[1]. Также в Беларуси существует межведомственная комиссия по борьбе с киберпреступностью, однако ее деятельность ограничивается реактивными мерами [Драгун 2020: 210].

В Казахстане вопросы кибербезопасности регулируются Законом "Об информатизации"[2] и Концепцией кибербезопасности («Киберщит Казастана»)[3], а также рядом подзаконных актов. Стоит выделить Казахстан на фоне других исследуемых стран, так как он имеет успехи по данной проблематике в правовом поле, в частности казахское правительство унифицировало требования в области информационно-коммуникационных технологий и информационной безопасности. В 2018г. был создан национальный координационный центр информационной безопасности, а также различные испытательные лаборатории по исследованию вредоносного кода. Правительство также предпринимает попытки по усилению данной отрасли, увеличивая число грантов по этой специальности[4].

В Азербайджане существует Закон "Об информации, информационных технологиях и защите информации"[5], а также ряд других законодательных актов, направленных на обеспечение безопасности в сфере информационных технологий. В защите кибербезопасности Азербайджана участвуют три основных государственных учреждения: Министерство связи и информационных технологий, Министерство национальной безопасности и Национальная академия наук Азербайджана. Также был создан Центр кибербезопасности (CERT.GOV.AZ), который учрежден при Министерстве связи и информационных технологий.

Данный центр действует в соответствии с полномочиями, делегированными Государственной службой специальной связи и информационной безопасности Азербайджанской Республики. Центр не имеет полномочий пресекать преступную деятельность, но оставляет за собой право передавать на рассмотрение материалы соответствующим правоохранительным органам. Центр является государственным органом, который занимается координацией действий субъектов информационной инфраструктуры, представлением отчетности о существующих и потенциальных рисках на уровне страны, обучением государственных, частных и других учреждений в области кибербезопасности и оказанием им методической помощи [Spînu 2020: 5]. Данный орган примечателен еще тем фактом, что является результатом сотрудничества Службы Электронной безопасности при Министерстве цифрового развития и транспорта Азербайджанской Республики и Израильским технологическим институтом Технион[6], с которым было подписано соглашение о взаимодействии в 2022г.

Однако, несмотря на наличие соответствующих законов и ведомств, эффективность мер по борьбе с кибертерроризмом в этих странах остается недостаточной. Как показывает анализ научных источников, существуют проблемы с координацией деятельности между различными ведомствами и организациями, занимающимися противодействием кибертерроризму. Также отмечается низкая осведомленность населения о проблемах

[1] Главное управление по противодействию киберпреступности ("Управление К") // МВД Республики Беларусь. URL: https://www.mvd.gov.by/ru/page/upravlenie-k/istoriya-urpsvt#!

[2] Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК "Об информатизации"

[3] Концепция кибербезопасности Казахстана от 30 июня 2017г. URL: https://adilet.zan.kz/rus/docs/P1700000407#z15

[4] Кибербезопасность в Казахстане – что сегодня актуально? // Mobilaser. 26.03.2021. URL: https://mobilaser.kz/kiberbezopasnost-v-kazahstane-chto-segodnya-aktualno/technologies/

[5] Закон Азербайджанской Республики от 3 апреля 1998г. №460-IГ "Об информации, информатизации и защите информации"

[6] Центр кибербезопасности Азербайджана: важный шаг на пути к инновационному обществу // Day.Az. 05.07.2022. URL: https://news.day.az/economy/1476391.html

кибербезопасности и отсутствие квалифицированных кадров в области кибербезопасности.

Общей проблемой всех трех стран является отсутствие единой координационной структуры, ответственной за противодействие кибертерроризму. Улучшение координации между ведомствами и организациями, увеличение финансирования программ обучения и повышения квалификации поможет странам выйти на новый уровень безопасности в данной области [Чубик 2013: 118].

Для оценки эффективности мер, принимаемых Беларусью, Казахстаном и Азербайджаном для борьбы с кибертерроризмом, можно провести анализ статистических данных по количеству кибератак и их последствиям в этих странах.

Согласно отчету компании Positive Technologies, за 2020 год в Беларуси зарегистрировано увеличение количества кибератак на банки на 23% больше, чем в предыдущем году. Казахстан также стал жертвой многочисленных кибератак в 2018 году, особенно в секторах государственного управления, здравоохранения и банковской сферы[1]. По данным Azerbaijan Cyber Security Centre, в Азербайджане зарегистрировано увеличение количества кибератак на банки и государственные учреждения, а также на крупные предприятия страны в 2020г. [Huseynov 2022: 165].

Таким образом, несмотря на принимаемые меры по противодействию кибертерроризму в Беларуси, Казахстане и Азербайджане, эффективность этих мер остается под вопросом, так как уровень угроз и атак на эти страны по-прежнему высок. Одной из главных проблем, с которыми сталкиваются Беларусь, Казахстан и Азербайджан в борьбе с кибертерроризмом, является отсутствие достаточной экспертизы в области кибербезопасности и недостаток квалифицированных кадров [Баширов 2015: 60]. Эта проблема может быть решена путем создания специальных образовательных программ и курсов, направленных на подготовку кадров в области кибербезопасности.

Возможно, необходимо улучшить и координировать действия по борьбе с кибертерроризмом на международном уровне, а также развивать национальные механизмы по обеспечению кибербезопасности. Также существует проблема отсутствия единой стратегии по противодействию кибертерроризму в каждой из этих стран. Для ее решения необходимо разработать и принять национальные стратегии и планы действий по борьбе с кибертерроризмом [Canzani 2018: 137].

В настоящее время важным вызовом в данном секторе является быстрое развитие технологий и постоянное изменение методов кибератак. Для более эффективной борьбы с кибертерроризмом необходимо постоянно совершенствовать и адаптировать технические средства и программы для защиты информационных систем. Стоит отметить, что в борьбе с кибертерроризмом необходимо учитывать не только технические аспекты, но и социальные и политические факторы [Лаврова 2021: 389]. Для решения этой проблемы необходимо улучшать информированность населения о кибербезопасности и расширять сотрудничество с другими странами в борьбе с кибертерроризмом.

Международное сотрудничество в борьбе с кибертерроризмом является одним из важнейших факторов в обеспечении кибербезопасности в мире [Tropina 2012: 88]. Беларусь, Казахстан и Азербайджан активно участвуют в различных инициативах и международных соглашениях.

Одним из ключевых документов в области кибербезопасности является Конвенция Совета Европы о киберпреступности (также известная как Будапештская конвенция), которая была подписана в 2001г. и вступила в силу в 2004г.[2] Беларусь и Казахстан присоединились к этой конвенции в 2016г., а Азербайджан - в 2011г. Конвенция Совета Европы о киберпреступности призывает к

[1] В Алматы открыто представительство Positive Technologies // Profit. 11.09.2018. URL: https://profit.kz/news/48596/V-Almati-otkrito-predstavitelstvo-Positive-Technologies/

[2] Convention on cybercrime // Council of Europe. 23.11.2001. URL: https://rm.coe.int/1680081561

принятию широкого спектра мер по борьбе с киберпреступностью, включая уголовное преследование киберпреступников, укрепление международного сотрудничества, защиту прав человека и свободы в интернете и т.д. [Левашова, Витюк 2021: С.128].

Другой важный международный документ, который затрагивает вопросы кибербезопасности — это Декларация ООН о праве на Интернет, которая была принята в 2011г.[1] Эта декларация призывает к обеспечению свободы доступа к информации в интернете, защите прав человека и свободы выражения в интернете, а также призывает государства предпринимать меры по борьбе с киберпреступностью.

Кроме того, существует ряд других международных инициатив и программ, направленных на укрепление кибербезопасности, таких как Глобальный центр кибербезопасности Интерпола, которые могут помочь Беларуси, Казахстану и Азербайджану в повышении своих возможностей по борьбе с кибертерроризмом [Колесников 2014].

Среди наиболее важных международных инициатив и организаций в области кибербезопасности можно выделить следующие:

- Международный союз электросвязи (ITU) - международная организация, которая занимается разработкой стандартов и регулированием телекоммуникационной инфраструктуры. Она также играет важную роль в разработке международных стандартов и практик по обеспечению кибербезопасности[2].
- Глобальный форум по кибербезопасности (GFCE) - международная платформа, которая объединяет государства, международные организации и частный сектор для обмена опытом и координации усилий по обеспечению кибербезопасности[3].
- Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) - международный орган, который занимается разработкой и реализацией международных мер борьбы с киберпреступностью, а также предоставляет помощь странам в развитии и улучшении их возможностей в борьбе с киберпреступностью[4].

В рамках этих инициатив и организаций Беларусь, Казахстан и Азербайджан могут получить доступ к международной экспертизе и помощи в разработке стратегий по борьбе с кибертерроризмом, обмену информацией и координации усилий с другими странами и организациями. Кроме того, участие в международных инициативах и соглашениях может способствовать повышению квалификации кадров в области кибербезопасности и усилению сотрудничества с частным сектором.

Однако, необходимо отметить, что успешная борьба с кибертерроризмом требует не только международного сотрудничества, но и наличия соответствующих национальных законодательных и организационных механизмов, а также развития кадрового потенциала в области кибербезопасности. Поэтому, кроме участия в международных инициативах, Беларусь, Казахстан и Азербайджан должны продолжать усиливать свои национальные возможности по борьбе с кибертерроризмом и обеспечению кибербезопасности.

Итоги анализа показывают, что Беларусь, Казахстан и Азербайджан сталкиваются с серьезными вызовами и проблемами в области кибербезопасности, включая угрозу кибертерроризма. В то же время, эти страны принимают меры для борьбы с этой угрозой, такие как развитие национальных центров кибербезопасности, законодательные инициативы и участие в международных

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression // Unites Nations. 16.05.2011. URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[2] ITU // About ITU. URL: https://www.itu.int/en/about/Pages/default.aspx

[3] GFCE // About GFCE. URL: https://thegfce.org/about-the-gfce/

[4] Контртеррористическое управление // Организации Объединенных Наций. URL: https://www.un.org/counterterrorism/ru

организациях и инициативах по данной проблематике. Однако, существующие проблемы, такие как недостаток кадров в области кибербезопасности, отсутствие единой стратегии по борьбе с кибертерроризмом и несовершенство законодательства, могут снизить эффективность этих мер. Международные соглашения и инициативы, такие как ITU, GFCE и UNODC, могут помочь этим странам улучшить свои возможности по борьбе с кибертерроризмом путем обмена опытом, разработки международных стандартов и координации усилий.

В целом, эффективность мер, которые принимают Беларусь, Казахстан и Азербайджан для борьбы с кибертерроризмом, зависит от того, насколько эффективно они смогут решить существующие проблемы и улучшить свою координацию с другими странами и международными организациями в области кибербезопасности.

В свете динамично развивающейся киберугрозы и нарастающих угроз кибертерроризма, важно проводить дальнейшие исследования и разработки в области кибербезопасности, которые могут быть полезны для Беларуси, Казахстана и Азербайджана. Одно из направлений исследований может быть связано с разработкой и реализацией новых технологий и инструментов для обнаружения, предотвращения и борьбы с кибертерроризмом. Например, использование искусственного интеллекта и машинного обучения для более точного и быстрого обнаружения кибератак, а также разработка новых методов анализа угроз и оценки рисков. Также важно проводить исследования в области кибернормативы и правовых аспектов кибербезопасности, чтобы совершенствовать существующие законы и политики в этой области, а также разработать новые международные договоренности и стандарты для борьбы с кибертерроризмом. Кроме того, следует обратить внимание на развитие образования и подготовки кадров в области кибербезопасности. Обучение специалистов и развитие квалификации в этой области могут помочь улучшить возможности стран в борьбе с кибертерроризмом и обеспечить эффективную защиту критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

Баширов А. В Вопросы информационной безопасности в Республике Казахстан // Актуальные проблемы современности. 2015. №4 (10). С. 59–61.

Буткевич С.А. Экстремизм и терроризм в киберпространстве: выявление, нейтрализация и предупреждение // Вестник Краснодарского университета МВД России. 2018. No 1. (39). С. 17–22.

Драгун Д.В. Кибертерроризм – новая и наиболее опасная форма терроризма в условиях цифровизации Белорусского государства / У истоков и в авангарде белорусской политологии: материалы науч. конф., посвящ. 30-летию кафедры политологии Белорус. гос. ун-та, Минск. 2020. С. 209-214.

Зейнельгабдин А.Б., Исабаева С.Б. Кибербезопасность Казахстана в период цифровой трансформации // Экономическая политика. 2019. No4(45). С. 47.

Колесников В.А. Международно-правовые основы сотрудничества по линии Интерпола // Вестник ВИ МВД России. 2014. №2.

Колин К.К. Современное международное информационное пространство и актуальные проблемы национальной и глобальной безопасности / Биосферная совместимость: человек, регион, технологии. 2022. С. 46-60.

Колин К.К. Цифровая трансформация общества и новое содержание проблемы информационной безопасности / Информационная безопасность личности субъектов образовательного процесса в цифровой информационно-образовательной среде. 2021. С. 72-86.

Лаврова Е.В. Цифровизация и угрозы национальной безопасности в контексте медийных технологий и систем мгновенного обмена сообщениями / Многонациональная Россия: вчера, сегодня, завтра. 2021. С. 385-390.

Левашова О.В., Витюк А.А. Положения Конвенции Совета Европы о кибербезопасности // Закон и право. 2021. №11. С.128-130

Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения / Правовые системы стран Азии. 2021. С. 49-55.

Чубик А.П. Терроризм в информационном пространстве // Известия Томского политехнического университета: философия, социология и культура. 2013. Т. 323. No 6. С. 117–121.

Canzani E. Risk management in (cyber-) Terrorism: Modeling insights and perspectives // Countering terrorist activities in cyberspace. 2018. P. 131-139.

Huseynov V. Hybrid Warfare in Azerbaijan: A Challenge to National Security / Media and Terrorism in the 21st Century. 2022. P. 164-182.

Spînu N. Azerbaijan Cybersecurity Governance Assessment // Geneva Centre for security sector Governance. 2020. C. 5

Tropina T. Fighting cybercrime: is it possible to develop a universal mechanism? // International justice. 2012. No 3. P. 86-95.

REFERENCES

Bashirov A. B. Issues of information security in the Republic of Kazakhstan // Actual problems of our time. 2015. №4 (10). C. 59-61.

Butkevich S.A. Extremism and terrorism in cyberspace: detection, neutralization and prevention // Bulletin of the Krasnodar University of the Russian Interior Ministry. 2018. No 1. (39). C. 17-22.

Dragun D.V. Cyber-terrorism - a new and most dangerous form of terrorism in conditions of digitalization of the Belarusian state / At the origins and in the forefront of Belarusian political science: materials of scientific conf. dedicated to the 30th anniversary of the Department of Political Science of the Belarusian State University, Minsk. 2020. C. 209-214.

Zeynelgabdin A.B., Isabaeva S.B. Cybersecurity of Kazakhstan in the Period of Digital Transformation // Economic Policy. 2019. No4(45). C. 47.

Kolesnikov V.A. International legal bases of cooperation on the Interpol line // Bulletin of the VI of the Ministry of Internal Affairs of Russia. 2014. №2.

Kolin K.K. Modern International Information Space and Current Problems of National and Global Security / Biosphere Compatibility: Man, Region, Technology. 2022. C. 46-60.

Kolin K.K. Digital transformation of society and the new content of the problem of information security / Information security of the subjects of the educational process in the digital information and educational environment. 2021. C. 72-86.

Lavrova E.V. Digitalization and threats to national security in the context of media technologies and instant messaging / Multinational Russia: yesterday, today, tomorrow. 2021. C. 385-390.

Levashova O.V., Vitiuk A.A. Provisions of the Council of Europe Convention on Cyber Security // Law and Law. 2021. №11. C.128-130

Mukhamedjanova A.D. Features of the dynamics of cybercrime in the Republic of Kazakhstan and its impact on its prevention / Asian Legal Systems. 2021. C. 49-55.

Chubik A.P. Terrorism in the information space // Proceedings of Tomsk Polytechnic University: Philosophy, Sociology and Culture. 2013. T. 323. No 6. C. 117-121.

Canzani E. Risk management in (cyber-) Terrorism: Modeling insights and perspectives // Countering terrorist activities in cyberspace. 2018. P. 131-139.

Huseynov V. Hybrid Warfare in Azerbaijan: A Challenge to National Security / Media and Terrorism in the 21st Century. 2022. P. 164-182.

Spînu N. Azerbaijan Cybersecurity Governance Assessment // Geneva Centre for security sector governance. 2020. C. 5

Tropina T. Fighting cybercrime: is it possible to develop a universal mechanism? 2012. No 3. P. 86-95.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Тарасов Даниил Станиславович, магистр в области «Зарубежного регионоведения», Российский университет дружбы народов им. П. Лумумбы. Москва, Россия. E-mail: 1032211937@rudn.ru

Солодухина Елизавета Александровна, магистр в области «Международных отношений», Российский университет дружбы народов им. П. Лумумбы. Москва, Россия. E-mail: 1132223119@rudn.ru

Марченкова Валерия Евгеньевна, магистр в области «Международных отношений», Российский университет дружбы народов им. П. Лумумбы. Москва, Россия. E-mail: 1032220375@rudn.ru

Скориков Владислав Витальевич, Магистрант в области «Международных отношений», Российский университет дружбы народов им. П. Лумумбы. Москва, Россия. E-mail: 1132223091@rudn.ru

Daniil S. Tarasov, MA in Regional Studies, RUDN University named after P. Lumumba. Moscow, Russia. E-mail: 1032211937@rudn.ru

Yelizaveta A. Solodukhina, MA in International Relations, RUDN University named after P. Lumumba, Moscow, Russia. E-mail: 1132223119@rudn.ru

Valeria E. Marchenkova, MA in International Relations, RUDN University named after P. Lumumba, Moscow, Russia. E-mail: 1032220375@rudn.ru

Vladislav V. Skorikov, MA in International Relations, RUDN University named after P. Lumumba, Moscow, Russia. E-mail: 1132223091@rudn.ru