Выпуск 1/2020

DOI: 10.25586/RNU.V9276.20.01.P.104 УДК 343.3

А.В. Костин

ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ: ИСТОРИЯ И СОВРЕМЕННОСТЬ

Посвящено специфике противодействия информационному терроризму. Подчеркивается, что в Российской Федерации проводится существенная работа в этом направлении. Отмечено, что к ключевым приоритетам нашей страны в сфере безопасности относится дальнейшее усиление бескомпромиссной борьбы с глобальной террористической угрозой не только внутри России и по периметру ее границ, но и на дальних рубежах. Предполагается, что национальные интересы и безопасность государства будут обеспечиваться и защищаться, помимо прочего, в информационно-коммуникационном пространстве.

Ключевые слова: информационный терроризм, информационная безопасность, кибертерроризм, кибербезопасность.

A.V. Kostin

COUNTERING INFORMATION TERRORISM: HISTORY AND MODERNITY

Dedicated to the specifics of countering information terrorism. It is emphasized that substantial work is being done in this direction in the Russian Federation. It is noted that the key strengthening of our country's security priorities includes the further strengthening of the uncompromising fight against the global terrorist threat not only within Russia and along the perimeter of its borders, but also at long distances. It is assumed that the national interests and security of the state will be ensured and protected, inter alia, in the information and communication space.

Keywords: information terrorism, information security, cyberterrorism, cybersecurity.

Развитие современного общества характеризуется возрастающими противоречиями между субъектами мировой политики, в первую очередь государствами, их коалициями, крупными ТНК. С 2008 г. экономика большинства стран пребывает в состоянии стагнации. Политические лидеры, находящиеся у власти, и их правительства не могут выработать и предложить народам оптимальный выход из затяжного кризиса.

По окончании очередной встречи руководителей государств G20 в столице Аргентины (30 ноября – 1 декабря 2018 г.) президент России заявил: «Не первый год отслеживаем решения "Большой двадцатки", ощущения очень странные: никаких прорывов, ничего нет. Вот сейчас очередная "двадцатка" закончилась, а ощущение точно такое же: что экономика после этого не ускорит рост, можем сползти в рецессию… очень много противоречий и разногласий». За год до этого, в декабре 2017 г., в докладе Римскому клубу отмечалось: «Сегодняшний кризис нециклический, но усиливающийся. Он не ограничен природой вокруг нас, но включает социальный, политический, культурный, моральный кризис, кризис демократии, идеологий и капиталистической системы».

Неравномерность экономического развития, усугубляемая постоянными кризисами, ведет к перманентным политическим и военным конфликтам, что сказывается на уровне жизни народов. С одной стороны, для начала XXI в. характерны цифровая экономика, роботизация, прорывы в создании искусственного интеллекта, с другой – мы сталкиваемся с размывание «среднего» класса, обнищанием народных масс, миллионами беженцев, необходимостью решать проблему «продовольственной безопасности, которая имеет решающее значение для достижения мира, свободного от голода и всех форм неполноценного питания» [6]. Эти и другие проблемы и противоречия объективно ведут к политической борьбе, принимающей различные формы и масштабы.

История дает нам немало примеров борьбы против существующей власти путем слова, проповедей, учений, теорий, распространяемых памфлетами, слухами, «подметными письмами», листовками и т.д. Примером могут служить события, развернувшиеся в Римской империи в I–III вв. н. э. в городах Малой Азии и Египта. Философы-киники и их приверженцы нападали на власть имущих, на римских префектов и даже императоров. Особенностью их действий были призывы к свержению римской власти, распространяемые путем памфлетов и листовок. До наших дней дошли документы, найденные среди египетских папирусов, получившие название «Акты языческих мучеников Александрии». Некоторые авторы считают их чуть ли не первым образцом нелегальной политической литературы [1, с. 11–17]. Протестуя против диктатуры рабовладельцев, киники ополчались против идеи государственности как таковой. (Киническая философия возникла в Афинах как реакция социальных низов свободной бедноты, метеков, вольноотпущенников на ухудшение жизни, усиление политической и экономической неустойчивости на рубеже V–IV вв. до н. э. Кинизм представлял собой не только философию, обосновывающую специфическую форму мировоззрения, но и способ жизнедеятельности, для которого характерно неприятие ценностей рабовладельческого общества, его законов, обычаев, традиций и морали).

Со своими подстрекательскими и очищающими речами киники шли в толпу: на рыночную площадь, в кварталы бедноты, портики, храмы, на стадионы, в парки и гавани, театры и бани, не гнушались заходить в притоны, кабаки, публичные дома. Они претендовали на подлинное руководство людьми, на власть над их душами. Киники, лишенные в жизни всех реальных прав, считали, что имеют моральное право, в силу авторитета своей философии и мудрости, на власть над людьми [13, с. 105–106].

Исследование истории политических отношений дает возможность проследить, как осуществлялась борьба власть имущих, государства с теми, кто видел в них своего врага.

При императоре Римской империи Тиберии против киников начались репрессии. При Нероне и других практиковались изгнание из Рима, бичевания и казни. Эффект был минимальный. Другую форму борьбы избрал император Юлиан. Он использовал против киников их же оружие – литературу. В своих работах (например, «К невежественным киникам», «Против Ираклия киника» и др.) он показывает слабость их философии, построенную на отрицании и отречении, а также вред их учения для государства. Он умело противопоставляет ранний кинизм тому, что произошло с учением к IV в., смело и с юмором пишет о своих ошибках, что несвойственно многим политическим лидерам и в наши

дни. По-видимому, Юлиан понимал, что идейная победа даст больший эффект, чем физическое уничтожение противника, хотя он не гнушался и этим. Многие века цитируется фрагмент указа Юлиана, направленного на школьную реформу: «Все, кто собирается чему-либо учить, должны быть доброго поведения и не иметь в душе направления, несогласного с государственным».

История кинизма дает нам еще один урок борьбы с терроризмом. Он заключается в том, что к «философам обездоленных» примыкало немало грязных элементов. «Квинтилиан в I в. н. э. с возмущением рассказывает о презренных людях, которые на людях ведут себя как аскеты, а тайком предаются самым разнузданным порокам и чревоугодию. Вот что рассказывает о лжекиниках своего времени Лукиан. Многие рабы и бедняки присвоили себе внешний вид философов: "...небольших хлопот стоило накинуть на себя грубый плащ, приладить суму, взять дубинку в руки, поднять крик... браня и порицая всех. Они знали, что нисколько не пострадают за свои речи, ибо уважение, внушаемое самим видом философа, сулило им полную безопасность..." Во II в. н. э. фигура киника стала обычной принадлежностью всякого сборища, причем настоящего подвижника было трудно отличить от шарлатана» [13, с. 207]. В идейной схватке с терроризмом важно выделять жуликов, авантюристов, обманщиков, эту так называемую пену политической борьбы.

Политическая практика показывает, что слово нередко оказывает более сильное воздействие на массы, чем акт вооруженного насилия. Страх, панику, неуважение к государственному строю можно инициировать или сформировать с помощью простых или даже примитивных тезисов, распространяемых различными способами и средствами. Неслучайно в современный политический лексикон вошли такие понятия, как «информационное оружие», «информационная борьба», «информационный терроризм», «информационная безопасность». «Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников» [7]. В наши дни этот тезаурус пополнился «кибервойной», «кибертерроризмом», «кибербезопасностью» и др.

Об информационном терроризме в современном понимании и необходимости борьбы с ним начали говорить и писать на международном уровне в конце XX – начале XXI в. Резолюция ООН A/53/70 от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» гласит: «Выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств, считая необходимым предотвратить неправомерное использование или использование информационных ресурсов или технологий в преступных или террористических целях, призываем государства-члены содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности. Определить основные понятия, относящиеся к информационной безопасности, включая

несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов. Целесообразно разработать международные принципы, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом» [18]. Затем подобные резолюции стали приниматься ежегодно.

Необходимо отметить роль Российской Федерации в организации борьбы с информационным и кибертерроризмом, а также обеспечении международной информационной безопасности. Именно Россия инициировала обсуждение этих вопросов на международном уровне и добилась их включения в постоянную повестку ООН. В мае 1996 г. на Международной конференции по глобальному информационному сообществу в Мидранде (ЮАР) представителями российской делегации впервые на мировом форуме был поднят вопрос о «новом информационном вызове», делегаты пришли к выводу, что это заслуживает серьезного переговорного процесса [9].

Первые атаки кибертеррористов были осуществлены в конце 90-х гг. XX в. В октябре 1999 г. индонезийская общественная организация East Timor Campaigning провела из Испании, Португалии и Франции атаку на государственные интернет-сайты Индонезии [21, с. 78]. Миру явился еще один лик терроризма – информационно-кибернетический.

Терроризм XXI в. характеризуется значительными военными, финансовыми и техническими возможностями, а также расширением масштабов. Поэтому для многих государств актуальной стала проблема борьбы с международными террористическими организациями. Пророческими оказались слова Е. Месснера, высказанные им более 60 лет назад: «Воевание без войск – воевание партизанами, диверсантами, террористами, вредителями, саботерами, пропагандистами примет в будущем огромные размеры» [11, с. 405]. Такая война (Е. Месснер назвал ее «мятежвойна») характеризуется отсутствием линии фронта и четких границ между противниками, превращением общественного сознания в основной объект воздействия и четырехмерным пространством (к трем традиционным добавляется информационно-психологическое измерение).

Перед специалистами по информационной борьбе таких государств, как Россия, Китай, Индия, США, Великобритания, Израиль и другие, возникла задача разработать концепции информационных операций против международного терроризма и создать соответствующие структуры по их проведению.

В 2006 г. данные структуры были созданы в США. В 2011 г. КНР объявила о создании «сетевой синей армии» в целях охраны интернет-пространства. В феврале 2017 г. войска информационных операций создали в Министерстве обороны Российской Федерации. Об этом заявил министр обороны Российской Федерации Сергей Шойгу на правительственном часе в Государственной думе. Он подчеркнул, что созданный за четыре года новый род войск «гораздо эффективнее и сильнее», чем направление контрпропаганды, которое существовало до этого. Министр также отметил, что «пропаганда должна быть умной, грамотной и эффективной» [12]. Информационное противоборство с условным противником впервые было отработано во время учений «Кавказ-2016».

В сентябре 2018 г. президент США утвердил обновленную стратегию кибербез-

опасности США (National Cyber Strategy of the United States of America). Помощник президента Дж. Болтон, представляя стратегию, заявил, что «Америка и ее союзники подвергаются атакам в киберпространстве каждый день. Злонамеренные государства, преступные и террористические организации стремятся похитить наши интеллектуальную собственность, персональные данные, нанести урон нашей инфраструктуре и даже подорвать нашу демократию с помощью киберинструментов… Стратегия предписывает федеральному правительству предпринимать действия для обеспечения долгосрочного улучшения состояния безопасности в киберпространстве для всех американцев» [20].

В Российской Федерации в 2006 г. был принят Федеральный закон «О противодействии терроризму» и издан Указ президента Российской Федерации «О мерах по противодействию терроризму», который ежегодно уточняется. Данные документы закрепили создание качественно новой, общегосударственной системы противодействия этому опасному явлению. В основу ее формирования был положен переход от преимущественно силового подавления очагов терроризма (борьбы с терроризмом) к комплексной работе в этой сфере (противодействию терроризму). Новая система включила меры по выявлению, предупреждению, пресечению, раскрытию и расследованию террористических актов, а также деятельность по профилактике терроризма, минимизации и ликвидации последствий его проявлений.

В марте 2006 г. в качестве основной организационной координирующей структуры для этой работы был образован Национальный антитеррористический комитет (НАК). В эти государственные органы входят руководители Федеральной службы безопасности, Министерства внутренних дел, Министерства транспорта, Министерства здравоохранения и других государственных структур. Важной особенностью Комитета является то, что в него, помимо руководителей федеральных органов исполнительной власти, входят также представители руководства обеих палат российского парламента, Администрации президента Российской Федерации и Правительства России. Председателем НАК по должности является директор ФСБ России.

Существенное внимание НАК уделяет противодействию информационному терроризму. К этой работе привлекаются различные государственные и негосударственные организации. Например, в Москве 24–25 сентября 2018 г. прошел ежегодный Всероссийский форум «Противодействие идеологии терроризма в образовательной сфере и молодежной среде». Организаторами выступили аппарат НАК, Министерство науки и высшего образования Российской Федерации, Министерство просвещения Российской Федерации, Департамент образования г. Москвы, Российский университет дружбы народов, Московский государственный институт международных отношений (университет) МИД России.

На форуме обсуждались актуальные вопросы противодействия идеологии терроризма в образовательной сфере и молодежной среде: организация работы по формированию антитеррористической грамотности учащихся при общении в сети Интернет; практика подготовки специалистов и методическое обеспечение педагогов и специалистов в рассматриваемой сфере; современные методики выявления среди учащихся лиц, подверженных воздействию радикальных идей, и организация индивидуальной профилактической работы с ними; формирование антитеррористического сознания среди студентов.

Неслучайно проблеме противодействия информационному терроризму в молодежной среде государство уделяет пристальное внимание. Одна из причин этого – внедрение в России форсайт-образования (от англ. *foresight* – «предвидение»). Новую модель образования сегодня определяют Интернет, цифровые технологии, онлайн-образование.

В 2006 г. Минобрнауки России была разработана Концепция долгосрочного прогноза научно-технологического развития Российской Федерации на период до 2025 г., давшая старт трем циклам прогнозных работ. В конце 2012 г. президент России в послании к Федеральному собранию подчеркнул значимость проведенных форсайт-исследований «как для подъема традиционных секторов, так и для прорыва на рынке высоких технологий…» [15]. К реализации данного проекта подключились ведущие вузы страны, в том числе Московский государственный университет, Московский физико-технический институт и др. В Программе развития форсайт-образования – 2035 Центра образовательных инициатив, созданного на базе Северо-Западного института управления РАНХиГС при Президенте Российской Федерации, выделены такие идеологические и политические тенденции в развитии общества, как отход от национально-культурных идентичностей в пользу глобально-сетевых (глобальная сословная структура), рост борьбы между вертикальными (национальными) и глобально-сетевыми принципами интеграции и их инфраструктурами, отказ от стремления к однозначному социальному отождествлению с крупными сообществами в пользу множественности отождествлений с микрогруппами («уникальность») [16]. Это, с одной стороны, усиливает субъектность обучающихся, дает им большую степень свободы в информационном пространстве, с другой – делает молодежь зависимой от воздействия сетевых структур, в том числе позволяет манипулировать сознанием. Как повлиять на поведение молодого человека в социальных сетях, как помочь ему построить оптимальную траекторию в виртуальном пространстве – одна из задач, которую необходимо решать уже сегодня. В этих целях в Китае внедряют рейтинг поведения молодого человека в цифровом пространстве, который затем учитывается при выдаче кредитов, поступлении в вуз и т.д. [10].

Современный терроризм можно побороть при условии объединения усилий большинства государств. В этом направлении Российская Федерация проводит существенную работу, о чем свидетельствует XVII совещание руководителей спецслужб, органов безопасности и правоохранительных органов – партнеров ФСБ России, прошедшее в Москве в ноябре 2018 г. В совещании приняло участие 124 делегации из 79 государств и от 5 международных организаций. (Следует заметить, что в первом таком совещании в 2002 г. принимали участие представители 39 государств).

В приветствии президента Российской Федерации участников совещания подчеркивалось, что «международные террористические организации пытаются активизироваться, в том числе в глобальном информационном пространстве... Приоритетами работы спецслужб является создание эффективной системы физического, информационного и идеологического подавления террористических группировок... Для решения столь серьезных задач необходимо укреплять доверие между государствами, повышать ответственность их действий и прозрачность намерений» [17].

К сожалению, согласованной деятельности государств в этой сфере достичь

не удается. Об этом прямо заявил в своем выступлении на совещании министр иностранных дел России С.В. Лавров: «Налаживанию подлинно коллективных скоординированных действий по-прежнему мешают геополитические амбиции, "скрытые повестки", двойные стандарты, а зачастую стремление использовать радикалов для решения собственных корыстных задач на международной арене» [5]. Примером является поддержка некоторыми игроками на Ближнем Востоке пресловутых «Белых касок», которые под прикрытием псевдогуманитарной деятельности осуществляют откровенные провокации и инсценировки в целях создания поводов для незаконного применения силы против суверенных государств.

В сфере маркетинга и рекламы идет постоянный поиск новых возможностей для воздействия на сознание человека. Поскольку информационное воздействие на человека имеет общие закономерности, можно технологии рекламы и маркетинга использовать и в преступных целях. Сами маркетинговые технологии, по сути, являются технологиями двойного назначения. Они разрабатываются спецслужбами государств и выстраиваются в систему определенных действий. В Европе одним из самых мощных разработчиков маркетинговых технологий является Федеральная разведывательная служба Германии (БНД), которая не только разрабатывает, но и продает их, контролирует их применение, имея систему обратной связи [2].

Как стало известно из документов, обнародованных несколько лет назад экс-сотрудником Агентства национальной безопасности США Эдвардом Сноуденом, спецслужбы Штатов занимаются разработкой и внедрением вредоносных программ, позволяющих вывести из строя системы командования и контроля вооруженных сил противника, а также объекты его критически важной инфраструктуры, включая банковскую систему, электро- и водоснабжение, заводы и аэропорты [19].

С таким подходом к борьбе с информационным терроризмом тяжело рассчитывать на успех. Это особенно опасно в связи с формированием цифрового общества, в котором появятся возможности информационного воздействия на человека с учетом знания практически всех его интеллектуальных и физических особенностей. Информационное влияние можно будет оказывать точечно на людей, занимающих государственные должности, и манипулировать ими. Примеры подобного мы видим и сегодня: в Интернете выкладываются финансовые счета чиновников и сотрудников силовых структур, раскрываются медицинские карты, кредитные истории, смакуются интимные подробности личной жизни и т.д.

Группа хакеров террористической организации «Исламское государство» (запрещена в Российской Федерации), называющая себя «Киберхалифат», 8 ноября 2015 г. поместила в Интернете персональные данные и номера телефонов руководителей Центрального разведывательного управления, Федерального бюро расследований и Агентства национальной безопасности США. Свои действия «Киберхалифат» назвал «местью за гибель» основателя группы, британца Джунаида Хуссейна, который был ликвидирован в августе 2015 г. в результате атаки американского беспилотника [8].

В целях защиты информационного пространства страны президент России 26 июля 2017 г. подписал федеральный закон о безопасности критической информационной инфраструктуры (КИИ): «Настоящий федеральный закон регулирует отношения в области обеспечения

безопасности критической информационной инфраструктуры Российской Федерации» [14]. Согласно закону к КИИ относятся информационные системы и информационно-телекоммуникационные сети госорганов, а также автоматизированные системы управления технологическими процессами в оборонной индустрии, здравоохранении, связи, на транспорте, в кредитно-финансовой сфере, энергетике, а также в ряде отраслей промышленности (топливной, атомной, ракетно-космической, металлургической, химической, горнодобывающей). Кроме того, в перечень объектов КИИ включены организации в сфере науки.

Законом устанавливаются основные принципы обеспечения безопасности КИИ, полномочия государственных органов Российской Федерации в области обеспечения ее безопасности, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

Как и во всякой деятельности, в которой участвуют такие мощные субъекты, как государства и их коалиции, возможны ошибки и курьезные ситуации. В ноябре 2018 г. лондонская газета *The Times* опубликовала статью, в которой детский мультсериал «Маша и Медведь» западные эксперты назвали инструментом «мягкой пропаганды» Кремля. Издание отмечало, что избалованная девочка и медведь, символизирующий Россию, влияют на неокрепший детский разум точно так же, как влияют на взрослых «российские пропагандистские каналы» вроде RT [3].

Сила государства заключается в том, может ли оно своевременно признавать свои ошибки и исправлять их. В 2014 г. Государственной думой Российской Федерации были внесены поправки в ст. 282 Уголовного кодекса Российской Федерации (далее – УК РФ) «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства», что позволило привлекать к уголовной ответственности «за лайки и репосты» в социальных сетях. Число уголовных дел, возбужденных по данной статье, стало расти из года в год, хотя многие осужденные не могли понять, за что они привлечены к уголовной ответственности. Некоторые чиновники критику в свой адрес стали воспринимать как экстремизм.

Во время «Прямой линии» с президентом Российской Федерации 7 июня 2018 г. депутат Госдумы Сергей Шаргунов задал вопрос о «тревожных сигналах с разных мест, особенно из провинции», о привлечении по 282-й статье за выражение мнений. Президент сказал, что правоприменение «не нужно доводить до маразма и абсурда». В октябре того же года были приняты поправки, смягчающие санкции ст. 282 УК РФ.

Существенный вклад в борьбу с информационным терроризмом вносят российские ученые. В начале 90-х гг. XX в. в печати начали появляться статьи, в которых рассматривались проблемы информационной безопасности [4]. Позднее стали проводиться научные конференции, семинары, круглые столы, на которых обсуждались вопросы, связанные с информационной борьбой, противодействием негативному информационному воздействию и др.

В 2017 г. в политическом лексиконе прочно закрепился термин “fake news”, обозначающий новостное сообщение, по форме отражающее реальное событие, а на самом деле заведомо несущее частичную или полную ложь. СМИ, социальные сети в погоне за сенсацией, увеличением числа

подписчиков тиражируют и распространяют подобную информацию. Поступая из разных источников, фейковые новости создают в сознании обычного человека искаженную информационную картину мира, и он становится объектом манипуляции.

В учебники по фейковой журналистике войдет «деятельность» К. Релоциуса в немецком еженедельном журнале *Der Spiegel* («Шпигель»). На протяжении нескольких лет он придумывал факты и душещипательные истории на различные политические темы. Получал премии. Был практически эталонным западным журналистом. «Шпигель» опубликовал десятки сфальсифицированных материалов Релотиуса, среди которых статьи о мальчике из Даръа, который винит себя в том, что из-за него началась сирийская гражданская война, об иракских детях, которых похитили и перевоспитали боевики-исламисты, о юном йеменском узнике Гуантанамо, которого мучили 14 лет, и др. «Клаас Релоциус совершал обман преднамеренно и методично, включая в свои статьи выдуманные диалоги, сфабрикованные истории героев и людей, с которыми он никогда не встречался», – говорится в заявлении *Der Spigel*.

Для проведения успешного противоборства с информационным терроризмом важно доводить до сознания людей, что любой террористический акт, вне зависимости от его мотивов, несет зло, представляет собой преступление, за которое неизбежно последует уголовное наказание. Необходимо лишать террористов ореола борцов за веру, справедливость, выступающих против любых форм угнетения и дискриминации. Учитывая общественную опасность и вред терроризма, нужно демонстрировать бесперспективность достижения политических целей путем террора.

Литература

1. Антология кинизма. М.: Наука, 1984.
2. Бомба для подсознания // Завтра. URL: http://zavtra.ru/blogs/bomba_dlya_podsoznaniya (дата обращения: 24.11.2019).
3. В посольстве России посоветовали Лондону защищаться от «Маши и Медведя» // Известия. 2018. 17 нояб.
4. *Владимиров А. Информационное оружие*: *миф или* реальность? // Красная звезда. 1991. 5 сент.
5. Выступление министра иностранных дел России С.В. Лаврова на XVII совещании руководителей спецслужб, органов безопасности и правоохранительных органов иностранных государств – партнеров ФСБ России (Москва, 7 ноября 2018 г.) // Министерство иностранных дел Российской Федерации. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3400807 (дата обращения: 24.11.2019).
6. Декларация лидеров «Группы двадцати» 1 декабря 2018 г. // Президент России. URL: http://www.kremlin.ru/supplement/5373 (дата обращения: 24.11.2019).
7. Доктрина информационной безопасности Российской Федерации // Российская газета. 2016. 6 дек.
8. Крупные атаки хакеров в 2001–2016 годах: хронология // ТАСС. URL: https://tass.ru/info/1408961 (дата обращения: 24.11.2019).
9. *Крутских А.В.* Информационный вызов безопасности на рубеже XXI века // Международная жизнь. 1999. № 2.
10. *Лифшиц Е.* Всевидящее око: как не оставить цифровой след в Интернете // Известия. 2018. 28 нояб.

11. *Месснер Е.* Лик современной войны // Военная мысль в изгнании. Творчество русской военной эмиграции / сост. И.В. Домнин; ред. А.Е. Савинкин. М.: Русский путь, 1999.
12. Минобороны России создало новые войска информационных операций // Известия. 2017. 22 февр.
13. *Нахов И.М.* Философия киников. М.: Наука, 1982.
14. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
15. Послание президента Федеральному собранию 12 декабря 2012 г. // Президент России. URL: http://kremlin.ru/events/president/news/17118 (дата обращения: 24.11.2019).
16. Программа развития форсайт-образования – 2035 // Tilda. URL: http://changelab.tilda.ws/2035 (дата обращения: 24.11.2019).
17. *Путин В.В.* Участникам XVII совещания руководителей специальных служб, органов безопасности и правоохранительных органов // Президент России. URL: http://www.kremlin.ru/events/president/letters/59052 (дата обращения: 24.11.2019).
18. Резолюция ООН A/RES/53/70 от 4 декабря 1998 г. // Генеральная Ассамблея ООН. URL: http://www.un.org/ru/ga/53/docs/53res1.shtml (дата обращения: 24.11.2019).
19. Сноуден: глобальная онлайн-слежка была лишь начальной целью АНБ, на очереди – вывод из строя инфраструктуры государств // D-Russia.ru. URL: http://d-russia.ru/snouden-globalnaya-onlajn-slezhka-byla-lish-nachalnoj-celyu-anb-na-ocheredi-vyvod-iz-stroya-infrastruktury-gosudarstv.html (дата обращения: 24.11.2019).
20. Трамп утвердил новую стратегию кибербезопасности США // ТАСС. URL: https://tass.ru/mezhdunarodnaya-panorama/5588614 (дата обращения: 24.11.2019).
21. *Федоров А.В.* Международная информационная безопасность: проблема общего подхода // Глобальное информационное общество и проблемы информационной безопасности: материалы круглого стола (Москва, Институт Европы РАН, 21 марта 2001 г.). М.: Экслибрис-Пресс, 2001.

Literatura

1. Antologiya kinizma. M.: Nauka, 1984.
2. Bomba dlya podsoznaniya // Zavtra. URL: http://zavtra.ru/blogs/bomba_dlya_podsoznaniya (data obrashcheniya: 24.11.2019).
3. V posol'stve Rossii posovetovali Londonu zashchishchat'sya ot "Mashi i Medvedya" // Izvestiya. 2018. 17 noyab.
4. *Vladimirov A.* Informatsionnoe oruzhie: mif ili real'nost'? // Krasnaya zvezda. 1991. 5 sent.
5. Vystuplenie ministra inostrannykh del Rossii S.V. Lavrova na XVII soveshchanii rukovoditelej spetssluzhb, organov bezopasnosti i pravookhranitel'nykh organov inostrannykh gosudarstv – partnerov FSB Rossii (Moskva, 7 noyabrya 2018 g.) // Ministerstvo inostrannykh del Rossijskoj Federatsii. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3400807 (data obrashcheniya: 24.11.2019).
6. Deklaratsiya liderov "Gruppy dvadtsati" 1 dekabrya 2018 g. // Prezident Rossii. URL: http://www.kremlin.ru/supplement/5373 (data obrashcheniya: 24.11.2019).
7. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii // Rossijskaya gazeta. 2016. 6 dek.
8. Krupnye ataki khakerov v 2001–2016 godakh: khronologiya // TASS. URL: https://tass.ru/info/1408961 (data obrashcheniya: 24.11.2019).
9. *Krutskikh A.V.* Informatsionnyj vyzov bezopasnosti na rubezhe XXI veka // Mezhdunarodnaya zhizn'. 1999. № 2.

10. *Lifshits E.* Vsevidyashchee oko: kak ne ostavit' tsifrovoj sled v Internete // Izvestiya. 2018. 28 noyab.
11. *Messner E.* Lik sovremennoj vojny // Voennaya mysl' v izgnanii. Tvorchestvo russkoj voennoj emigratsii / sost. I.V. Domnin; red. A.E. Savinkin. M.: Russkij put', 1999.
12. Minoborony Rossii sozdalo novye vojska informatsionnykh operatsij // Izvestiya. 2017. 22 fevr.
13. *Nakhov I.M.* Filosofiya kinikov. M.: Nauka, 1982.
14. O bezopasnosti kriticheskoj informatsionnoj infrastruktury Rossijskoj Federatsii: federal'nyj zakon ot 26 iyulya 2017 g. № 187-FZ. Dostup iz sprav.-pravovoj sistemy "Konsul'tantPlyus".
15. Poslanie prezidenta Federal'nomu sobraniyu 12 dekabrya 2012 g. // Prezident Rossii. URL: http://kremlin.ru/events/president/news/17118 (data obrashcheniya: 24.11.2019).
16. Programma razvitiya forsajt-obrazovaniya – 2035 // Tilda. URL: http://changelab.tilda.ws/2035 (data obrashcheniya: 24.11.2019).
17. *Putin V.V.* Uchastnikam XVII soveshchaniya rukovoditelej spetsial'nykh sluzhb, organov bezopasnosti i pravookhranitel'nykh organov // Prezident Rossii. URL: http://www.kremlin.ru/events/president/letters/59052 (data obrashcheniya: 24.11.2019).
18. Rezolyutsiya OON A/RES/53/70 ot 4 dekabrya 1998 g. // General'naya Assambleya OON. URL: http://www.un.org/ru/ga/53/docs/53res1.shtml (data obrashcheniya: 24.11.2019).
19. Snouden: global'naya onlajn-slezhka byla lish' nachal'noj tsel'yu ANB, na ocheredi – vyvod iz stroya infrastruktury gosudarstv // D-Russia.ru. URL: http://d-russia.ru/snouden-global-naya-onlajn-slezhka-byla-lish-nachalnoj-celyu-anb-na-ocheredi-vyvod-iz-stroya-infrastruktury-gosudarstv.html (data obrashcheniya: 24.11.2019).
20. Tramp utverdil novuyu strategiyu kiberbezopasnosti SSHA // TASS. URL: https://tass.ru/mezhdunarodnaya-panorama/5588614 (data obrashcheniya: 24.11.2019).
21. *Fedorov A.V.* Mezhdunarodnaya informatsionnaya bezopasnost': problema obshchego podkhoda // Global'noe informatsionnoe obshchestvo i problemy informatsionnoj bezopasnosti: materialy kruglogo stola (Moskva, Institut Evropy RAN, 21 marta 2001 g.). M.: Ekslibris-Press, 2001.

DOI: 10.25586/RNU.V9276.20.01.P.114 УДК 341.4

А.В. Креховец, М.А. Степанова, Е.В. Царёв

ХАРАКТЕРИСТИКА УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА СТРАН ЗАПАДНОЙ АЗИИ (НА ПРИМЕРЕ УГОЛОВНОГО ЗАКОНА КОРОЛЕВСТВА БАХРЕЙН)

Анализируются основные источники уголовного права в странах Западной Азии, а также положения Уголовного кодекса Королевства Бахрейн. В частности, рассматриваются структура Уголовного кодекса Бахрейна, характеристика основных институтов общей части уголовного закона, а также особенности установления уголовной ответственности за отдельные виды преступных деяний.
Ключевые слова: Западная Азия, уголовный закон, Королевство Бахрейн, мусульманское право, смешанная правовая система, структура Уголовного кодекса Королевства Бахрейн, преступление, проступок.