Научная статья
УДК 343.7
https://doi.org/10.33874/2072-9936-2024-0-3-200-212

КИБЕРТЕРРОРИЗМ КАК УГРОЗА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА

Владимир Владимирович Баранов[1]

Вадим Михайлович Пашин[2]

[1] Академия управления МВД России, 125993, Россия, г. Москва, ул. 3ои и Александра Космодемьянских, д. 8

[2] Всероссийский государственный университет юстиции (РПА Минюста России), 117638, Россия, г. Москва, ул. Азовская, д. 2, корп. 1

[1] de_la_sergio@mail.ru

[2] paschin@mail.ru

Аннотация

Исследование различных аспектов проявления кибертерроризма актуализируется в связи с ускорением роста числа совершаемых преступлений террористической и экстремистской направленности в киберпространстве с применением новейших технических средств и методов психологического воздействия. Целью настоящей работы является определение специфических признаков кибертерроризма как угрозы информационно-психологической безопасности. Основными методами исследования выступили исторический анализ, сравнительный анализ, индукция и дедукция, герменевтика. На основе изучения эволюции понятия «кибертерроризм» в научной литературе и средств осуществления террористического воздействия в киберпространстве авторами определены основные отличия кибертерроризма и преступлений террористической направленности, выявлены наиболее эффективные средства осуществления такого воздействия в сети Интернет и социальных сетях. Особое внимание уделено механизмам воздействия на индивидуальное и коллективное сознание. В статье даны рекомендации по совершенствованию методов противодействия кибертерроризму и обеспечению информационно-психологической безопасности человека и общества.

Ключевые слова: кибертерроризм; терроризм; кибербезопасность; информационная безопасность; информационно-психологическая безопасность.

Для цитирования: *Баранов В. В., Пашин В. М.* Кибертерроризм как угроза информационно-психологической безопасности личности, общества и государства // Вестник Российской правовой академии. 2024. № 3. С. 200–212. https://doi.org/10.33874/2072-9936-2024-0-3-200-212

Research Article

CYBERTERRORISM AS A THREAT TO THE INFORMATION AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL, SOCIETY AND THE STATE

Vladimir V. Baranov[1]

Vadim M. Pashin[2]

[1] Academy of the Ministry of Internal Affairs of Russia, 8 Zoia and Alexander Kosmodemianskikh St., Moscow, 125993, Russia

[2] All-Russian State University of Justice, 2, Bldg. 1 Azovskaia St., Moscow, 117638, Russia

[1] de_la_sergio@mail.ru

[2] paschin@mail.ru

Abstract

The study of various aspects of the manifestation of cyberterrorism is being updated in connection with the accelerated growth in the number of terrorist and extremist crimes committed in cyberspace using the latest technical means and methods of psychological influence. The purpose of this study is to identify specific signs of cyberterrorism as a threat to information and psychological security. The main research methods were historical analysis, comparative analysis, induction and deduction, hermeneutics. Based on the study of the evolution of the concept of "cyberterrorism" in the scientific literature and the means of carrying out terrorist influence in cyberspace, the authors have identified the main differences between cyberterrorism and terrorist crimes, and identified the most effective means of carrying out such influence on the Internet and social networks. Special attention is paid to the mechanisms of influence on individual and collective consciousness. The article provides recommendations on improving methods of countering cyberterrorism and ensuring information and psychological security of a person and society.

Keywords: cyberterrorism; terrorism; cybersecurity; information security; information and psychological security.

For citation: *Baranov V. V., Pashin V. M.* Cyberterrorism as a Threat to the Information and Psychological Security of the Individual, Society and the State. *Herald of the Russian Law Academy*, 2024, no. 3, pp. 200–212 . (In Russ.) https://doi.org/10.33874/2072-9936-2024-0-3-200-212

Введение

В XXI в. проблема кибертерроризма приобретает все бóльшую актуальность в связи с бурным развитием информационных технологий. В отличие от традиционных способов воздействия на сознание людей, заключавшихся в совершении прямых актов насилия, организации взрывов, террористических атак на социальные объекты и правительственные учреждения и т.д. с целью провокации паники, страха, подрыве основ безопасности, кибертеррористы применяют различные методы психологического воздействия, которые сложнее идентифицировать и предотвратить.

Развитие информационных технологий и их транснациональный характер, а также ускорение процессов глобализации информационного пространства и сети Интернет, привело правительства большинства стран мира к необходимости разработки и внедрения правовых механизмов регулирования процессов взаимодействия между субъектами такого пространства. Так, с начала 2000-х гг. был принят ряд международных актов и соглашений, в частности Хартия глобального информационного общества (Окинава, 22 июля 2000 г.); Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве) (Будапешт, 23 ноября 2001 г.); Конвенция Совета Европы «О предупреждении терроризма» (Варшава, 16 мая 2005 г.) и др. В Российской Федерации сферы информации и информационной безопасности регулируются Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказом ФСБ РФ от 31 августа 2010 г. № 416 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования», указом Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», указом Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности», распоряжением Правительства РФ от 21 декабря 2021 г. № 3759-р «От утверждении Стратегического направления в области цифровой трансформации науки и высшего образования».

1. Эволюция понятия «кибертерроризм» в научной литературе

На сегодняшний день различные аспекты кибертерроризма и его влияния на общество и государственную безопасность являются предметом междисциплинарных исследований, количество которых неуклонно растет. Так, в 2019–2022 гг. было опубликовано 178 научных статей [8]. Тем не менее, несмотря на достаточно широкую научную изученность проблемы и наличие достаточно большого числа

эмпирических исследований, включающих в том числе анализ судебной практики по делам, связанным с кибертерроризмом и киберэкстремизмом, в научной литературе не существует единого определения базовых понятий «кибертерроризма» и «информационно-психологическая безопасность».

Первая попытка определения понятия «кибертерроризм» была предпринята Б. Коллином в середине 1980-х гг. Однако данное понятие Коллин использовал для описания потенциальной угрозы, связанной с развитием средств связи и сети Интернет [5, с. 188–190]. На основе подробного исследования основных подходов к определению понятия «кибертерроризма» Л. Я. Тарасова [21, с. 213] приходит к выводу, что большинство существующих определений данного понятия находят свое отражение в судебных решениях, однако, учитывая скорость изменения цифровой среды, появления новых технологий обработки и распространения информации, следует ожидать, что содержание данного понятия будет изменяться.

Научно-правовое определение понятие кибертерроризма опирается в первую очередь на диспозицию ч. 1 ст. 205 УК РФ, согласно которой террористический акт – это «совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо нанесения иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях». Сегодня данная статья УК РФ трактуется в расширенном смысле, включая любые действия, имеющие указанные цели, таким образом в определении кибертерроризма на первый план выносится объект посягательства, а не непосредственные методы и способы воздействия.

Исходя из выше изложенного, А. Н. Васильева предлагает определить кибертерроризм как «преднамеренную, политически мотивированную атаку на глобальную компьютерную сеть, компьютерную систему и содержащуюся в компьютере информацию» [6, с. 234]. Последствие такой атаки отвечают содержанию диспозиции ч .1 ст. 205 УК РФ и заключаются в создании опасности для жизни и здоровья людей, а также стремлении субъекта действия к нарушению общественной безопасности, запугиванию и провокации военного конфликта. Объектами кибератак могут быть компьютерные системы управления объектами инфраструктуры, финансовые системы, личные данные пользователей сети Интернет и другие элементы информационных систем. Основными средствами осуществления кибератак выступают вредоносные компьютерные программы, вирусы, «логические бомбы», и другие виды информационного оружия [6].

Таким образом, в отечественной науке складываются два основных направления определения понятия «кибертерроризм»: «техническое» – использование программных средств воздействия на информационные системы с целью нанесения ущерба и нарушения работы различных стратегических и инфраструктурных объектов; «междисциплинарное» – совершение в информационном пространстве любых действий, направленных на дестабилизацию общества, работы органов государственного управления, формирование страха и искаженных представлений о происходящих событиях и т.д.

2. Разграничение кибертерроризма и преступлений экстремистской и террористической направленности, совершаемых с использованием информационных технологий и сети Интернет

Важным вопросом является принципиальное различение террористической деятельности, осуществляемой с использованием информационных технологий и посредством сети Интернет, и собственно кибертерроризма, реализуемого исключительно в цифровом информационном пространстве. Так, те террористические действия, целью которых является вывод из строя объектов инфраструктуры, осуществление террористических актов на территории страны, организация захвата заложников, взрывов, актов насилия и устрашения в реальности, следует отличать от психологического воздействия, осуществляемого с целью дестабилизации психического состояния индивидов, социальных групп и общества в целом.

Отдельно следует анализировать и квалифицировать действия, относимые к категории информационно-технического терроризма. Например, взлом системы управления авиапассажирскими перевозками с целью организации столкновения авиалайнеров является террористическим актом, осуществленным с применением информационно-компьютерных технологий (ИКТ), в то время как взлом правительственного ресурса с целью размещения на нем заведомо ложной, провокационной, шокирующей и иной информации, способной нанести ущерб психологическому здоровью граждан, является непосредственно актом кибертерроризма. Аналогичным образом организация подготовки террористического акта посредством общения в социальной сети, мессенджерах, вербовка новых членов террористической организации и привлечение их к организации террористической деятельности следует определять как террористическую деятельности с использованием социальных сетей, в то время как распространение в социальной сети видеороликов, сообщений, постов и ложной информации о совершенных преступлениях, актах терроризма, гибели мирных людей, злоупотреблениях органов государственной власти и т.д. с целью формирования паники, страхов, ощущения опасности и недоверия к государственной власти подходит под определение кибертерроризма.

Обоснованной выглядит концепция критериев кибертеррторизма, описанная А. Ю. Пинчуком с опорой на труды Дж. Бреннона (*J. W. Brennan*), С. Годона (*S. Gordon*), Т. Томаса (*T. L. Thomas*) [19, с. 92]:

1) осуществление террористического воздействия через киберпространство;

2) наличие политических и (или) идеологических целей и мотивов;

3) наличие насилия или угрозы насилием;

4) наличие продолжительных психологических последствий, выходящих за рамки непосредственной жертвы;

5) наличие определенного субъекта воздействия (организации, конспиративной ячейки, представителя/представителей террористического движения;

6) субъект террористического воздействия должен относиться к негосударственным образованиям или субнациональным группам.

Вместе с тем А. Ю. Пинчук подчеркивает, что применение интернет-технологий для организации террористических актов, привлечения сторонников, получения финансовой поддержки и совершения других преступлений, связанных с деятель-

ность террористической организации следует рассматривать как злонамеренное использование сети Интернет. Кибертерроризм реализуется исключительно внутри киберпространства.

Представленная идея о разделении действий террористического характера на те, что совершаются с использованием сети Интернет, и собственно кибертерроризма, не выходящего за рамки интернет-пространства, видится целесообразной.

Показательным с этой точки зрения является размещение в сети Интернет различных инструкций по изготовлению взрывчатых веществ, оружия, наркотиков, способов взлома компьютерных программ и шифров [22, с. 142]. Такая информация предлагается в качестве научно-просветительской, однако ее воздействие на сознание человека и коллективное сознание имеет далеко идущие последствия.

В первое десятилетие XXI в. одним из основных каналов террористического воздействия в киберпространстве были сайты террористических организаций. Основной целью таких сайтов было формирование определенных ценностей и установок у широкой аудитории и деморализация противников. В состав размещаемых материалов включались информация о террористической организации, история ее создания и деятельности, программу (манифесты), биографии лидеров, хроники совершенных террористический актов как свидетельства успешности и эффективности работы организации. При этом сайт сам по себе выполнял одну из главных функций террористической деятельности – устрашение, формирование чувства незащищенности и психологического давления. Средствами достижения данной цели являлась публикация видеозаписей с казнями заложников, сообщений о готовящихся террористических актах, о наличии агентов во всех городах, о больших поставках оружия и боеприпасов и т.д. Поддержка сайтов и привлечение новых членов осуществлялась при помощи *e-mail*-рассылок [4, с. 13, 15].

Таким образом, целесообразно понимать под кибертерроризмом действия, направленные на оказание психологического воздействия и осуществляемые исключительно в киберпространстве. Основным объектом кибертерроризма в таком контексте определения данного феномена становится информационно-психологическая безопасность.

3. Механизмы воздействия на индивидуальное и коллективное сознание. Разработка мер по противодействию кибертерроризму

Кибертерроризм как угроза информационно-психологической безопасности личности представляет собой применение различных способов воздействия на индивидуальное и массовое сознание с целью формирования деструктивных установок, социально опасного поведения, привлечения человека к противоправной и преступной деятельности за счет внедрения в сознание ложных представлений о необходимости, правильности и обоснованности таких действий.

Для разработки мер по противодействию кибертерроризму и обеспечению информационно-психологической безопасности необходимо изучить механизмы воздействия на психику человека, социальных групп и общества, используемые кибертеррористами.

Анализируя проблему информационно-психологической безопасности личности, А. А. Бастрон справедливо указывает на отсутствие технологического инстру-

ментария измерения оценок ущерба психическому здоровью [3, с. 27]. Тем не менее возможно выделить объект информационного воздействия, которым является сфера индивидуального, сфера группового и сфера массового сознания. Г. В. Емельянов, В. Е. Лепсков, А. А. Стрельцов под такой сферой на личностном уровне понимают «способность человека адекватно воспринимать окружающую действительность, свое место во внешнем мире, формировать в соответствии со своим жизненным опытом определенные убеждения и принимать решения в соответствии с ними» [10, с. 48].

Групповое и массовое сознание в данном контексте целесообразно понимать как систему базовых ментальных ценностей, обеспечивающих стойкую групповую и социальную идентичность, социально адаптированные модели поведения, систему восприятия и отношений к различным явлениям. Информационное воздействие на такие сферы осуществляются с целью разрушения или замещения таких ценностей, моделей и установок [13, с. 82].

И. Ф. Кефели и Р. М. Юсупов приводят следующие деструктивные составляющие информационной среды, являющиеся угрозой информационно-психологической безопасности личности:

1) широко распространяемые ложные сведения о государственных, политических, религиозных деятелях, участниках различных выборных кампаний;

2) ложные сообщения об авариях на предприятиях промышленности (атомных электростанциях, химических заводах и других), о заминированных домах, поездах, самолетах, о финансовых крахах компаний, провокации и слухи в политической сфере;

3) различного вида информация, вызывающая страх, агрессию, недовольство, раздражительность, порождающая сомнения, призывающая к деструктивным действиям;

4) информационные сигналы, изменяющие психофизическое состояние людей, повышающие их утомляемость, вызывающие головные боли, повышающие давление и другие;

5) деструктивные программы, как отрицательно влияющие на людей, так и дезорганизующие различные системы управления, вычислительные сети и технические средства и т.д. [13, с. 162].

Негативному воздействию кибертеррористов подвергаются следующие элементы общественного порядка: идеологическая, символическая, нормативная и экономическая системы [13, с. 57].

Целью воздействия на идеологическую систему является национальных замещение политических идеалов иными, что в конечном счете приводит к развитию в обществе различных форм экстремизма. В рамках атаки на символическую систему производится дискредитация важных государственных (флаг, герб, гимн) и социокультурных символов (памятников, мемориалов, объектов культурного наследия), что способствует распространению актов вандализма. При воздействии на нормативные установки производится разрушение основ правового сознания, дискредитация действующего законодательства, этических норм, что приводит к распространению девиантных и делинквентных форм поведения, нарушениям правопорядка. Целенаправленное

воздействие на экономическую систему состоит в формировании представлений о несправедливости распределения ресурсов, необходимости восстановления такой справедливости за счет активных действий, что в свою очередь приводит к повышению числа экономических преступлений, а также массовым беспорядкам, сопряженным с мародерством и нанесением экономического ущерба.

Таким образом, очевидно, что кибертерроризм имеет более глубокие и системные последствия, нежели простое использование компьютерных и Интернет технологий с целью организации террористической деятельности на территории страны. Применение различных технологий психологического воздействия кибертеррористами подвергает опасности большинство сфер безопасности общества.

О. А. Нестерчук в своем исследовании негативного психологического воздействия с использованием информационных технологий использует понятие «хоррор-менеджмента», решающего задачи умышленного и целенаправленного внедрения негативной информации в массовое сознание, формирование чувства незащищенности за счет создания и поддержки атмосферы ненависти, страха, агрессии и тревоги, а также формирование общественного мнения, необходимого для обеспечения возможности реализации целей воздействующего субъекта. Такое воздействие ставит под угрозу не только психическое здоровье и благополучие человека и общества, но и национальную безопасность, поскольку субъекты воздействия, формируя у масс представление о слабости действующей государственной системы и власти, подталкивают общество к мысли о необходимости смены властного субъекта на более сильного, способного решить социальные проблемы и гарантировать безопасность страны [17].

В исследовании А. В. Манойло к методам психологического воздействия относятся:

1) создание перенасыщенного информационного фона (эффект эмоциональной перегрузки);

2) намеренное дозирование информации с целью исключения ценных фрагментов и представления искаженной картины происходящего;

3) сообщение заведомо ложных сведений, имеющих ценность для общества, представляющих угрозу и т.д. («большая ложь»);

4) создание сообщений, содержащих как реальные факты, так и вымысел и создающих эффект достоверности за счет подтверждения правдивой информации;

5) сообщение лживой информации в качестве ответа на острый социальный запрос («своевременная ложь»);

6) намеренное замалчивание важной информации и сообщение ее тогда, когда уже невозможно ничего изменить [9].

Развитие социальных сетей и совершенствование технологий менеджмента восприятия [11] актуализирует вопросы применения таких инструментов, как формирование новостных лент, предложение контента (контекстная реклама, таргетинг), модерация комментариев и т.д. Во многом содержание и речевое поведение участников коммуникации на виртуальных площадках определяется политикой владельцев и менеджеров, однако существуют и государственные механизмы регулирования, например, вступивший в силу 1 февраля 2021 г. Закон № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологи-

ях и о защите информации» предусматривает ограничение и блокировку противоправного контента.

Алгоритмы подбора контента на основе предпочтений пользователя фактически способствуют формированию в киберпространстве множества изолированных «эхо-камер» – замкнутых сообществ пользователей, придерживающихся сходных позиций и солидаризирующихся вокруг них. Пользователи с отличными взглядами в таких «эхо-камерах» не воспринимаются, дискредитируются и получают статус «чужих» [2, с. 153]. Данный механизм опирается на базовые психологические реакции и потребности человека в построении ментальной разметки реальности и оценочной системы, позволяющей принимать решения и делать рациональный выбор. Границы «эхо-камеры» и ее архитектура формируют четкую структуру убеждения и внутренние фильтры информации, не допускающие в сознание альтернативные сведения и информацию, ставящую под угрозу сложившуюся систему убеждений [25]. Данное свойство социальных сетей и интернет-сообществ позволяет кибертеррористам легко выстраивать самоподдерживающиеся сообщества пользователей, увеличивая эффективность распространяемой информации экстремистского и террористического характера. Важным аспектом функционирования «эхо-камер» в кибертерроризме является целенаправленное применение техник убеждения и дискредитации информации, опровергающей фальсифицированные сообщения. Наибольшую опасность для информационно-психологической безопасности человека и общества представляет эффект психологического комфорта, возникающий внутри «эхо-камеры». Люди, находящиеся внутри такого информационного пространства, не воспринимают внешнюю аргументацию вследствие работы глубинных психологических механизмов, поддерживающих целостность психики. Вовлечение в «эхо-эхокамеру» происходит постепенно с опорой на базовые ценности человека – ценность жизни, справедливости, безопасности, честности, открытости, защиты своих интересов. В «эхо-камерах» доминирует эмоциональный дискурс, воздействующий на бессознательные структуры, радикализирующий мышление и активирующий защитные механизмы психики, которые впоследствии работают на воспроизводство внедренных в сознание установок.

С 2017 г. в спектр инструментов, используемых кибертеррористами, активно внедряется технология *Deepfake* (от англ. *deep learning* – «глубокое обучение» и *fake* – «фальшивый»), представляющая собой реалистичную манипуляцию аудио- и видеоматериалами с помощью искусственного интеллекта. При помощи специальных программ производится наложение лиц и голосов людей на видеоматериалы различного содержания, позволяющего создавать убедительные сообщения. При использовании простых программ подделка легко определяется визуально, однако сегодня существуют достаточно сложные программные продукты, позволяющие производить замену лица и голоса на протяжении длительного отрезка видеозаписи и даже в режиме потокового видео [7]. Таким образом, террористические организации получают возможность создавать провокационный контент, выглядящий достоверно, например, фальсифицировать выступления государственных лидеров, предоставлять пользователям видеозаписи якобы секретных заседаний членов правительства и представителей международных организаций с целью их дискредитации и т.д.

Развитие технологий создания и распространения вредного контента, ставящего под угрозу информационно-психологическую безопасность человека и общества, сопровождается не менее быстрым развитием средств выявления и блокировки такого контента [7].

Обзор существующих технологий и методов организации кибер-террористической деятельности в контексте расширенного определения понятия кибертерроризма позволяет выделить программные и психологические средства воздействия. Программные средства включают в себя применение различных вредоносных программ, алгоритмов распространения и продвижения контента, создания фальсифицированного контента и т.д. Такие средства определяются при помощи специальных компьютерных программ и средств мониторинга с использованием искусственного интеллекта, потому могут быть сравнительно легко зафиксированы. Причем, на сегодняшний день существуют апробированные методики определения ущерба, нанесенного информационной системе [15], опирающиеся на количественную и качественную оценки материального (стоимость восстановления поврежденного оборудования и программного обеспечения, финансовые потери и т.д.) и нематериального (репутационные потери, сокращение числа пользователей, клиентов, дискредитация организации и пр.) ущерба.

Выявление и оценка психологического ущерба существенно затруднены. С одной стороны, известны и определены способы и механизмы воздействия на индивидуальное и массовое сознание, однако степень такого воздействия, а также его последствия во многом зависят от личностных особенностей объекта воздействия, более того, нейтральная информация может искажаться внутри сознания индивида, создавая угрозу его психическому состоянию.

Заключение

Таким образом, очевидно, что дальнейшее совершенствование способов выявления и предотвращения кибертерроризма как угрозы информационно-психологической безопасности требует разработки методов оценки психологического ущерба, распознавания и блокировки контента, внедрение новых систем безопасного поиска, блокирующих потенциально опасные запросы пользователей и т.д.

Пристатейный библиографический список

1. *Алескеров В. И., Колокольчикова О. Н.* О преступлениях экстремистской и террористической направленности с использованием сферы телекоммуникаций и компьютерной информации // Научный компонент. 2020. № 3 (7).

2. *Бажанов В. А.* Особенности познавательных механизмов в информационную эпоху: «эхо-пузыри» и «эхо-камеры» // Философский журнал/Philosophy Journal. 2022. Т. 15. № 4.

3. *Бастрон А. А.* Проблема информационно-психологической безопасности личности // Научные труды Института непрерывного профессионального образования. 2016. № 6.

4. *Белоножкин В. И., Остапенко Г. А.* Информационные аспекты противодействия терроризму. М. : Горячая линия-Телеком, 2009.

5. *Бураева Л. А.* Кибертерроризм как новая и наиболее опасная форма терроризма // Проблемы экономики и юридической практики. 2017. № 2.

6. *Васильева А. Н.* Понятие и проблемы противодействия кибертерроризму // Успехи современного естествознания. 2011. № 8.

7. *Власенко А. В., Киселев П. С., Склярова Е. А.* Искусственный интеллект и проблемы кибербезопасности. Технология Deepfake // Молодой ученый. 2021. № 21 (363).

8. Вызовы 21 века: Кибертерроризм и информационные войны. Противостояние в информационном пространстве Интернета: библиографический список статей (2020–2022 гг.) / сост. Т. В. Нездоймина. Ростов-на-Дону, 2022.

9. *Манойло А. В.* Государственная информационная политика в особых условиях : монография. М. : МИФИ, 2003.

10. *Емельянов Г. В., Лепский В. Е., Стрельцов А. А.* Проблемы обеспечения информационно-психологической безопасности России // Информационное общество. 1999. № 3.

11. *Забарин А. В.* Менеджмент восприятия как психолого-политический феномен: генезис проблемы // Вопросы политической психологии. 2001. № 1.

12. *Зинченко Ю. П., Шайгерова Л. А., Шилко Р. С.* Психологическая безопасность личности и общества в современном информационном пространстве // Национальный психологический журнал. 2011. № 2 (6).

13. Информационно-психологическая и когнитивная безопасность : коллективная монография / под ред. И. Ф. Кефели, Р. М. Юсупова. СПб. : ИД «Петрополис», 2017.

14. *Камергоев Б. М.* Кибертерроризм – актуальная проблема современного общества // Вопросы российского и международного права. 2019. Т. 9. № 8А.

15. *Карпычев В. Ю.* Экономические аспекты формирования информационной безопасности // Вестник Самарского государственного аэрокосмического университета. 2004. № 2.

16. *Мезенцев Д. Ф.* Психологическое воздействие информационных фантомов // Хрестоматия к учебнику по политической психологии. СПб. : Коло, 2012.

17. *Нестерчук О. А.* Традиционные и инновационные политические технологии в информационно-психологическом противоборстве // PolitBook. 2015. № 2.

18. *Огородник А. В.* История возникновения кибертерроризма: от киберпреступности до кибертерроризма // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности. 2021.

19. *Тарасова Л. Я.* Эволюция понятия информационного терроризма (кибертерроризма) и его значение на современном этапе // Научный вестник Омской академии МВД. 2022. № 3 (86).

20. *Пинчук А. Ю.* Кибертерроризм как актуальная проблема современного мирового порядка // Теории и проблемы политических исследований. 2018. Т. 7. № 5.

21. *Пучков Д. В.* Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8. № 4.

22. *Юсупов Р. М.* Наука и национальная безопасность. СПб. : Наука, 2006.

23. *Boutyline A., Wilier R.* The Social Structure of Political Echo Chambers: Variation in Ideological Homophily in Online Networks // Political Psychology. 2017. Vol. 38. No. 3.

24. *Sasa-hara K., Chen W., Peng H. et al.* Social Influence and Unfollowing Accelerate the Emergence of Echo Chambers // Journal of Computational Social Science. 2021. Vol. 4.

25. *Brenner S. W.* Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford : Oxford University Press, 2009.

References

1. *Aleskerov V. I., Kolokolchikova O. N.* On Extremist and Terrorist Crimes Using the Sphere of Telecommunications and Computer Information. *Scientific Component*, 2020, no. 3 (7). (In Russ.)

2. *Bazhanov V. A.* Features of Cognitive Mechanisms in the Information Age: "Echo Bubbles" and "Echo Chambers". *Philosophy Journal*, 2022, vol. 15, no. 4. (In Russ.)

3. *Bastron A. A.* The Problem of Information and Psychological Security of the Individual. *Scientific Works of the Institute of Continuing Professional Education*, 2016, no. 6. (In Russ.)

4. *Belonozhkin V. I., Ostapenko G. A.* Information Aspects of Countering Terrorism. Moscow: Hotline-Telecom, 2009. (In Russ.)

5. *Buraeva L. A.* Cyberterrorism as a New and Most Dangerous Form of Terrorism. *Problems of Economics and Legal Practice*, 2017, no. 2. (In Russ.)

6. *Vasilieva A. N.* Concept and Problems of Countering Cyber Terrorism. *Advances in Modern Natural Science*, 2011, no. 8. (In Russ.)

7. *Vlasenko A. V., Kiselev P. S., Skliarova E. A.* Artificial Intelligence and Cybersecurity Issues. Deepfake Technology. *Young Scientist*, 2021, no. 21 (363). (In Russ.)

8. *Nezdoimina T. V. (comp.).* Challenges of the 21st Century: Cyber Terrorism and Information Wars. Confrontation in the Information Space of the Internet: Bibliographic List of Articles (2020–2022). Rostov-on-Don, 2022. (In Russ.)

9. *Manoilo A. V.* State Information Policy in Special Conditions: Monograph. Moscow: MIPhI, 2003. (In Russ.)

10. *Emelianov G. V., Lepsky V. E., Streltsov A. A.* Problems of Ensuring Information and Psychological Security of Russia. *Information Society*, 1999, no. 3. (In Russ.)

11. *Zabarin A. V.* Perception Management as a Psychological and Political Phenomenon: The Genesis of the Problem. *Questions of Political Psychology*, 2001, no. 1. (In Russ.)

12. *Zinchenko Iu. P., Shaigerova L. A., Shilko R. S.* Psychological Safety of the Individual and Society in the Modern Information Space. *National Psychological Journal*, 2011, no. 2 (6). (In Russ.)

13. *Kefeli I. F., Iusupov R. M. (eds.).* Information-Psychological and Cognitive Security: Collective Monograph. St. Petersburg: Petropolis, 2017. (In Russ.)

14. *Kamergoev B. M.* Cyberterrorism Is a Pressing Problem of Modern Society. *Issues of Russian and International Law*, 2019, vol. 9, no. 8A. (In Russ.)

15. *Karpychev V. Iu.* Economic Aspects of the Formation of Information Security. *Bulletin of Samara State Aerospace University*, 2004, no. 2. (In Russ.)

16. *Mezentsev D. F.* Psychological Impact of Information Phantoms. In Reader for a Textbook on Political Psychology. St. Petersburg: Kolo, 2012. (In Russ.)

17. *Nesterchuk O. A.* Traditional and Innovative Political Technologies in Information-Psychological Confrontation. *PolitBook*, 2015, no. 2. (In Russ.)

18. *Ogorodnik A. V.* The History of the Emergence of Cyberterrorism: From Cybercrime to Cyberterrorism. In Donetsk Readings 2021: Education, Science, Innovation, Culture and Challenges of Our Time. 2021. (In Russ.)

19. *Tarasova L. Ia.* The Evolution of the Concept of Information Terrorism (Cyberterrorism) and its Significance at the Present Stage. *Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs*, 2022, no. 3 (86). (In Russ.)

20. *Pinchuk A. Iu.* Cyberterrorism as an Urgent Problem of the Modern World Order. *Theories and Problems of Political Research*, 2018, vol. 7, no. 5. (In Russ.)

21. *Puchkov D. V.* Cyberterrorism as a New Threat. *Victimology*, 2021, vol. 8, no. 4. (In Russ.)

22. *Iusupov R. M.* Science and National Security. St. Petersburg: Nauka, 2006. (In Russ.)

23. *Boutyline A., Wilier R.* The Social Structure of Political Echo Chambers: Variation in Ideological Homophily in Online Networks. *Political Psychology*, 2017, vol. 38, no. 3.

24. *Sasa-hara K., Chen W., Peng H. et al.* Social Influence and Unfollowing Accelerate the Emergence of Echo Chambers. *Journal of Computational Social Science*, 2021, vol. 4.

25. *Brenner S. W.* Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford: Oxford University Press, 2009.

Сведения об авторах:
В. В. Баранов – кандидат юридических наук.
В. М. Пашин – доктор юридических наук.

Information about the authors:
V. V. Baranov – PhD in Law.
V. M. Pashin – Doctor of Law.

Статья поступила в редакцию 27.05.2024; одобрена после рецензирования 01.07.2024; принята к публикации 26.08.2024.

The article was submitted to the editorial office 27.05.2024; approved after reviewing 01.07.2024; accepted for publication 26.08.2024.