

## ОТЕЧЕСТВЕННЫЕ И ЗАРУБЕЖНЫЕ ПОДХОДЫ ПО РАЗРАБОТКЕ ПОНЯТИЙНОГО АППАРАТА В СФЕРЕ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ И ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ДАННОГО НОРМОТВОРЧЕСКОГО ПРОЦЕССА

**Петр Николаевич Кобец**

*Всероссийский научно-исследовательский институт МВД России, Москва, Россия  
pkobets37@rambler.ru, <https://orcid.org/0000-0001-6527-3788>*

**Аннотация.** В современных условиях законодательная база должна способствовать адекватному и своевременному реагированию на новейшие вызовы и угрозы, в том числе и кибертерроризму. В настоящее время, как в отечественной юридической науке, так и зарубежной, существует не столь уж большое количество исследований, посвященных понятийному аппарату в сфере кибертерроризма при том, что само возникновение терминологии связанной с кибертеррором относится еще к 1980-м годам. В настоящее время многими экспертами отмечается отсутствие четко сформулированного понятия рассматриваемого вида преступления, что в свою очередь обуславливает множество законодательных пробелов по борьбе с кибертерроризмом в ряде мировых держав. И это совершенно понятно, поскольку кибертерроризм стал досконально изучаться только в условиях начала нового тысячелетия. Сегодня существенное и тормозящее значение в сфере международного сотрудничества в сфере противодействия кибертерроризму, происходит из-за не в достаточной степени понимание рядом стран всей значимости рассматриваемых вопросов. Вследствие этого в некоторых государствах до настоящего времени не разработаны законодательные основы противодействия кибертерроризму. В этой связи, в настоящее время, исследование проблематики основных подходов законодательных основ в сфере кибертерроризма, как в нашей стране, так и за рубежом приобретает особую актуальность, как для юридической науки, так и правоприменительной практики. Обозначенные проблемные вопросы актуализируют важность и потребность проведения такого исследования, и последующего переосмысления, как зарубежного, так и отечественного понятийного аппарата, в сфере противодействия кибертерроризму, а также разработке предложений в сфере нормотворческой деятельности по борьбе с кибертеррором.

**Ключевые слова:** терроризм, кибертерроризм, информационная безопасность, информационное пространство, экспертные рекомендации, законодательные пробелы, международное сотрудничество, правовое регулирование, понятийный аппарат

**Для цитирования:** Кобец П. Н. Отечественные и зарубежные подходы по разработке понятийного аппарата в сфере борьбы с кибертерроризмом и предложения по совершенствованию данного нормотворческого процесса // Правопорядок: история, теория, практика. 2022. № 1 (32). С. 94–101.

Original article

## DOMESTIC AND FOREIGN APPROACHES TO THE DEVELOPMENT OF CONCEPTUAL APPARATUS IN THE FIELD OF COMBATING CYBERTERRORISM AND PROPOSALS FOR IMPROVING THIS NORMATIVE PROCESS

Peter N. Kobets

National Research Institute of the Ministry of Interior  
of the Russian Federation, Moscow, Russian Federation  
pkobets37@rambler.ru, <https://orcid.org/0000-0001-6527-3788>

**Abstract.** In modern conditions, the legal framework should facilitate an adequate and timely response to the latest challenges and threats, including cyber terrorism. Currently, both in domestic legal science and foreign, there is not so much research devoted to the conceptual apparatus in the field of cyber terrorism, despite the fact that the very emergence of terminology associated with cyber terrorism dates back to the 1980s years. Currently, many experts note the absence of a clearly formulated concept of the type of crime under consideration, which in turn leads to many legislative gaps in the fight against cyber terrorism in a number of world powers. And this is completely understandable, since cyber terrorism began to be thoroughly studied only at the beginning of the new millennium. Today, the significant and inhibiting importance in the field of international cooperation in the field of countering cyber terrorism is due to a lack of understanding by a number of countries of the full significance of the issues under consideration. As a result, some states have not yet developed a legislative framework for countering cyberterrorism. In this regard, at present, the study of the problems of the main approach of the legislative framework in the field of cyberterrorism, both in our country and abroad, becomes especially relevant, both for legal science and law enforcement practice. The identified problematic issues actualize the importance and need for such a study, and the subsequent rethinking of both foreign and domestic conceptual apparatus in the field of countering cyber terrorism, as well as the development of proposals in the field of norm-setting activities to combat cyber terrorism.

**Keywords:** terrorism, cyberterrorism, information security, information space, expert recommendations, legislative gaps, international cooperation, legal regulation, conceptual apparatus

**For citation:** Kobets P. N. Domestic and foreign approaches to the development of conceptual apparatus in the field of combating cyberterrorism and proposals for improving this normative process. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2022;(1):94-101. (In Russ.)

### Введение

В настоящее время терроризм признан одной из серьезнейших угроз глобальной мировой безопасности. Терроризм является одной из главных проблем современного мира, его предупреждение все больше становится важнейшей из сфер сотрудничества в международных отношениях в XXI столетия [6, с. 75]. Поэтому проблематика борьбы с терроризмом и соответственно с кибертерроризмом, широко исследуется многими отечественными и зарубежными специалистами.

Уже на протяжении нескольких лет различные террористические группы проявляют свою активность, технические и финансовые средства для проведения крупномасштабных операций в киберпространстве. Кибератаки террористов, которые

приводят к прерыванию работы различных государственных систем, в первую очередь направлены на то, чтобы произвести сильное впечатление на государство и общество, и способствовать дальнейшей радикализации отдельных слоев граждан, которая в последствии приводит к возросшим террористическим актам.

Существенная опасность кибертерроризма обуславливается, как масштабом его пагубного воздействия, так и ежегодно возрастающим количеством совершаемых рассматриваемых противоправных деяний. При этом важно подчеркнуть о том, что официальные статистические данные в силу высокой латентности киберпреступности, не могут отражать реальное положение дел в рассматриваемой сфере. В том числе, важнейшей

и основополагающей проблемой остается отсутствие специально закрепленного в международных правовых актах понятий, кибертерроризм, киберпреступности и ее основных признаков. По этой причине за последние 20 лет нового тысячелетия ряд государств разработали собственные подходы, регулирующие уголовную ответственность за киберпреступность. К примеру, уголовное законодательство некоторых стран, рассматриваемые преступления выделяет, как отдельные составы преступления, а других, как квалифицированные или специальные по отношению к общим составам преступлений. При этом, в рекомендациях экспертов ООН под киберпреступления подпадают любые противоправные действия, совершаемые при помощи компьютерных систем, либо сетей, в рамках компьютерных систем, либо сетей, против компьютерных систем [3, с. 24].

### **Материалы и методы**

В качестве объекта исследования выступили общественные отношения, которые складываются относительно правовой регламентации противоправных деяний в сфере кибертерроризма. Предметом исследования выступили международно-правовые акты, законодательство Российской Федерации и ряда иностранных государств, регулирующие отношения в сфере кибертерроризма, материалы экспертно-аналитических отчетов в области информационной безопасности, специальная литература и Интернет-ресурсы, освещающие различные проблемы противодействия кибертерроризму. В качестве цели исследования явилось изучение понятийного аппарата в сфере противодействия кибертерроризму и разработка обоснованных предложений по его совершенствованию. Методологическую основу данной работы составили, применяемые для проведения исследования общенаучные методы, в том числе формальной логики, анализа, синтеза и диалектический; частнонаучные методы, среди которых сравнительно-правовой, логико-юридический, анализа документов, системно-структурный.

### **Обсуждение проблемы**

В современной зарубежной юридической науке, как и среди отечественных правоведов прочно утвердилась теория, подтверждающая общественную опасность кибертеррора, которая доказывает, что современными достижениями в области науки и техники способствуют увеличению вероятности использования кибертехнологий в качестве основного средства при проведении актов кибертерроризма.

Кроме того, зарубежными экспертами убедительно доказано, что возрастающие изощренные акты кибертеррористов в дальнейшем могут приводить к реальным возможным нарушениям «нормального функционирования критически важных государственных объектов, среди которых ядерные реакторы, биологические и химические лаборатории и др., что в итоге приведет к неисчислимому количеству жертв среди мирного населения» [15, р. 307].

В одной из фундаментальных работ «Cyber warfare and cyber terrorism» зарубежных исследователей кибертерроризма Леха Янчевского, доцента факультета информационных наук и управления операциями университета Окленда, имеющего более чем тридцатипятилетний опыт работы в области информационных технологий и доктора философии в области информационных систем Эндрю М. Коларика, председателя Новозеландского форума по информационной безопасности, члена Новозеландского компьютерного общества и секретаря Технического комитета IFIPs по безопасности и защите в системах обработки информации (ТК-11) имеющего более чем двадцатипятилетний опыт использования компьютерных информационных систем, рассматривается кибертерроризм и связанные с ним проблемы. В указанной работе коллектив авторов подробно обсудил основные целевые объекты кибертеррористов, особенности их внешнего проникновения, отправные точки при планировании и для подготовки к кибератакам, а также проблемные вопросы совершенствования систем безопасности по противодействию кибертерроризма. Кроме того, авторами даны рекомендации о том, как бороться с кибератаками и сделан обзор основных определений кибертерроризма, в результате которых им дается собственное определение рассматриваемого феномена. Под кибертерроризмом ими понимаются политически мотивированные атаки, которые совершают субнациональные группы, либо тайные агенты, или же определенные индивиды в отношении телекоммуникационных информационных систем, компьютерных информационных данных и программ, в результате чего подвергаются насилию некомбатанты [13, р. 14].

Авторское определение кибертерроризма сделанное Лехой Янчевским и Эндрю М. Колариком отличается от ряда других дефиниций, поскольку в нем содержатся два ключевых компонента, которые помогают отграничить проявления кибертерроризма от иных противоправных форм и видов киберпреступности, а именно: обязательным наличием

доказанной мотивации, имеющей политическую основу и желанием, связанным с осуществлением насильственных действий в отношении нонкомбатантов.

Анализ «Словаря терроризма» — одной из крупнейших зарубежных справочных работ в области териологии (новое научное направление, исследующее терроризм с точки зрения особого социального феномена, его сущность, тенденции, формы, цели причины, отдельные проявления и др.) которая определяет и описывает большинство аспектов терроризма, освещает такие вопросы, как деятельность террористических организаций, виды терроризма, меры по борьбе с терроризмом, историю терроризма и др., в том числе содержит множество определений с использованием примеров со всего мира [16, р. 61]. Это издание автора Такры Джона Ричарда — широко известного исследователя в области противодействия терроризма, в частности по работе, подготовленной им в 1980-х гг. под названием «Энциклопедия терроризма и политического насилия» [14, р. 92], определяет кибертерроризм, как вид преступного посягательства, к которому с каждым годом все чаще будут прибегать кибертеррористы. Также автором делается акцент на то, что мотивация для совершения актов террора имеет политический характер.

Мириам Данн Кавелти — заместитель по исследованиям и преподаванию Цюрихского Центра исследований в области безопасности (CSS), в настоящее время работающая над проектом, анализирующим политику угроз в киберпространстве, в одной из своих работ по кибертерроризму «Кибервойна: концепция, статус-кво и ограничения», определяет кибертерроризм, в качестве незаконного нападения, осуществляемого негосударственными субъектами на компьютеры, сети и информацию, содержащуюся в них, для запугивания правительств, либо населения, в целях достижения определенных задач<sup>1</sup>. Мириам Данн Кавелти, полагает, что кибератаку следует квалифицировать, как акт кибертерроризма, если ее последствия спровоцировали физическое насилие в отношении граждан или собственности, а также способствовали появлению страха относительно возможности осуществления указанных последствий.

Необходимо отметить, что в последнее десятилетие кибер-инциденты, связанные

<sup>1</sup> См.: Myriam Dunn Cavelti. Cyberwar: concept, status quo, and limitations [Electronic resource] / Center for Security Studies (CSS), ETH Zurich. Access mode: URL: www.sta.ethz.ch (дата обращения: 15.12.2021).

с кибератаками террористов, стали более дорогостоящими, более разрушительными и во многих случаях более политическими, параллельно с этим появляется новый массив теоретически обоснованных исследований. Так, в частности, по мнению американского исследователя, кибертерроризма К. Уилсона под кибертерроризмом следует понимать «использование компьютерной техники в качестве оружия международными или национальными группами, или тайными агентами, которые политически мотивированы и могут нанести, либо угрожают нанесением ущерба, в целях влияния на население или правительства для решения политических вопросов»<sup>2</sup>.

Также, нельзя не сказать о том, что зарубежные исследователи рассматриваемого вида террористической угрозы, описывая понятие кибертерроризма и его различных проявлений, часто акцентируют внимание на идеологических, пропагандистских и абстрактно-теоретических особенностях его составляющих. Решая данную проблему Верховным судом США были даны разъяснения по всем из перечисленных выше терминов, и кроме того в принятом в 2001 г. «Закоме о патриотизме США 2001» — USA Patriot Act of 2001, который был принят после террористических актов в Нью-Йорке и Вашингтоне, 11 сентября 2001 г., содержится трактовка раскрывающая понятие кибертерроризма<sup>3</sup>.

В Российской Федерации дефиниция «кибертерроризм» в настоящее время не получила легального закрепления несмотря на то, что относительно ее содержания многие годы не утихают споры между юристами, теоретиками, практиками, а также всеми остальными специалистами, исследующими вопросы борьбы с кибертерроризмом. По мнению ряда отечественных экспертов, «признавать актами кибертерроризма необходимо лишь такие действия, когда их разрушительный характер можно связать напрямую с использованием программного обеспечения и компьютерных технологий» [9, с. 81]. Сегодня отдельные отечественные исследователи предлагают считать кибертерроризм «составной частью информационного терроризма» [7, с. 183], при этом «ряд специалистов об информационном

<sup>2</sup> См.: Clay W. Computer Attack and Cyberterrorism (Vulnerabilities and Policy Issues for Congress) [Electronic resource] / Federation of American Scientists. URL: <http://www.fas.org/sgp/crs/terror/index.htm> (дата обращения: 15.12.2021).

<sup>3</sup> См.: USA Patriot Act of 2001 URL: <https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf> (дата обращения: 15.12.2021).

терроризме рассуждают, как об одном из видов проявлений терроризма» [8, с. 123]. Однако многие специалисты рассматривают кибертерроризм, как отдельный вид преступного деяния, при этом указывая на то, что проявления кибертерроризма необходимо квалифицировать, как применение информационных телекоммуникационных систем для осуществления актов терроризма [2, с. 542].

При всем многообразии подходов к анализируемой проблематике, следует отметить, что большинство представителей отечественной юридической науки обладают сходными позициями по рассматриваемой проблеме, и под проявлениями «кибертерроризма» понимают действия, выражающиеся в преднамеренных, политически мотивированных атаках на информационные данные, обрабатываемые компьютерной системой, представляющие повышенную опасность для жизни и здоровья людей, либо связанные с наступлением иного тяжкого последствия, если данные деяния были совершены в целях нарушения общественной безопасности, запугивания общественности, либо для провокации военных конфликтов» [11, с. 8]. При этом важно подчеркнуть, что о том, что не всех ученых устраивает подобное видение кибертерроризма, некоторые из исследователей обладают собственной точкой зрения на данную проблему и полагают, что под данным явлением следует рассматривать совокупность противоправных деяний, которые могут быть связаны с угрозами безопасности, личности, общества и государства, деятельностью в отношении материальных объектов, искажением объективной информации, для получения преимущества в целях решения различных задачи, при помощи использования разнообразных средств в сфере программного обеспечения в киберпространстве [1, с. 53].

Кроме того, некоторые специалисты под кибертерроризмом понимают оказание воздействия на компьютерные системы, программы, сети, а также информацию, которая обрабатывается ими в киберпространстве, в целях подготовки или проведения актов кибертерроризма [4, с. 19]. Отдельным специалистам «кибертерроризм представляется комплексной акцией, выражающейся в преднамеренной политической атаке на информационное пространство, обрабатываемое при помощи компьютеров и компьютерных систем» [12, с. 105].

Необходимо отметить, что рядом отечественных исследователей, оперирующих дефиницией кибертерроризма, как правило подразумевается совершением исключительно

террористических атак только отдельными кибертеррористами или группами [5, с. 11]. По мнению автора, такое понимание кибертерроризма с методологических позиций не может быть верным. При этом важно отметить, что основные реальные угрозы объектам критически важной инфраструктуре ведущих зарубежных держав, наносили не только отдельные террористические группы, а в том числе и специально подготовленные информационно и материально обеспеченные специализированные организации [10, с. 77].

### **Пути решения проблемы**

Анализируя вышесказанное важно подчеркнуть, что вне всякого сомнения, угрозы, связанные с кибертерроризмом будут только нарастать и усиливаться, как и развитие самих информтехнологий. А поскольку кибертерроризм несет в себе вред не только обществу и гражданам отдельных государств, а в том числе и всему мировому сообществу, все большее значение начинают приобретать вопросы эффективного международного сотрудничества в сфере борьбы с кибертерроризмом. При этом нельзя не отметить, что ряд стран накопили большой положительный опыт и значительно продвинулись в рассматриваемой сфере. Их совместные усилия могли бы способствовать обеспечению достижения глобальной международной безопасности. Однако, немаловажное значение для оптимизации осуществления международного сотрудничества по противодействию кибертерроризму должно отводиться обязательному участию в этой деятельности всего мирового сообщества, так как рассматриваемое явление носит транснациональный характер. В этой связи понятие кибертерроризма должно быть закреплено международным законодательством. Поскольку крайне сложно противодействовать кибертерроризму силами одного государства, важно консолидировать усилия не только на национальных, но и на межгосударственных уровнях, посредством разработки и внедрения межгосударственных правил поведения в киберпространстве. Возможно даже создать наднациональные институты, регулирующие киберпространство и глобальную сеть Интернет, предварительно изучив и проработав вопросы правового регулирования борьбы с кибертерроризмом на международном уровне.

В конечном счете, эту проблему нельзя рассматривать исключительно на уровне одной страны и на основе упрощенных терминов. Киберпространство 2020-х гг. это

динамичная и сложная экосистема связей, и таким же должно быть и правовое регулирование по осуществлению ее безопасности. Совместная международная правотворческая работа в сфере борьбы с кибертерроризмом требует доверительных отношений между правительствами зарубежных стран, чтобы создать многополярную сеть сотрудничества между всеми сторонами, а не просто набор двумерных связей. Это позволит обеспечить более широкий спектр правовых оснований в сфере противодействия угрозам международному кибертерроризму и станет важной вехой достижения взаимовыгодного международного сотрудничества.

Также в дальнейшем необходимо продолжать развивать международный диалог по рассматриваемой проблеме на различных форумах в рамках международного сотрудничества в борьбе с кибертерроризмом. Только в этом случае международному сообществу удастся проработать вопрос о создании системы по координации и взаимодействию всех служб, отвечающих за борьбу с кибертерроризмом, как на внутригосударственном, так и международном уровнях. Только реализация указанных положений сможет в полной мере способствовать успешному и эффективному международному сотрудничеству в сфере борьбы с кибертерроризмом.

Так, например, в информационном пространстве террористические преступления могут совершаться, как отдельными лицами, так и организованными террористическими преступными группами, и сообществами. Поэтому в отношении организованной террористической киберпреступности могут быть применены международные договоры, направленные на противодействие в целом организованных преступных групп, в том числе положения Конвенции ООН против транснациональной организованной преступности 2000 г.<sup>1</sup> Однако при этом было бы логично разграничить деятельность организованных террористических преступных групп

---

<sup>1</sup> См.: Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН) (с изм. от 15.11.2000) URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_121543/](http://www.consultant.ru/document/cons_doc_LAW_121543/) (дата обращения: 15.12.2021).

и сообществ, которые совершают киберпреступления, и тех, которые проявляют себя в иной сфере преступных посягательств, при этом использующих телекоммуникационные сети.

Таким образом, в настоящее время правовое регулирование противодействия кибертерроризму требует своего дальнейшего совершенствования, для обеспечения полной информационной безопасности государственных структур и общества. Помимо законодательного определения самого явления кибертерроризма, также необходимо совершенствовать ряд законодательных актов, а также отдельных правовых норм, чтобы эффективно противодействовать кибертерроризму, поскольку пока что данный процесс нельзя признать в достаточной степени совершенным. Кроме того, возможные масштабы причинения вреда кибертеррористами и санкции за совершенные ими противоправные деяния должны быть соизмеримы и соответствовать друг другу.

### **Заключение**

Завершая рассмотрение проблематики понятийному аппарату в сфере кибертерроризма, которая основана на исследовании точек зрения отечественных и зарубежных ученых, в том числе и по вопросам содержательной части дефиниции кибертерроризма, необходимо отметить, что как в нашей стране, так и зарубежом, законодательное закрепление понятия кибертерроризма на сегодняшний день осуществили не во всех странах, и это не смотря на то, что кибертерроризм на сегодняшний день представляет из себя, пожалуй, самую значимую и глобальную проблему современности. Также, важно отметить, что несмотря на то, что в мире кибертерроризм с каждым годом продолжает «набирать обороты», до сих пор отсутствует определяющее его единое общепринятое понятие. В дальнейшем необходимо стремиться к тому, чтобы межгосударственное взаимодействие по противодействию кибертерроризму выстраивалось с учетом необходимых правовых основ. Роль в координации данной деятельности необходимо предоставить ООН, и в ее рамках также следует принять специальные резолюции по различным аспектам борьбы с кибертеррором.

### **Список литературы**

1. Асеев С. Ю., Воронцов В. А. Проблема определения кибертерроризма // Общество и цивилизация. 2016. Т. 2. С. 49–53.

2. Белоножкин В. И. Информационная сущность и структура терроризма // *Информация и безопасность*. 2007. Т. 10, № 4. С. 541–546.
3. Дашян М. Обзор Конвенции Совета Европы и киберпреступности // *Современное право*. 2002. № 11. С. 20–24.
4. Диденко А. И. Понятие и место кибертерроризма в уголовном праве России // *Отечественная юриспруденция*. 2016. № 9 (11). С. 17–21.
5. Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // *Информационное право*. 2013. № 5. С. 10–13.
6. Кобец П. Н. Генезис опасной разновидности террористической угрозы — биологического терроризма и меры по его профилактике // *Правопорядок: история, теория, практика*. 2021. № 1 (28). С. 72–78.
7. Ковлагина Д. А. Информационный терроризм // *Вестник Саратовской государственной юридической академии*. 2013. № 6 (95). С. 181–184.
8. Лопатина Т. М. Новые виды современной террористической деятельности // *Современное право*. 2012. № 4. С. 122–126.
9. Маслакова Е. А. Кибертерроризм как новая форма терроризма // *Наука и практика*. 2015. № 2 (63). С. 79–81.
10. Соколов А. С., Поволоцкий А. Ю. Кибертерроризм в России и странах Центральной Азии // *Российско-азиатский правовой журнал*. 2020. № 2. С. 75–79. DOI: 10.14258/ralj(2020)2.10
11. Услинский Ф. А. Кибертерроризм в России: его свойства и особенности // *Право и кибербезопасность*. 2014. № 1. С. 6–11.
12. Федулов В. И. Компьютерный терроризм как инновация современного высокотехнологического общества // *Вестник Московского государственного областного университета. Серия: Юриспруденция*. 2007. № 1-2. С. 103–107.
13. *Cyber warfare and cyber terrorism* / L. J. Janczewski, A. M. Colarik, Hershey; New York: Information science reference, cop. 2008. 532 с.
14. *Encyclopedia of terrorism and political violence* / J. R. Thackrah. London; New York: Routledge & Kegan Paul, 1987. 308 p.
15. Solodov A., Williams A., Hanaei S. A., Goddard B. Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities. *Security Journal*. 2018. Vol. 31. Iss. 1. pp. 305–324.
16. Thackrah J. R. *Dictionary of terrorism*. 2 ed. London; New York: Routledge. 2004. 318 p.

## References

1. Aseev SYu, Vorontsov VA. The problem of defining cyberterrorism. *Obshchestvo i civilizaciya* [Society and civilization]. 2016;2:49-53. (In Russ.)
2. Belonozhkin VI. Informational essence and structure of terrorism. *Informaciya i bezopasnost'* [Information and security]. 2007;10(4):541-546. (In Russ.)
3. Dashyan M. Review of the Convention of the Council of Europe and Cybercrime. *Sovremennoe pravo* [Modern Law]. 2002;(11):20-24. (In Russ.)
4. Didenko AI. The concept and place of cyberterrorism in the criminal law of Russia. *Otechestvennaya yurisprudenciya* [Domestic jurisprudence]. 2016;(9):17-21. (In Russ.)
5. Efremova MA. Criminal and legal support kiberbezopasnost-STI: some problems and solutions. *Informacionnoe pravo* [Information law]. 2013;(5):10-13. (In Russ.)
6. Kobets PN. Genesis threat varieties of the terrorist threat — biological terrorism and measures for its prevention. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2021;(1):72-78. (In Russ.)
7. Kovlagina DA. Informational terrorism. *Vestnik Saratovskoj gosudarstvennoj yuridicheskoy akademii* [Bulletin of the Saratov State Law Academy]. 2013;(6):181-184. (In Russ.)
8. Lopatina TM. New types of modern terrorist activity. *Sovremennoe pravo* [Modern Law]. 2012;(4):122-126. (In Russ.)
9. Maslakova EA. Cyberterrorism as a new form of terrorism. *Nauka i praktika* [Science and Practice]. 2015;(2):79-81. (In Russ.)
10. Sokolov AS. Povolotskaya AY. Cyber terrorism in Russia and Central Asia countries. *Rossijsko-aziatskij pravovoj zhurnal* [Russian-Asian legal journal]. 2020;(2):75-79. DOI: 10.14258/ralj(2020)2.10 (In Russ.)
11. Ulinski FA. Cyberterrorism in Russia: its properties and peculiarities. *Pravo i kiberbezopasnost'* [Law and cybersecurity]. 2014;(1):6-11. (In Russ.)

12. Fedulov VI. Computer terrorism as an innovation of modern high-tech society. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Yurisprudenciya* [Bulletin of the Moscow State Regional University. Series: Jurisprudence]. 2007;(1-2):103-107. (In Russ.)
13. Janczewski LJ, Colarik AM. *Cyber warfare and cyber terrorism*. Hershey; New York: Information science reference; cop. 2008.
14. Thackrah JR. *Encyclopedia of terrorism and political violence*. London; New York: Routledge & Kegan Paul; 1987.
15. Solodov A, Williams A, Hanaei SA, Goddard B. Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities. *Security Journal*. 2018;31(1):305-324.
16. Thackrah JR. *Dictionary of terrorism*. 2 ed. London; New York: Routledge; 2004.

Дата поступления статьи / Received: 15.12.2021.  
Дата рецензирования статьи / Revised: 14.01.2022.  
Дата принятия статьи к публикации / Accepted: 09.03.2022.

---