УДК 130.2:172.1

DOI: 10.26456/vtphilos/2023.3.078

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ВИДОВ КИБЕРТЕРРОРИЗМА КАК ГИБРИДНОЙ УГРОЗЫ НА УСТОЙЧИВОСТЬ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.А. Ковалев

ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Санкт-Петербург

Актуальность данного исследования заключается в том, что современный кибертерроризм ставит своей целью воздействие на все сферы активности не только государства, но и общества, формирующего его, на их политическое пространство, экономическую деятельность и социальные институты. Следовательно, уже необходимо говорить о кибертерроризме как о феномене гибридной угрозы для национальной безопасности современного государства, исследовать не только методы и механизмы электронного терроризма, но и те области, которые он начинает охватывать, формируя виды технологического и информационного воздействия. Предметом данного исследования стало влияние видов информационного воздействия кибертерроризма на устойчивость национальной безопасности. Объектом исследования были особенности влияния различных видов информационного воздействия кибертерроризма на устойчивость национальной безопасности. Целью исследования было определение степени влияния политических, экономических и социальных угроз на устойчивость национальной безопасности. Для достижения цели исследования и решения поставленных задач были использованы логический метод анализа для структурирования материалов, исторический метод для корректного и хронологически последовательного изложения фактов, сравнительный метод с целью выявления отличительных параметров в сравниваемых суждениях и дедуктивный метод для определения выводов по результатам исследования. Научная новизна заключается в исследовании влияния политических, экономических и социальных угроз на устойчивость национальной безопасности. В ходе исследования было дано современное понятие кибертерроризма, исходя из понимания сущности национальной безопасности, и определение гибридной угрозе в контексте наличия феномена кибертерроризма, выделены две группы видов влияния кибертерроризма на устойчивость национальной безопасности – технологическая и информационная, определены виды информационного воздействия кибертерроризма, которые имеют наиболее эффективное влияние на устойчивость национальной безопасности, и проанализированы особенности влияния видов информационного воздействия кибертерроризма на устойчивость национальной безопасности.

Ключевые слова: *национальная безопасность, кибертерроризм, гибридные угрозы, электронное пространство.*

Введение

В современном социально-политическом аспекте формирования и развития общества кибертерроризм является неотъемлемой угрозой, которая порождена такими явлениями, как глобализация, автоматизация и цифровизация. Современное общество стремится к совершенствованию всех систем, которые регулируют ее активность. Результатом этого процесса стало возникновение компьютерных систем и далее электронного пространства – Интернета. С появлением большого количества информации стала развиваться система серверов – хранилищ информации в цифровом виде. Цифровизация породила не только специалистов, которые трудятся на благо общества, но и тех, которые начали формировать нелегитимные идеи воздействия на электронную среду в криминальных целях. В результате, появились такие формы, как кибермошенничество и киберпреступность, которые в дальнейшем переросли в кибертерроризм.

Актуальность данного исследования заключается в том, что современный кибертерроризм ставит своей целью воздействие на все сферы активности не только государства, но и общества, формирующего его, на их политическое пространство, экономическую деятельность и социальные институты. Следовательно, необходимо говорить о кибертерроризме как о феномене гибридной угрозы для национальной безопасности современного государства, исследовать не только методы и механизмы электронного терроризма, но и те области, которые он начинает охватывать, формируя виды технологического и информационного воздействия.

Предметом данного исследования стало влияния видов информационного воздействия кибертерроризма на устойчивость национальной безопасности.

Объектом исследования были особенности влияния различных видов информационного воздействия кибертерроризма на устойчивость национальной безопасности.

Целью исследования было определение степени влияния политических, экономических и социальных угроз на устойчивость национальной безопасности.

Исходя из цели исследования, были поставлены следующие задачи:

- дать современное определение понятию «кибертерроризм», исходя из понимания сущности национальной безопасности;
- дать определение «гибридной угрозе» в контексте наличия феномена кибертерроризма;
- выделить виды информационного воздействия кибертерроризма, которые имеют наиболее эффективное влияние на устойчивость национальной безопасности;

– проанализировать особенности влияния видов информационного воздействия кибертерроризма на устойчивость национальной безопасности;
– сделать выводы по актуальности развития механизмов национальной безопасности с учетом развития кибертерроризма.

Для достижения цели исследования и решения поставленных задач были использованы логический метод анализа для структурирования материалов, исторический метод для корректного и хронологически последовательного изложения фактов, сравнительный метод с целью выявления отличительных параметров в сравниваемых суждениях и дедуктивный метод для определения выводов по результатам исследования.

Научная новизна исследования заключается в исследовании влияния политических, экономических и социальных угроз на устойчивость национальной безопасности.

В ходе исследования были использованы материалы научных трудов отечественных и зарубежных исследователей в области философской антропологии, социологии и политологии, в том числе работы О.В. Алексеенко, Н.В. Гайдук, Н.В. Левченко, Д.В. Пучкова, С. Бреннер (S.W. Brenner), Г. Ласвелла (H.D. Lasswell), П. Палери (P. Paleri).

Материалы исследования

Считается, что кибертерроризм – это использование Интернета для совершения насильственных действий, которые приводят к гибели людей или причинению значительного телесного повреждения, с целью достижения политических или идеологических выгод путем угроз или запугивания [3]. Акты преднамеренного крупномасштабного нарушения работы компьютерных сетей, особенно персональных компьютеров, подключенных к Интернету, с помощью таких инструментов, как компьютерные вирусы и черви, фишинг, вредоносное программное обеспечение, аппаратные методы, программные скрипты – все это можно назвать формами интернет-терроризма [9, с. 15–16].

Необходимо отметить, что кибертерроризм является достаточно противоречивым термином. Некоторые авторы выбирают очень узкое определение, акцентируя внимание на развертывании террористическими организациями атак с целью нарушения работы информационных систем, чтобы, в основном, создать психологическую панику без какого-либо физического воздействия. Термин вовсю используется многими СМИ и производителями средств информационной безопасности, желающими увеличить продажи своих продуктов, что, естественно, порождает обратную реакцию потребителя – недоверие к теме, которая излишне давит на сознание человека и формирует у него устойчивую негативную реакцию.

Другие авторы предпочитают более широкое определение, которое включает понятие «киберпреступность». Участие в кибератаке влияет на

восприятие террористической угрозы, даже если это не связано с применением насилия. По некоторым определениям может быть трудно идентифицировать виды онлайн-активности, которые необходимо относить к кибертерроризму или киберпреступности [9, с. 43–м44].

Кибертерроризм также можно определить как преднамеренное использование компьютеров, сетей и общедоступного Интернета для причинения разрушений и вреда в личных целях. Опытные кибертеррористы, которые очень искусны в плане взлома, могут нанести огромный ущерб правительственным системам и коммерческим структурам, что может послужить уходу определенных организаций из страны с целью минимизации риска продолжения таких атак [10, с. 52–53; 3]. Следовательно, данные персоналии принимают участие в макроэкономической и политической войне за определенные сферы влияния, что также можно рассматривать как форму терроризма.

Общественный интерес к кибертерроризму возник в конце 1990-х гг., когда этот термин был введен старшим научным сотрудником Калифорнийского института безопасности и разведки Барри К. Коллином. Громкие террористические атаки в Соединенных Штатах Америки 11 сентября 2001 года и последовавшая за ними война с терроризмом со стороны США привели в последующие годы к широкому освещению в средствах массовой информации потенциальных угроз кибертерроризма [5]. В основных средствах массовой информации часто обсуждается возможность масштабной атаки с использованием компьютерных сетей для саботажа критически важных инфраструктур с целью подвергнуть опасности человеческие жизни или вызвать сбои в национальном масштабе либо напрямую, либо путем подрыва национальной экономики.

Такие авторы, как Уинн Шварцау (Winn Schwartau) и Джон Аркилла (John Arquilla), добились значительного финансового успеха, продавая книги, в которых описывались якобы правдоподобные сценарии хаоса, вызванного кибертерроризмом. Многие критики утверждают, что эти книги были нереалистичны в своих оценках того, были ли возможны описанные атаки, например ядерные катастрофы и взрывы на химических заводах. Общей чертой всего того, что критики воспринимают как шумиху вокруг кибертерроризма, является отсутствие фальсификации, т. е., когда предсказанные катастрофы не происходят, это только показывает, насколько нам до сих пор везло, а не ставит под сомнение теорию [2]. В принципе, такие аналитические работы могут считаться некоей формой пособничества кибертерроризму, т. к. предлагают не только объяснение актуальности угроз, но и фактическое руководство по созданию такой угрозы.

Хотя в 2016 г. Министерство юстиции США впервые предъявило обвинение в кибертерроризме Ардиту Феризи за взлом военного веб-сайта и кражу персональных данных правительственных и военных сотрудников, а

также их продажу ИГИЛ, за последующие 6 лет стало очевидным, что контроль за кибермошеничеством и терроризмом не улучшается из-за «гонки интеллекта» между хакерами и контролирующими организациями.

С другой стороны, также утверждается, что, несмотря на значительные исследования по кибертерроризму, объем литературы по-прежнему не позволяет дать реалистичную оценку реальной угрозы. Например, в случае кибертеррористической атаки на общественную инфраструктуру, такую как электростанция или управление воздушным движением, существует неопределенность относительно ее успеха, поскольку данные, касающиеся таких явлений, ограничены [14, с. 354].

Гибридные угрозы – это объединение дипломатических, военных, экономических и информационно-коммуникационных методов воздействия, которые могут быть использованы в вооруженном конфликте государственными или негосударственными субъектами для достижения особых целей, не доходя при этом до формального объявления войны. В современном контексте реализации гибридной войны необходимо более широкое и форматное определение: гибридная угроза – это использование различных эффективных методов технологического и информационного воздействия на человека для достижения преимущества в ведении необъявленных форм противостояния между государствами или социально-политическими системами. В категорию эффективных методов технологического воздействия необходимо отнести разработку и внедрение вредоносного программного продукта, ведущего к нанесению различного рода урона юридическим или физическим лицам, в том числе кражи персональных данных физических лиц и информации, содержащей коммерческую тайну юридического лица, физического вывода из строя оборудования, обесточивания электроэнергией, отключения от сети Интернет.

Однако особой категорией эффективных методов является информационное воздействие, т. к. оно крайне тяжело определяемо, имеет большую возможность распространения и направленно на психику человека. В данную категорию необходимо отнести политическое, социальное и экономическое [5]. Именно информационное воздействие является наиболее опасным и уязвимым для национальной безопасности и национальной идентичности.

Как было отмечено выше, к эффективным видам информационного воздействия кибертерроризма необходимо отнести политическое, социальное и экономическое воздействие, т. к. на современном этапе развития цивилизации они уже находятся в плоскости цифровизации и виртуализации. Например, многие персональные данные граждан Российской Федерации уже внесены в Единый портал государственных и муниципальных услуг (функций) «Госуслуги», который ставит своей целью облегчить жизнь россиян. Подобные системы уже давно созданы и функционируют в развитых странах мира, например в США, Канаде, Японии, Израиле, ФРГ. Экономи-

ческая деятельность человека в основном не так сконцентрирована и автоматизирована ввиду того, что часть физических и юридических лиц пользуются различными финансовыми организациями одновременно. Тем не менее каждая такая финансовая организация размещает персональные данные своих клиентов на сервере или серверах, т. е. в цифровой форме, что также является виртуальным пространством.

Следовательно, социально значимая и финансово значимая информация физических и юридических лиц отдельного государства все больше автоматизируется, переносится в цифровую форму и размещается на носителях, подключенных к сети Интернет. С одной стороны, это облегчает работу государства и финансовых институтов по контролю за всеми манипуляциями лиц и в то же время предоставляет гражданам современные возможности по быстрому доступу к информации и услугам. С другой стороны, цифровизация и виртуализация персональных данных и активности физических и юридических лиц становится реальной мишенью для кибермошенников, киберпреступников и кибертеррористов.

Необходимо отметить, что при информационном воздействии в киберпространстве, или цифровой среде, различия между мошенничеством, преступностью и терроризмом во многом сглаживаются, нивелируются. Принято считать, что кибермошенничество, или электронное мошенничество, – это вид мошенничества с использованием виртуального пространства, которое может включать в себя скрытие информации или предоставление неверной информации, чтобы отнять у жертв финансовые средства, физическое имущество или наследство [12, с. 47]. В отличие от преступности в этом случае жертва условно добровольно и сознательно предоставляет преступнику информацию, деньги или имущество [7, с. 121]. Бонни Фишер и Стивен Лэб также дополняют, что в кибермошеничестве участвуют криминальные лица, разделенные во времени и пространстве [8, с. 493]. Однако понятие «добровольность», указанное у Сьюзан Бреннер, является условным, т. к. лицо вводится в заблуждение информационной атакой, некорректными адресами и психологическим давлением. Можно утверждать, что лицо принуждается к действию нелегитимными методами. Следовательно, мошенничество становится крайне близким к преступности. Ведь киберпреступность – это вид преступления, в котором задействован компьютер или компьютерная сеть [12, с. 10] и которое может нанести ущерб чьей-либо безопасности или финансам. Из этого следует, что кибермошенничество и киберпреступность, имея в своей основе компьютерную среду, или электронную среду, направлены на нелегитимное воздействие на человека или его окружающую среду, в том числе и технологическую, с целью получения своей выгоды из наличия информации или средств у него.

На современном этапе развития технологий становится очевидным, что методы и инструменты кибермошенничества и киберпреступности используются и в кибертерроризме [6]. Фактически уже сложно различить эти три вида криминалистического воздействия на человека или организацию.

Поэтому в 2022–2023 гг. встречается все больше дел в правовом поле Российской Федерации и иных развитых государств мира, которые из первичного электронного мошенничества переходят в итоге в категорию электронной преступности, и в то же время первичные обвинения в электронной преступности начинают в ходе дела переквалифицироваться в категорию электронного терроризма, т. е. кибертерроризма.

Следовательно, кибертерроризм расширяет свои границы как по своей сути, так и по значимости для физических и юридических лиц государства [1]. Деятельность кибертерроризма ведет к дестабилизации общества, слагающего данное государство. Кибертеррористическая деятельность развивается в различных направлениях, указанных выше, – политической, экономической и социальной, что неизбежно приводит к нарушению устойчивости национальной безопасности [4].

Национальная безопасность как обороноспособность суверенного государства, включая его граждан, экономику и институты, выполняет функцию недопущения военной эскалации внутри страны и за ее пределами [13, с. 3–4]. Гарольд Дуайт Ласвелл отмечал, что «отличительный смысл национальной безопасности означает свободу от иностранного диктата» [11, с. 14], а Арнольд Оскар Вулферс с коллегами расширил это понятие, дав определение, что «национальная безопасность объективно означает отсутствие угроз приобретенным ценностям, а субъективно – отсутствие страха, что такие ценности подвергнутся нападению» [15, с. 27]. Следовательно, применяя более современное понятие национальной безопасности, выраженное группой Арнольда Вулферса, можно соотнести угрозы кибертерроризма и его более легких форм с устойчивостью национальной безопасности через механизмы предупреждения и предотвращения электронных угроз, которые потенциально или фактически способны нанести политический, экономический или социальный урон физическим и юридическим представителям данного государства, а также государственным структурам и лицам, поддерживающим их работу.

Политический урон является самым значимым для государства. Слабость национальной безопасности перед киберпреступностью и кибертерроризмом влечет за собой снижение политического имиджа государства вплоть до его потери в глазах государств-союзников. В свою очередь, политическая имиджевая составляющая национальной безопасности используется и врагами государства для усиления кибернетического воздействия с целью нанесения полномасштабного экономического урона противнику. Следовательно, сохранение устойчивости национальной безопасности в электронном пространстве государства, как в его управленческих структурах, так и в территориальном понимании, является важным аспектом политической стабильности.

Экономический урон также является значимым для государства. Низкий уровень национальной безопасности ведет к ослаблению системы контроля за финансовыми структурами государства, в основном банками,

что, в свою очередь, повышает риски эффективного воздействия на их электронную среду со стороны кибертеррористов. Это приобретает особой смысл в период жесткого политического давления на отдельное государство, когда интересы государств-агрессоров совпадают с интересами кибермошенников и киберпреступников, которые реабилитируются и «принимаются на работу» с целью якобы стороннего, независимого от государств-агрессоров нападения на финансовые структуры как самого государства, так и лиц внутри него. Причем экономический кибертерроризм нацеливает свою деятельность не только на юридические лица финансового сектора, например банки с государственным управлением или сугубо коммерческие негосударственные банки, но и на физические лица, повышая уровень тревожности электората политических элит, а в некоторых случаях добиваясь некоторых форм радикализма в их действия в отношении беспомощности государственного аппарата предотвратить угрозы, что, в свою очередь, ведет к реализации внутренних социальных угроз.

Социальный урон необходимо также считать значимым для устойчивости национальной безопасности. Кибертерроризм может быть направлен на само общество государства, которое причислено к врагам. Причем в этом случае тесная связь кибертеррористов с каким-либо государством может и не прослеживаться, т. к. преступники могут проявлять активность по своим социальным и политическим убеждениям. Это еще более усложняет реализацию методов и механизмов национальной безопасности, т. к. государство не может точно и гарантированно идентифицировать террориста с учетом того, что преступление совершается в электронной среде, в которой понятие границ и территории крайне размыто. Целями кибертеррористов становятся государственные порталы, на которых аккумулируется персональная информация граждан общества и юридических лиц, зарегистрированных в правовом поле данного государства. Необходимо отметить, что персональные данные и активность лиц постоянно обновляется на таких порталах, что требует высочайшего уровня защиты от DDOS-атак и внедрения вирусных программ копирования или удаления данных с серверов. Для физических и юридических лиц государства важным является не столько факт «обрушения» серверов, на которых хранится актуализированная информация про них, сколько гарантии невозможности копирования данных во внешние ресурсы. В противном случае данные лица становятся прямой мишенью для кибертеррористов и киберпреступников, минуя государственные и муниципальные порталы. Это неизбежно приведет к социальному возмущению, его росту и трансформации в открытое противостояние правящим элитам в лице государственного аппарата. Следовательно, национальная безопасность должна распространяться и на социальную сферу электронной активности граждан, т. е. разрабатывать механизмы постоянного развития систем предупреждения и защиты граждан и организаций от потери их данных на государственных и муниципальных порталах.

Влияние видов информационного воздействия кибертерроризма на устойчивость национальной безопасности крайне велико. Политическое, экономическое и социальное воздействие по отдельности способны нарушить стабильность государства. Если же методами кибертерроризма становятся два или все три вида воздействия, то государство имеет большой шанс потерять свою независимость или же прекратить свое существование. Поэтому система национальной безопасности должна быть устойчивой ко всем видам информационных угроз как технологически, так и методологически с целью предупреждения, профилактики и предотвращения кибернетического воздействия на государственные структуры и общество.

Заключение

Кибертерроризм может рассматриваться как феномен гибридной угрозы для национальной безопасности государства, т. к. развивается технологически и распространяет свое влияние на различные сферы деятельности государства и общества. В ходе исследования было дано современное определение понятию «кибертерроризм», исходя из понимания сущности национальной безопасности, и определение «гибридная угроза» в контексте наличия феномена кибертерроризма; выделены две группы видов влияния кибертерроризма на устойчивость национальной безопасности – технологическая и информационная; определены виды информационного воздействия кибертерроризма, которые имеют наиболее эффективное влияние на устойчивость национальной безопасности, и проанализированы особенности влияния видов информационного воздействия кибертерроризма на устойчивость национальной безопасности.

Список литературы

1. Алексеенко О.В., Гайдук Н.В. Кибертерроризм, методы атаки и способы борьбы с ними // Цифровизация экономики: направления, методы инструменты. 2022. С. 100–104.
2. Амирова Д.К., Габдрахманова Р.И. Кибертерроризм как современная угроза безопасности граждан // Ученые записки Казанского юридического института МВД России. 2021. Т. 6. № 2 (12). С. 126–131.
3. Колосова А.Б., Старичков М.В. Кибертерроризм как форма компьютерной преступности // Вопросы российского и международного права. 2022. Т. 12. № 10-1. С. 556–562.
4. Левченко Н.В. Кибертерроризм как современная угроза человечеству // Сборник научных статей по итогам недели российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя. 2022. С. 258–262.
5. Огородник А.В. История возникновения кибертерроризма: от киберпреступности до кибертерроризма // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности. 2021. С. 146–149.
6. Пучков Д.В. Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8. № 4. С. 382–391.

7. Brenner S.W. Cyberthreats: The emerging fault lines of the Nation State. Oxford University Press, 2009. 320 p.
8. Fisher B.S., Lab S. Encyclopedia of victimology and crime prevention. Thousand Oaks, CA: SAGE Publications, 2010. 1224 p.
9. Hower S., Uradnik K. Cyberterrorism. Santa Barbara, CA: Greenwood, 2011. 410 p.
10. Laqueur W., Smith C., Spector M. Cyberterrorism. Facts on File. Berkley, 2002. 355 p.
11. Lasswell H.D. Power and Society. NY, Toronto, London: McGrow-Hill Book Company, 1950. 295 p.
12. Moore R. Cybercrime: Investigating high-technology computer crime. Cleveland, Mississippi: Anderson Publishing, 2005. 385 p.
13. Paleri P. National security: Imperatives and challenges. New Delhi: Tata McGraw-Hill, 2008. 285 p.
14. Reich P.C. Law, policy, and technology: Cyberterrorism, information warfare, and internet immobilization. Hershey, PA: Information Science Reference, 2012. 496 p.
15. Wolfers A.O., Nitze P.H., King J... Developments in military technology and their impact on United States strategy and foreign policy. USA: Washington Center of Foreign Policy Research for U.S. Senate Foreign Relations Committee, 1959. 73 p.

THE IMPACT OF INFORMATION TYPES OF CYBERTERRORISM AS A HYBRID THREAT ON NATIONAL SECURITY STABILITY

A.A. Kovalev

Russian Academy of National Economy and Public Administration under the President of the Russian Federation, St. Petersburg

The relevance of the study lies in the fact that modern cyberterrorism aims to influence all spheres of activity not only of the state, but also of the society forming it, their political space, economic activity, and social institutions. Therefore, it is already necessary to talk about cyberterrorism as a phenomenon of a hybrid threat to the national security of a modern state, to investigate not only the methods and mechanisms of electronic terrorism, but also those areas that it begins to cover, forming types of technological and informational impact. The study subject was the influence of the information impact types of cyberterrorism on national security stability. The study object was the peculiarities of the influence of various information impact types of cyberterrorism on national security stability. The study purpose was to determine the degree of influence of political, economic, and social threats on national security stability. To achieve the study purpose and solve the tasks set, the logical method of analysis for structuring materials, the historical method for correct and chronologically consistent presentation of facts, the comparative method for identifying distinctive parameters in the compared judgments and the deductive method for determining conclusions based on the results of the study were used. The scientific novelty of the study lies in the research of influencing political, economic, and social threats on national security stability. In the study course, the

modern cyberterrorism concept, based on the understanding of the essence of national security, and the definition of a hybrid threat in the context of cyberterrorism phenomenon was given, two groups of types of cyberterrorism influence on national security stability – technological and informational – were identified, the types of information impact of cyberterrorism that have the most effective impact on national security stability are identified and the features of the impact of information impact types of cyberterrorism on national security stability are analyzed.
Keywords: *national security, cyberterrorism, hybrid threats, electronic space.*

Об авторе:

КОВАЛЕВ Андрей Андреевич – кандидат политических наук, доцент, доцент кафедры государственного и муниципального управления Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, г. Санкт-Петербург. E-mail: kovalev-aa@ranepa.ru

Author information:

KOVALEV Andrey Andreevich – PhD (Political Sciences), Associate Professor, Associate Professor of the Department of State and Municipal Administration of the North-Western Institute of Management – a branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, St. Petersburg. E-mail: kovalev-aa@ranepa.ru

Дата поступления рукописи в редакцию: 02.07.2023.
Дата принятия рукописи в печать: 20.08.2023.