DOI 10.24411/2076-1503-2020-10756
УДК 34.096

ЛОБАЧ Дмитрий Владимирович,
кандидат юридических наук,
доцент кафедры теории и истории
российского и зарубежного права Института
права Владивостокского государственного
университета экономики и сервиса
e-mail: dimaved85@mail.ru

СМИРНОВА Евгения Александровна,
кандидат юридических наук,
старший преподаватель кафедры трудового
и экологического права Юридической школы
Дальневосточного федерального университета,
г. Владивосток
e-mail: smirnova.ea@dvfu.ru
ORCID 0000-0002-7606-4444

МИРОШНИЧЕНКО Ольга Игоревна,
кандидат юридических наук,
заведующая кафедрой теории и истории
государства и права Юридической школы
Дальневосточного федерального университета,
г. Владивосток
e-mail: olga-star.05@mail.ru

НАЦИОНАЛЬНЫЙ УГОЛОВНО-ПРАВОВОЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННЫХ УСЛОВИЯХ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-511-00009.

Аннотация. *В статье рассматривается зарубежный опыт уголовно-правового противодействия кибертерроризму, представляющему собой нетипичную разновидность традиционного терроризма. Отмечается, что, хотя в системе современного международно-правового противодействия терроризму всё ещё нет единого универсального определения данному явлению, однако кибертерроризм как деструктивное явление социальной действительности начинает получать правовую оценку в национальном уголовном законодательстве разных стран, что предполагает установление уголовной ответственности за его различные проявления. Анализируются два подхода криминализации общественно опасных деяний, квалифицируемых как кибертерроризм. В рамках первого подхода противоправные действия, совершаемые посредством использования информационно-коммуникационных технологий в сети Интернет, могут охватываться расширенной дефиницией террористического акта за счёт включения в объективную сторону этого преступления обобщенной формы возможных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба или наступления иных тяжких последствий. На примере российского опыта противодействия преступлениям в сфере компьютерной информации в части криминализации неправомерного воздействия на критическую информационную инфраструктуру (КИИ) обосновывается вывод, что компьютерные атаки против объектов КИИ в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений также можно квалифицировать как террористический акт. В рамках второго подхода кибертерроризм на законодательном уровне закреплен в качестве самостоятельного преступления.*

Ключевые слова: *терроризм, компьютерные преступления, кибертерроризм, теракт, критическая информационная инфраструктура.*

LOBACH Dmitry Vladimirovich,
PhD in Law,
associate Professor of theory and history
Russian and foreign law Institute
rights of the Vladivostok state University
University of Economics and service

SMIRNOVA Evgenia Aleksandrovna,
PhD in Law,
senior lecturer of the Department of labor
and environmental law School
Far Eastern Federal University,
Vladivostok

MIROSHNICHENKO Olga Igorevna,
PhD in Law,
head of the Department of theory and history
States and Law school rights
Far Eastern Federal University,
Vladivostok

NATIONAL CRIMINAL LAW EXPERIENCE IN COUNTERING CYBER TERRORISM IN MODERN CONDITIONS

The research was carried out with the financial support of the RFBR in the framework of scientific project No. 20-511-00009.

Annotation. *The article presents the foreign experience of criminal-legal counteraction to cyberterrorism, which is an atypical variety of traditional terrorism. It is noted that although in the system of modern international legal counteraction to terrorism there is still no single universal definition of this phenomenon, however, cyber terrorism as a destructive phenomenon begins to operate a legal assessment in the national criminal legislation of different countries, which implies the establishment of criminal responsibility for its various manifestations. Two approaches to the criminalization of socially dangerous acts classified as cyber terrorism are analyzed. Within the framework of the first approach, illegal actions committed through the use of information and communication technologies in the network, a terrorist act due to the inclusion in the objective form of this generalized activity of actions that create the danger of death of people, causing significant property damage or the onset of grave consequences. Based on the example of the Russian experience in combating crimes in the field of computer information in terms of critical information infrastructure (CII), the conclusion is substantiated that computer attacks against CII facilities in order to destabilize the activities of authorities or international organizations, or influencing their decision-making can also be qualified as a terrorist act. Within the framework of the second version, cyber terrorism is enshrined at the legislative level as an independent development.*

Key words: *terrorism, computer crimes, cyber terrorism, terrorist attack, critical information infrastructure.*

Широкое распространение и интенсивное применение информационно-коммуникационных технологий в условиях цифровой трансформации социальных отношений предопределяет сущностные изменения природы преступности, выражаемые в увеличении криминальных актов, которые совершаются в информационном пространстве [26; 27]. Действительно, даже поверхностный анализ состояния и динамики преступлений, совершаемых в интернет-пространстве, свидетельствует о тенденции криминализации Интернета по мере роста цифровых ресурсов и увеличения количества лиц, интегрированных в цифровое взаимодействие. При этом криминализация Интернета выражается в совершении преступлений в сфере компьютерной информации (например, неправомерный доступ к компьютерной информации, распространение вредоносных программ, неправомерное воздействие на критическую информационную

инфраструктуру), преступлений против собственности (хищение чужого имущества посредством мошенничества, вымогательство), завладении чужими конфиденциальными данными, нарушении аутентичности данных с последующим их использованием в противоправных целях (подлог), распространение информации с запрещенным контентом (детская порнография, экстремистские идеи), нарушении авторских и смежных прав. Особое внимание в научной литературе [1] и средствах массовой информации обращается на использование преступниками интернет-пространства и информационно-коммуникационных технологий в целях противоправного воздействия на органы власти и (или) создание атмосферы страха в обществе, что обусловливает зарождение кибертерроризма как нетипичного вида традиционного терроризма [2]. Подобное обособление происходит в результате расширения информационно-коммуникационных отношений в сети Интернет, интенсивного развития современных цифровых технологий и активной интеграции систем управления в цифровое пространство. Кибертерроризм как принципиально новое явление криминогенного характера в современных условиях не имеет четких правовых критериев в юридической науке, что предопределяет сложности в части его отграничения от смежных понятий (например, кибератака, кибервойна, хактивизм, кибершпионаж, преступления в сфере компьютерной информации) [3]. В свою очередь, отсутствие идентифицируемых признаков этого явления приводит к разнообразию релевантных представлений и предложений относительно выработки наиболее приемлемого определения данного вида терроризма. Ситуация во многом усугубляется еще и тем фактом, что в системе международного конвенционного механизма противодействия терроризму отсутствует легальное закрепление данного деструктивного явления, а региональные конвенции в области информационной безопасности лишь в некоторых случаях регламентируют привязку отдельных проявлений терроризма к компьютерным преступлениям. Например, ст. 15 Конвенции Лиги арабских государств «О борьбе с преступлениями в области информационных технологий» [4] от 2010 г. раскрывает юридическое содержание преступлений, связанных с терроризмом, совершенных путем информационных технологий. К таким преступлениям относятся: распространение и пропаганда идей и принципов террористических групп; финансирование и подготовка террористических операций, а равно обеспечение связи между террористическими организациями; распространение методов изготовления взрывчатых веществ в целях использования в террористических операциях; распространение религиозного фанатизма, разногласий и религиозной вражды. Обязательным контекстным признаком выступает условие совершения этих деяний, которое выражается в использовании информационных технологий. Похожая ситуация наблюдается в Конвенции Африканского Союза «О кибербезопасности и защите персональных данных» [5] от 27 июня 2014 г., где в п. «b» ч. 1 ст. 30 определено, что государства-участники должны принять необходимые нормативно-правовые меры, закрепляющие в качестве отягчающего обстоятельства использование информационно-коммуникационных технологий для совершения краж, мошенничества, сокрытия похищенного имущества, злоупотребления доверием, вымогательства, отмывания денег и терроризма.

Вместе с тем, кибертерроризм как деструктивное явление социальной действительности начинает получать правовую оценку в национальном законодательстве отдельных стран, что предполагает установление уголовной ответственности за его различные проявления. При этом прослеживаются два подхода в криминализации деяний, охватываемых данным понятием.

В рамках первого подхода кибертерроризм как самостоятельное юридическое понятие в национальном законодательстве отсутствует, однако юридическая конструкция правовых норм, регламентирующих ответственность за террористический акт, в контексте расширенного толкования допускает регулятивную экстраполяцию этих норм в отношении других общественно опасных деяний, не указанных в диспозиции самой нормы. Проиллюстрировать сказанное можно на примере отдельных уголовных законов государств, являющихся членами Содружества Независимых Государств. Так, анализируя диспозиции правовых норм о терроризме (террористическом акте) в ряде национальных уголовных законов, усматривается унифицированный подход в закреплении неисчерпывающего (открытого) перечня общественно опасных деяний, составляющих объективную сторону терроризма. В частности, в ст. 214 УК Азербайджана [6], ст. 217 УК Армении [7], ст. 255 УК Казахстана [8], ст. 239 УК Киргизии [9], ст. 179 УК Таджикистана [10], ст. 278 УК Молдавии [11], ст. 271 УК Туркменистана [12], ст. 258 УК Украины [13] и ст. 205 УК России [14] объективная сторона терроризма (террористического акта) выражается в совершении взрыва, поджога или других действий, создающих опасность гибели людей, причинения значительного имущественного ущерба или других общественно опасных последствий. В этом случае способы совершения террористического акта определяются через законодательное закрепление наиболее типичных действий (взрыва, поджога), а также указывается

обобщенная форма возможных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба или наступления иных тяжких последствий. Таким образом, законодатель подчеркивает основное характерное свойство этих действий – их общеопасный характер, а с другой стороны, указывает на обязательные свойства взрыва, поджога и иных подобных действий – их реальную способность повлечь обозначенные в законе последствия [15]. В российской судебной правоприменительной практике к тяжким последствиям относят: причинение тяжкого вреда здоровью хотя бы одному человеку, а также средней тяжести вреда здоровью двум и более лицам; дезорганизацию деятельности органов государственной власти и местного самоуправления; длительное нарушение работы предприятия (предприятий) и (или) учреждения (учреждений) независимо от их ведомственной принадлежности, формы собственности, организационно-правовой формы; существенное ухудшение экологической обстановки (например, деградация земель, загрязнение поверхностных и внутренних вод, атмосферы, морской среды и иные негативные изменения окружающей среды, препятствующие ее сохранению и правомерному использованию, устранение последствий которых требует длительного времени и больших материальных затрат) [16].

В контексте расширенного перечня деяний, приводящих к тяжким последствиям в свете российской судебной правоприменительной практики, актуализируется вопрос о возможности наступления обозначенных последствий посредством совершения кибератак на объекты критической информационной инфраструктуры Российской Федерации. С одной стороны, российский законодатель еще в 2017 г. криминализировал неправомерное воздействие на критическую информационную инфраструктуру государства [17]. Уголовно-правовая норма ст. 274.1 УК РФ предусматривает уголовную ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в т.ч. для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Данная норма по способу закрепления является бланкетной, т.к. отсылает к Федеральному закону от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [18]. В ст. 2 данного Закона дается легальное определение критической информационной инфраструктуре, под которой понимаются объекты критической информационной инфраструктуры (далее – КИИ, объекты КИИ), а также сети электросвязи, используемые для организации взаимодействия таких объектов. В свою очередь, объекты критической информационной инфраструктуры определяются как информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Дается и определение компьютерной атаки, определяемой как целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Несмотря на то что в определении компьютерной атаки отсутствует указание на наступление тяжких последствий, указанных в Постановлении Пленума Верховного Суда РФ от 09.02.2012 г. № 1, однако эти последствия предполагаются исходя из категорирования объектов критической информационной инфраструктуры в соответствии со ст. 7 рассматриваемого Закона. В ч. 2 данной статьи регламентируется, что категорирование объектов КИИ осуществляется исходя из социальной значимости (которая выражается в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимального времени отсутствия доступа к государственной услуге для получателей такой услуги), политической значимости (выражается в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики), экономической значимости (выражается в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации), экологической значимости, которая выражается в оценке уровня воздействия на окружающую среду, и значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Более подробные значения показателей возможного причинения вреда объектам КИИ, дифференцируемым по трем категориям, отражены в постановлении Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации,

а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [19].

Таким образом, последствия от неправомерного воздействия на объекты КИИ Российской Федерации также могут совпадать с негативными последствиями при террористическом акте (например, возникновение опасности гибели человека, причинение значительного имущественного ущерба, устрашение населения, ухудшение экологической обстановки и др.), а в случае, если преследуется цель дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, то по правилам конкуренции правовых норм окончательная квалификация должна происходить по ч. 1 ст. 205 УК РФ, т.е. как террористический акт. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации будет являться только способом совершения террористического акта, подлежащего правовой оценке только с учетом остальных элементов состава преступления (в частности, объекта и субъективной стороны).

В рамках второго подхода в уголовном законодательстве зарубежных стран имеются специальные нормы, которые устанавливают ответственность не только за традиционные преступления террористического характера, но и непосредственно за кибертерроризм как самостоятельное преступление террористического характера. Проиллюстрировать данный подход можно на примере уголовно-правовых норм, предусматривающих ответственность за кибертерроризм в уголовных законах Грузии, Индии, США и Великобритании.

Так, например, в 2006 г. грузинский законодатель криминализировал кибертерроризм (ст. 324.1 УК Грузии), под которым понимается противоправное завладение охраняемой законом компьютерной информацией, ее использование или угроза использования, создающие опасность наступления тяжких последствий, совершенных в целях устрашения населения или (и) воздействия на органы власти [20]. В сравнении с основным составом преступления террористического акта (ст. 323 УК Грузии) кибертерроризм выступает его частным проявлением.

Широкое легальное определение понятия «кибертерроризм» дано в Законе Индии «Об информационных технологиях» от 2000 г. (Information Technology Act). В соответствии со ст. 66F этого документа кибертерроризм охватывает следующие случаи.

Во-первых, это действия, совершенные любым лицом с намерением угрожать единству, целостности, безопасности или суверенитету Индии или посеять страх среди народа или его отдельной группы. К таким действиям относятся: запрещенный доступ или запрещение доступа любому лицу, официально имеющему право доступа к компьютерным ресурсам; попытка войти в компьютерный ресурс или получить к нему доступ, не имея на то официального права или превышая объем санкционированного доступа; распространение компьютерного вируса или содействие в его распространении, что приводит к смерти или наносит травмы людям или причиняет ущерб собственности или уничтожает ее, или создает условия, которые могут привести к смерти или травмированию людей, порче или уничтожению собственности; распространение компьютерного вируса или содействие в его распространении с осознанием того, что такие действия с большой вероятностью приведут к повреждению или нарушению системы жизнеобеспечения общества или к неблагоприятному воздействию на важную информационную инфраструктуру.

Во-вторых, это сознательные действия, связанные с намеренным входом в компьютерный ресурс или получением к нему доступа, не имея на то официального права или превышая объем санкционированного доступа, что обусловливает получение доступа к информации, данным или компьютерной базе данных, которые являются закрытыми по соображениям безопасности государства или отношений с другими странами, или к любой закрытой информации, данным или компьютерной базе данных, использование которых при получении такого доступа, как считается, может нанести вред интересам суверенитета и целостности Индии, безопасности государства, добрососедским отношениям с другими государствами, общественному порядку, нормам приличия и морали, или может привести к неуважению суда, к диффамации или подстрекательству к совершению правонарушения, или может быть выгодно для любого иностранного государства, группы лиц или иных объединений, совершающих преступление кибертерроризма [21].

Предметный анализ криминообразующих признаков данного определения показывает, что по логике индийского законодателя обязательным контекстуальным элементом кибертерроризма является общественная опасность действий, совершаемых в компьютерной информационной среде, которая выражается в угрозе для публичных интересов страны. Обращает на себя внимание тот факт, что Закон Индии «Об информационных технологиях» от 2000 г. предписывает не только, чтобы правонарушитель действовал с целью, присущей терроризму (намерение поставить под угрозу единство, целостность, безопас-

ность или суверенитет Индии или создать атмосферу страха в обществе или отдельной группы), но также и то, чтобы преступление причиняло иные тяжкие последствия – смерть, вред здоровью, нарушение услуг, влияющих на критически важную информационную инфраструктуру.

Не менее интересным представляется опыт криминализации деяний, составляющих кибертерроризм, в федеральном уголовном законодательстве США. Нормативно-правовые начала противодействия преступлениям в сфере компьютерной информации закреплены в подразделе 1030 титула 18 Акта о компьютерном мошенничестве и злоупотреблениях (The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030). В своем нынешнем выражении преступления против компьютерной информации (киберпреступления) представлены семью видами криминальных актов: взлом правительственных компьютеров; взлом компьютеров, приводящий к воздействию на правительственную, кредитную, финансовую или компьютерную информацию; повреждение правительственного, банковского компьютера или компьютера, используемого или затрагивающего внутреннюю или внешнюю торговлю; совершение мошенничества через несанкционированный доступ к правительственному компьютеру, банковскому компьютеру или компьютеру, используемому во внутренней или внешней торговле; угроза повреждения правительственного, банковского компьютера или компьютера, который используется во внутренней или внешней торговле; незаконный оборот паролей для правительственного компьютера, а также влияние такого оборота на внутреннюю или внешнюю торговлю; использование компьютера для шпионажа [22].

В соответствии с подразд. 2332b титула 18 Акта о патриотизме от 2001 г. (террористические акты, выходящие за национальные границы) к преступлениям террористического характера были отнесены деяния, совершаемые через использование компьютера и связанные со шпионажем, а также акты, связанные с распространением вредоносных программ, кодов или команд, причиняющих ущерб компьютеру, а также преднамеренное получение доступа к защищенному компьютеру без авторизации, что приводит к причинению ущерба и убыткам. При этом под убытками в рамках этой диспозиции понимаются любые разумные расходы, связанные с причинением вреда, в т.ч. расходы, понесенные в связи с реагированием на преступление, проведением оценки ущерба, восстановлением данных до исходного состояния, возмещением потерянного дохода и иных косвенных расходов, понесенных из-за прерывания обслуживания [23]. Под акты кибертерроризма подпадают только деяния, выражаемые в распространении вредоносных программ и неправомерном доступе к компьютеру, которые совершаются в отношении только определенных компьютеров или компьютерных систем, используемых исключительно для правительства США, банка или другого финансового учреждения, интересов правительства отдельного штата или компьютеры, которые используются внутренней или внешней торговлей.

Представляется интересным национальный опыт нормативно-правового регулирования отношений в сфере противодействия терроризму в киберпространстве, отраженный в Законе Великобритании о терроризме от 2006 г. (The Terrorism Act 2006). В вводной части Закона дается легальное определение терроризма, под которым понимаются противоправные деяния, а равно угроза таких деяний, которые совершаются для воздействия на правительство или международную организацию или запугивания общества (части общества) с намерением продвижения политических, религиозных или идеологических идей. В соответствии с п. 2 объективная сторона этого преступления охватывает серьезное насилие в отношении человека, значительный имущественный ущерб, создание угрозы для жизни человека, создание серьезных рисков для здоровья и безопасности всего населения или его части, а также деяния, совершаемые с намерением серьезного вмешательства или в целях серьезного нарушения работы электронной системы [24]. Из данной дефиниции видно, что терроризм (точнее акт терроризма) как преступление против общественной безопасности может совершаться не только традиционными способами (причинение вреда жизни, здоровью, а также имущественного ущерба), но и посредством противоправного вмешательства в электронные системы или нарушение их работы. Несмотря на то что в Законе отсутствует нормативное определение того, что такое электронные системы и в чем именно должно выражаться вмешательство в их работу, однако современные реалии, отражающие интенсивное развитие информационно-коммуникационных технологий и возможности дистанционного воздействия на объекты критической информационной инфраструктуры, в совокупности с предпринимаемыми мерами противодействия информационным угрозам позволяют сделать достаточное предположение о нетипичном (нетрадиционном) виде террористического акта. В свою очередь, террористический акт, совершаемый посредством использования информационно-коммуникационных технологий против электронных систем, может быть конкретизирован через положения Закона о

неправомерном использовании компьютеров от 1990 г. [25].

Таким образом, противоправное использование информационно-коммуникативных технологий в отношении компьютерной информации, компьютерных систем и сетей в критических сегментах государства и в частном секторе, которые создают опасность гибели людей, причинения значительного имущественного ущерба или наступления иных общественно опасных последствий (например, сбой системы электроснабжения, дезорганизация работы предприятий, входящих в военно-промышленный комплекс, нарушение работы транспорта и др.) также целесообразно рассматривать в качестве одного из общественно опасных способов совершения террористического акта. При этом кибертерроризм как негативное явление социальной действительности проявляет амбивалентную криминогенную сущность. С одной стороны, объективная сторона кибертерроризма охватывает противоправные действия, связанные с использованием информационно-коммуникативных технологий, а с другой – эти действия направлены против публичных интересов государства, проявляемых в общественной безопасности и общественном порядке.

Список литературы:

[1] Frolova E.E., Polyakova T.A., Dudin M.N., ect. Information security of Russia in the digital economy: the economic and legal aspects // Journal of Advanced Research in Law and Economics. - 2018. - Vol. 9. - № 1. - P. 89–95.

[2] Janczewski L.J., Colarik A.M. Cyber Warfare and Cyber Terrorism. - New York: Information science reference, 2008. - 532 p.; Colarik A.M. Cyber Terrorism: Political and Economic Implications. - Hershey, 2006. - P. 2–7.

[3] Brickey J. Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace // Westpoint CTC Sentinel. - 2012. - Vol. 5. - Iss. 8. - P. 4–6; Theohary C.A., Rollins J.W. Cyberwarfare and Cyberterrorism: In Brief [Электронный ресурс]. The Federation of American Scientists. Режим доступа: https://fas.org/sgp/crs/natsec/R43955.pdf

[4] Arab Convention on Combating Information Technology Offences [Электронный ресурс]. Asian school of cyber laws. Режим доступа: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

[5] Конвенции Африканского Союза «О кибербезопасности и защите персональных данных» (Малабо, 27 июня 2014 г.) [Электронный ресурс]. Режим доступа: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/African%20Union%20Convention%20on%20CyberSecurity%20%26%20Personal%20Data%20Protection_1.pdf

[6] Уголовный кодекс Азербайджанской Республики от 1 сентября 2000 г. [Электронный ресурс]. СПС «Юрист». Режим доступа: https://online.zakon.kz/m/document/?doc_id=30420353

[7] Уголовный кодекс Республики Армения от 29 апреля 2003 г. [Электронный ресурс]. Официальный сайт Национального Собрания Республики Армения. Режим доступа: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus

[8] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. [Электронный ресурс]. СПС «Юрист». Режим доступа: https://online.zakon.kz/m/document?doc_id=31575252

[9] Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. [Электронный ресурс]. СПС «Юрист». Режим доступа: https://online.zakon.kz/m/document?doc_id=34350840

[10] Уголовный кодекс Республики Таджикистан от 21 мая 1998 г. [Электронный ресурс]. СПС «Юрист». Режим доступа: https://online.zakon.kz/Document/?doc_id=30397325#pos=4656;-60

[11] Уголовный кодекс Республики Молдова от 18 апреля 2002 г. [Электронный ресурс]. Официальный сайт парламента Республики Молдова. Режим доступа: http://lex.justice.md/ru/331268/

[12] Уголовный кодекс Туркменистана от 12 июня 1997 г. [Электронный ресурс]. СПС «Юрист». Режим доступа: https://online.zakon.kz/document/?doc_id=31295286#pos=6;-106

[13] Уголовный кодекс Украины от 5 апреля 2001 г. [Электронный ресурс]. Официальный сайт Верховной Рады Украины. Режим доступа: https://zakon.rada.gov.ua/laws/show/2341-14#Text

[14] Уголовный кодекс Российской Федерации от 13 июня 1996 г. [Электронный ресурс]. Режим доступа: СПС «КонсультантПлюс».

[15] Ткаченко В.В., Ткаченко С.В. Российский терроризм: проблемы уголовной ответственности: монография. - М.: ИНФРА-М., 2015. - С. 38.

[16] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: Постановление Пленума Верховного Суда РФ от 09.02.2012 г. № 1 (ред. от 03.11.2016) [Электронный ресурс]. Режим доступа: СПС «КонсультантПлюс».

[17] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации Федеральный закон» [Электронный ресурс]: Федеральный закон от 26.07.2017 г. № 194-ФЗ. Режим доступа: СПС «КонсультантПлюс».

[18] О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федеральный закон от 26.07.2017 г. № 187-ФЗ. Режим доступа: СПС «КонсультантПлюс».

[19] Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [Электронный ресурс]: Постановление Правительства РФ от 8 февраля 2018 г. № 127. Режим доступа: СПС «КонсультантПлюс».

[20] Уголовный кодекс Грузии от 22 июля 1999 г. / науч. ред. З.К. Бигвава / пер. с груз. И. Мериджанашвили. - СПб.: Изд-во «Юридический центр Пресс», 2001; Уголовный кодекс Грузии от 22 июля 1999 г. [Электронный ресурс]. Законодательный вестник Грузии. Режим доступа: https://matsne.gov.ge/ru/document/view/16426

[21] Understanding cybercrime: Phenomena, challenges and legal response. September 2012. - P. 221, 222. [Электронный ресурс]. Режим доступа: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[22] Charles D. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws [Электронный ресурс]. The Federation of American Scientists. Режим доступа: https://fas.org/sgp/crs/misc/RS20830.pdf

[23] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001 [Электронный ресурс]. United States Government Publishing Office. Режим доступа: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[24] The Terrorism Act 2006 [Электронный ресурс]. Режим доступа: https://www.gov.uk/government/publications/the-terrorism-act-2006

[25] Computer Misuse Act 1990 [Электронный ресурс]. Режим доступа: http://www.legislation.gov.uk/ukpga/1990/18/enacted

[26] Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75–87. DOI: 10.31857/S013207690009678-7

[27] Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Обзор Международной научно-практической конференции «Информационное пространство: обеспечение информационной безопасности и право» – Первые Бачиловские чтения // Государство и право. 2018. № 9. С. 138–148. DOI: 10.31857/S013207690001525-9

Spisok literatury:

[1] Frolova E.E., Polyakova T.A., Dudin M.N., ect. Information security of Russia in the digital economy: the economic and legal aspects // Journal of Advanced Research in Law and Economics. - 2018. - Vol. 9. - № 1. - P. 89–95.

[2] Janczewski L.J., Colarik A.M. Cyber Warfare and Cyber Terrorism. - New York: Information science reference, 2008. - 532 p.; Colarik A.M. Cyber Terrorism: Political and Economic Implications. - Hershey, 2006. - P. 2–7.

[3] Brickey J. Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace // Westpoint CTC Sentinel. - 2012. - Vol. 5. - Iss. 8. - P. 4–6; Theohary C.A., Rollins J.W. Cyberwarfare and Cyberterrorism: In Brief [Elektronnyj resurs]. The Federation of American Scientists. Rezhim dostupa: https://fas.org/sgp/crs/natsec/R43955.pdf

[4] Arab Convention on Combating Information Technology Offences [Elektronnyj resurs]. Asian school of cyber laws. Rezhim dostupa: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

[5] Konvencii Afrikanskogo Soyuza «O kiberbezopasnosti i zashchite personal'nyh dannyh» (Malabo, 27 iyunya 2014 g.) [Elektronnyj resurs]. Rezhim dostupa: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/African%20Union%20Convention%20on%20CyberSecurity%20%26%20Personal%20Data%20Protection_1.pdf

[6] Ugolovnyj kodeks Azerbajdzhanskoj Respubliki ot 1 sentyabrya 2000 g. [Elektronnyj resurs]. SPS «Yurist». Rezhim dostupa: https://online.zakon.kz/m/document/?doc_id=30420353

[7] Ugolovnyj kodeks Respubliki Armeniya ot 29 aprelya 2003 g. [Elektronnyj resurs]. Oficial'nyj sajt Nacional'nogo Sobraniya Respubliki Armeniya. Rezhim dostupa: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus

[8] Ugolovnyj kodeks Respubliki Kazahstan ot 3 iyulya 2014 g. [Elektronnyj resurs]. SPS «Yurist». Rezhim dostupa: https://online.zakon.kz/m/document?doc_id=31575252

[9] Ugolovnyj kodeks Kyrgyzskoj Respubliki ot 2 fevralya 2017 g. [Elektronnyj resurs]. SPS «Yurist». Rezhim dostupa: https://online.zakon.kz/m/document?doc_id=34350840

[10] Ugolovnyj kodeks Respubliki Tadzhikistan ot 21 maya 1998 g. [Elektronnyj resurs]. SPS «Yurist». Rezhim dostupa: https://online.zakon.kz/Document/?doc_id=30397325#pos=4656;-60

[11] Ugolovnyj kodeks Respubliki Moldova ot 18 aprelya 2002 g. [Elektronnyj resurs]. Oficial'nyj sajt parlamenta Respubliki Moldova. Rezhim dostupa: http://lex.justice.md/ru/331268/

[12] Ugolovnyj kodeks Turkmenistana ot 12 iyunya 1997 g. [Elektronnyj resurs]. SPS «Yurist». Rezhim dostupa: https://online.zakon.kz/document/?doc_id=31295286#pos=6;-106

[13] Ugolovnyj kodeks Ukrainy ot 5 aprelya 2001 g. [Elektronnyj resurs]. Oficial'nyj sajt Verhovnoj Rady Ukrainy. Rezhim dostupa: https://zakon.rada.gov.ua/laws/show/2341-14#Text

[14] Ugolovnyj kodeks Rossijskoj Federacii ot 13 iyunya 1996 g. [Elektronnyj resurs]. Rezhim dostupa: SPS «Konsul'tantPlyus».

[15] Tkachenko V.V., Tkachenko S.V. Rossijskij terrorizm: problemy ugolovnoj otvetstvennosti: monografiya. - M.: INFRA-M., 2015. - S. 38.

[16] O nekotoryh voprosah sudebnoj praktiki po ugolovnym delam o prestupleniyah terroristicheskoj napravlennosti: Postanovlenie Plenuma Verhovnogo Suda RF ot 09.02.2012 g. № 1 (red. ot 03.11.2016) [Elektronnyj resurs]. Rezhim dostupa: SPS «Konsul'tantPlyus».

[17] O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i stat'yu 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii v svyazi s prinyatiem Federal'nogo zakona «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii Federal'nyj zakon» [Elektronnyj resurs]: Federal'nyj zakon ot 26.07.2017 g. № 194-FZ. Rezhim dostupa: SPS «Konsul'tantPlyus».

[18] O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [Elektronnyj resurs]: Federal'nyj zakon ot 26.07.2017 g. № 187-FZ. Rezhim dostupa: SPS «Konsul'tantPlyus».

[19] Ob utverzhdenii pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij [Elektronnyj resurs]: Postanovlenie Pravitel'stva RF ot 8 fevralya 2018 g. № 127. Rezhim dostupa: SPS «Konsul'tantPlyus».

[20] Ugolovnyj kodeks Gruzii ot 22 iyulya 1999 g. / nauch. red. Z.K. Bigvava / per. s gruz. I. Meridzhanashvili. - SPb.: Izd-vo «Yuridicheskij centr Press», 2001; Ugolovnyj kodeks Gruzii ot 22 iyulya 1999 g. [Elektronnyj resurs]. Zakonodatel'nyj vestnik Gruzii. Rezhim dostupa: https://matsne.gov.ge/ru/document/view/16426

[21] Understanding cybercrime: Phenomena, challenges and legal response. September 2012. - P. 221, 222. [Elektronnyj resurs]. Rezhim dostupa: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[22] Charles D. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws [Elektronnyj resurs]. The Federation of American Scientists. Rezhim dostupa: https://fas.org/sgp/crs/misc/RS20830.pdf

[23] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001 [Elektronnyj resurs]. United States Government Publishing Office. Rezhim dostupa: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[24] The Terrorism Act 2006 [Elektronnyj resurs]. Rezhim dostupa: https://www.gov.uk/government/publications/the-terrorism-act-2006

[25] Computer Misuse Act 1990 [Elektronnyj resurs]. Rezhim dostupa: http://www.legislation.gov.uk/ukpga/1990/18/enacted

[26] Polyakova T.A., Minbaleev A.V., Krotkova N.V. Novye vektory razvitiya informacionnogo prava v usloviyah civilizacionnogo krizisa i cifrovoj transformacii // Gosudarstvo i pravo. 2020. № 5. S. 75–87. DOI: 10.31857/S013207690009678-7

[27] Polyakova T.A., Minbaleev A.V., Krotkova N.V. Obzor Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnoe prostranstvo: obespechenie informacionnoj bezopasnosti i pravo» – Pervye Bachilovskie chteniya // Gosudarstvo i pravo. 2018. № 9. S. 138–148. DOI: 10.31857/S013207690001525-9