нию — с другой стороны. Однако и в действующей системе уголовно-правовой охраны возможна адекватная оценка подобных деяний. Так, цифровая валюта может рассматриваться как предмет преступления при совершении хищений, а также взяток и коммерческого подкупа, и как средство совершения преступления при легализации имущества, приобретенного преступным путем, обналичивания денежных средств, уклонения от уплаты налогов, а равно иных схожих преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Как все начиналось. История криптовалюты. URL: https://pikabu.ru/story/kak_vse_nachinalos_istoriya_kriptovalyutyi_6540989 (дата обращения: 05.09.2021).

2. О криптовалютах. URL: https://iamforextrader.ru/skolko-vsego-sushhestvuet-kriptovalyut/ (дата обращения: 05.09.2021).

3. Сколько всего существует криптовалют. URL: https://internationalwealth.info/cryptocurrency/cryptocurrency-regulation-in-2020-in-different-regions-europe/ (дата обращения: 05.09.2021).

4. Her Majesty's Revenue and Customs, Управление Её Величества по налогам и таможенным пошлинам). URL: https://nesrakonk.ru/hm-revenue-and-customs-hmrc/ (дата обращения: 05.09.2021).

4. Как в разных странах регулируют криптовалюту: обзор законов в 2020 г. URL: https://habr.com/ru/company/moneypipe/blog/523354/ (дата обращения: 05.09.2021).

5. Абрамова Е. Н. К вопросу о понятии криптовалюты: проблемы терминологии и формирования дефиниции // Банковское право. 2021. № 2. С. 23–27.

6. Шарапов Р. Д., Минин Р. В., Капаева Е. О. Криптовалюта: уголовно-правовой аспект // Юридическая наука и правоохранительная практика. 2018. № 2. С. 43–49.

7. Маслакова Е. Е. Предмет преступления как форма выражения общественных отношений // Ученые записки Орловского гос. ун-та. Серия: Гуманитарные и социальные науки. 2015. № 1. С. 257–261.

8. Уголовное право Российской Федерации. Общая часть: учебник / Ю. В. Грачева, Л. Д. Ермакова, Г. А. Есаков и др. ; под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. 2-е изд., перераб. и доп. М. : КОНТРАКТ; ИНФРА-М, 2008. 600 с.

9. Информационное сообщение Росфинмониторинга от 6 февраля 2014 г. «Об использовании криптовалют». Документ опубликован не был // СПС «КонсультантПлюс».

10. Коренная А. А., Тыдыкова Н. В. Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 408–415.

УДК 343.341
ББК 67.408.131.11

О НЕКОТОРЫХ АСПЕКТАХ МЕТОДИКИ БОРЬБЫ С ИДЕОЛОГИЕЙ ТЕРРОРИЗМА И КИБЕРТЕРРОРИЗМА В СРЕДЕ РОССИЙСКИХ ВУЗОВ (НА ПРИМЕРЕ АЛТАЙСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА)

В. А. Мазуров, М. А. Стародубцева
Алтайский государственный университет (Барнаул, Россия)

Вследствие пандемии новой коронавирусной инфекции, ознаменовавшейся локдаунами 2020 г., криминогенная обстановка как в России, так и в мире вышла на качественно новый уровень. Можно сказать, что был достигнут предсказанный на 12-м Конгрессе ООН по предупреждению преступности и уголовному правосудию В. В. Лунеевым порог терпимости населения, отразивший критическую массу преступности, после чего она под воздействием пандемии перешла в цифровую сферу. В очередной раз подтвердился диалектический закон о переходе количествен-

ных изменений в качественные. Нужно отметить, что данный процесс продолжает наращивать свои темпы и в 2021 г.: все большие отрасли преступности уходят в киберпространство. На этой почве актуально усиление взаимодействия институтов гражданского общества и правоохранительных органов, особенно в молодежной среде. Именно молодежь является потенциальной «группой риска» в террористической и кибертеррористической преступности прежде всего как объект вербовки. Но именно молодежь выступает активнейшим пользователем информационно-телекоммуникационных сетей, в том числе и сети Интернет. В связи с этим, думается, приоритет лежит именно в среде институтов гражданского общества, напрямую работающих с молодежью. А одним из основных институтов выступает среднее и высшее образование, и именно сеть университетов может стать флагманом формирования антитеррористической идеологии и навыков противодействия кибертерроризму.

Ключевые слова: терроризм, кибертерроризм, стратегия, идеология, цифровая криминология, цифровое просвещение, студенческие организации.

ON SOME ASPECTS OF THE METHODOLOGY OF COMBATING THE IDEOLOGY OF TERRORISM AND CYBERTERRORISM IN THE AMONG RUSSIAN UNIVERSITIES (ON THE EXAMPLE OF THE ALTAI STATE UNIVERSITY)

V. A. Mazurov, M. A. Starodubtseva
Altai State University (Barnaul, Russia)

After the pandemic of the new coronavirus infection, marked by the «lockdowns' of 2020, the crime situation both in Russia and in the world has reached a qualitatively new level. We can say that the threshold of population tolerance predicted at the 12th UN Congress on Crime Prevention and Criminal Justice by V. V. Luneev. Once again, the dialectical law on the transition of quantitative changes to qualitative ones was confirmed. It should be noted that this process continues to increase its pace in 2021: all large branches of crime are going into cyberspace. On this basis, the strengthening of the interaction of civil society institutions and law enforcement agencies, especially among the youth, is becoming increasingly important. It is young people who are a potential «risk group» in terrorist and cyber-terrorist crime, primarily as an object of recruitment. But it is young people who are the most active users of information and telecommunication networks, including the Internet. In this regard, it seems that the priority lies precisely in the environment of civil society institutions that directly work with young people. And one of the main institutions is secondary and higher education, and it is the network of universities that can become the flagship of the formation of anti-terrorist ideology and skills in countering cyber terrorism.

Keywords: terrorism, cyber terrorism, strategy, ideology, digital criminology, digital education, student organizations.

DOI: https://doi.org/10.14258/ralj(2021)3.2

Серия локдаунов, прокатившихся по мировому сообществу в 2020 г., ознаменовала собой фактический переход преступности на новый, цифровой уровень, и резкое изменение криминогенной обстановки как на международном, так и на национальном уровнях [1, с. 24].

С криминологической точки зрения можно отметить произошедший переход как достижение «предела терпимости к уровню преступности в обществе», прогнозированный российским криминологом В. В. Лунеевым на 12 Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, прошедшем в 2010 г. в Бразилии [2, с. 7]. Изменение картины преступности и перевод ее в киберпространство иллюстрирует также один из фундаментальных диалектических законов, а именно закон перехода количественных изменений в качественные. Сама же борьба также перешедших в цифровую сферу правоохранителей с новой фазой киберпре-

ступности отражает еще один из законов диалектики: формулу единства и борьбы противоположностей.

Количественный рост киберпреступлений подтверждает и статистика 2021 г. В частности, в России за январь 2021 г. число выявленных киберпреступлений возросло на 32,2% по сравнению с аналогичным периодом 2020 г. Эта тенденция наблюдается и на международном уровне. При этом идет и качественный рост данной сферы криминального мира. Киберпреступность быстро прогрессирует, соответственно растут и расходы на борьбу с ней. Обратимся к данным аналитиков. Американская компания по киберзащите Cybersecurity Ventures ожидает, что в 2021 г. киберпреступность нанесет общий мировой ущерб в 6 трлн долларов США. Прогнозируется, что мировые затраты на киберпреступность будут непрерывно расти на 15% в год, достигнув 10,5 трлн долларов США в год к 2025 г. по сравнению с 3 трлн долларов США в 2015 г. [3, с. 14].

Данная тенденция может означать крупнейшее перераспределение экономических благ за период цивилизации. Риск киберпреступности для стимулов к инновациям и инвестициям экспоненциально больше, чем годовой ущерб, нанесенный стихийными бедствиями. Указанные цифры касаются только видимой части сети Интернет. Необходимо отметить, что в «теневом Интернете» ущерб от киберпреступности на сегодняшний день невозможно измерить в количественном отношении. По некоторым данным, размер теневой сети (которая не индексируется и недоступна для поисковых систем) в 5 тысяч раз превышает размеры официального Интернета. Однако речь идет не об официальных данных, а о результатах журналистских расследований, которые не обладают валидностью и доказательственной силой [3, с. 16].

Быстрее всех к виртуальной реальности адаптировалась кибермафия, о которой впервые официально заговорили именно в 2020 г. Сетевые структуры объединяют усилия, и вероятность установления их местонахождения и привлечения к уголовной ответственности составляет 0,05%, по данным Отчета о глобальных рисках 2020 Всемирного экономического форума. Также Европол в 2021 г. активно заинтересовался кибермафией, что отражают его отчеты о преступных угрозах [4, с. 48].

27 июля 2021 г. Россия внесла в ООН проект конвенции о противодействии киберпреступности и криминальному использованию криптовалюты, являющийся первым нормативным документом непосредственно в данной области. Проект предлагает, в частности, классифицировать киберпреступления на 23 вида, а не на девять, как это принято в настоящий момент в положениях Будапештской конвенции Совета Европы, разработанной с 1997 по 2001 гг. Сюда относятся такие составы преступлений, как несанкционированный доступ к персональным данным, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий, терроризм, экстремизм, реабилитация нацизма, незаконный оборот наркотиков, оружия, вовлечение несовершеннолетних в противоправную деятельность. Одну из основных ролей здесь играет и противодействие кибертерроризму [5, с. 1182].

Рассмотренные нами действия государств и международных и национальных организаций различного уровня свидетельствуют о напряженной работе как международного, так и российского правового и экономического сообщества. Однако при детальном рассмотрении ситуации мы сразу наталкиваемся на терминологическую проблему. На сегодняшний день на международном уровне сохраняется тенденция к расширительному, индуктивному подходу в определении собственно кибертерроризма, при котором имеет место множество конвенций, дающих определение и признаки кибертерроризма применительно к разным составам преступлений. Проект универсальной конвенции в данной области может стать началом перехода к дедуктивному подходу в международной практике и выделению единого определения и критериев кибертерроризма [6, с. 412].

Укажем, что аналогичная ситуация сохраняется и в российской нормативно-правовой сфере.

Термин «кибертерроризм» в национальном праве не имеет закрепления ни в законодательных актах, ни в ведомственных нормативных документах. Уголовная ответственность за совершение террористического акта предусмотрена ст. 205 УК РФ, однако сам Уголовный кодекс РФ не предусматривает квалифицированного признака состава преступления, выражающего осуществление данного акта в киберпространстве [7, с. 156].

Рассмотрим некоторые аспекты развернувшейся по этому поводу дискуссии. Некоторые исследователи считают, что кибертерроризм вполне объективно подпадает под ст. 205 УК РФ, которая не требует дополнительной нормы. Только указанные кибертеррористические акты — это не взрыв,

поджог, а «другие действия». А чтобы кибертеррористы были привлечены к ответственности по этой статье, не требуется вносить поправки в статью, необходимо лишь дать ей более широкое толкование.

Однако есть и другое мнение. В ч. 2 ст. 205 УК РФ предлагается поправка, которая повысит уголовную ответственность за терроризм с использованием компьютерной информации, компьютера, компьютерной системы или их сети.

В таком случае можно будет квалифицировать кибертерроризм как преступление против общественной безопасности и общественного порядка.

В противовес этому некоторые исследователи полагают, что подобные нововведения будут означать излишнюю перегрузку в нормах УК РФ, поскольку кибертерроризм ничем не отличается от обычного терроризма [8, с. 106].

Рассмотренная нами дискуссия и терминологический вакуум не означают, что кибертерроризм полностью отсутствует в российской правовой сфере. Например, термин «кибертерроризм» используется в контексте подготовки по борьбе с терроризмом. Россия также имеет много двусторонних договоров о правовой помощи по уголовным делам с иностранными государствами, где также упоминается сфера кибербезопасности и борьба с кибертерроризмом [9, с. 21].

Наиболее полно, по нашему мнению, кибертерроризм рассматривается в рамках научной дискуссии в российской юридической науке. Однако и здесь нет четко оформленного понимания данного явления и не разработана целостная система профилактики и возможного противодействия терроризму в цифровом пространстве. Основными препятствиями для достижения данной цели, как считается, можно назвать отсутствие связей между вузами регионов, занимающимися разработкой указанных проблем. Единственным средством взаимодействия в научной среде, по сути, выступают межвузовские конференции, а как раз по ним весомо ударил объявленный в России в марте 2020 г. локдаун — большинство мероприятий до сих пор проводится в онлайн-режиме, что, по мнению многих, существенно затрудняет возможность построения дискурса.

С момента начала пандемии затруднено взаимодействие и со студентами. Фактически большая часть учащихся остается не охваченной комплексом проводимых в образовательных учреждениях мероприятий по противодействию терроризму и кибертерроризму. А поскольку именно молодежь как активный пользователь сети Интернет может выступать объектом потенциальной вербовки, на работу с ней необходимо обратить особое внимание.

О желании молодежи участвовать в данном процессе говорит проведенное нами в 2020 г. в Алтайском крае эмпирическое исследование — анонимное анкетирование школьников, студентов и преподавателей по вопросу их правовой осведомленности в отношении экстремизма. Опрошены 74 человека, разделенных нами на две группы. Из них 45 человек — студенты 1–2 курсов СПО (колледж АлтГУ), ученики 9–11 классов МКОУ «Гилевская СОШ». 29 опрошенных — преподаватели колледжа ФГБОУ ВО «Алтайский государственный университет», МКОУ «Гилевская СОШ». Возраст респондентов первой группы 15–17 лет, возраст второй группы — 30–50 лет. По итогам исследования мы увидели, что 69% педагогов знают о проводимых в их школах и колледжах круглых столах по профилактике распространения идеологии терроризма и борьбе с кибертерроризмом, но не вовлекают сюда своих студентов. 31% указали, что не знают о программах мероприятий по профилактике экстремизма и идеологии терроризма в их образовательных учреждениях. Это показывает невовлеченность в подобные мероприятия практически трети педагогического состава. Опрошенные нами школьники и студенты в большинстве указали, что хотят участвовать в борьбе с идеологией терроризма и кибертерроризмом, но не имеют возможности это делать [10, с. 82].

Стоит отметить, что одновременно с началом пандемии и введением дистанционного формата обучения по всей стране непрерывно идет процесс работы с преподавателями по их адаптации в цифровой среде. Уже в 2021 г. произошел качественный скачок в привлечении преподавателей российских вузов к разработке новых образовательных курсов с использованием технологий дистанционного обучения и взаимодействия, налажена в рекордно короткие сроки система обучения преподавательского состава Digital technology на платформах «Университет 20.35», «Университет Иннополис». Отмеченные программы и курсы позволили адаптировать большинство преподавателей к реалиям цифрового мира и помогли возобновить частично прерванный научный процесс. Особенно это касается уголовного права и криминологии, оказавшихся на передовой разработки антитеррористической идеологии среди молодежи.

Увеличение знаний о цифровом мире побудило интерес к цифровым технологиям и адаптации их для нужд криминологии, напрямую занимающейся анализом и прогнозированием противодействия кибертерроризму. В 2018 г. вышел учебник для магистратуры «Криминология цифрового мира» под редакцией В. С. Овчинского, а в 2021 г. презентуется учебное пособие коллектива авторов «Цифровая криминология». Электронные курсы преподавателей на образовательных платформах массово наполняются формами дистанционного взаимодействия, активно применяемыми в учебном процессе. Рабочие программы по предметам уголовно-правового цикла в целом и по криминологии в частности корректируются на изучение криминологии в киберпространстве, где определяющую роль начинает играть проблема кибертерроризма. Ожидается, что рост вовлечения преподавателей в цифровую среду повлечет за собой рост правового просвещения и обучаемой ими молодежи.

Обобщим, что массовая цифровизация университетского образования и научного дискурса идет сейчас по всей территории России и, как ожидается, должна закончиться созданием системы интерактивных учебных заведений, способных непрерывно взаимодействовать с обучающимися в любом уголке страны [11, с. 42]. На территории непосредственно Алтайского края роль флагмана высшего образования отдана Алтайскому государственному университету. Университет с момента начала пандемии 2020 г. активно включился в сферу дистанционного обучения и начал применять цифровые методы общения со студентами. Были проведены десятки научно-практических конференций в онлайн-формате, что позволило существенно сгладить процесс адаптации к новой цифровой сфере как у преподавателей, так и у студентов.

В 2021 г. организовано обучение сотрудников Юридического института на платформе «Университет Иннополис», актуализированы рабочие программы по криминологии и уголовному праву с преимущественным ориентированием на цифровую сферу и проблемы борьбы с киберпреступностью и кибертерроризмом.

В киберпространстве сотрудники и волонтеры университета активно взаимодействуют с правоохранительными органами в вопросе профилактики преступности террористической и кибертеррористической направленности. На основании решения Антитеррористической комиссии Алтайского края (протокол № 73 от 02.03.2020 г.) на базе Юридического института Алтайского государственного университета создан Региональный антитеррористический научно-методический центр (РАНМЦ). Данная структура функционирует в качестве опорного центра по методической, научно-исследовательской работе и проведению региональных профилактических мероприятий антитеррористической направленности.

Сотрудники РАНМЦ при поддержке Министерства образования и науки Алтайского края участвовали в разработке концепции информационной политики в сфере профилактики идеологии терроризма в Алтайском крае в 2021 г. Налажено системное проведение криминолого-психологических исследований и очно-дистанционных научно-практических конференций в области профилактики кибертерроризма регионального, российского и международного уровня.

Необходимо подчеркнуть инициативу вуза и Юридического института по привлечению к вышеуказанной деятельности представителей студенческого сообщества. По инициативе кафедры уголовного права и криминологии Алтайского государственного университета созданы и результативно работают волонтерские студенческие организации «Антиэкстремизм» и «Кибердружина 22», которые принимают активное участие в подготовке и проведении студенческих научно-практических мероприятий, профилактических встреч с обучающимися образовательных учреждений. Руководители данных организаций участвовали в работе Всероссийского форума «Противодействие идеологии терроризма в образовательной сфере и молодежной среде» 24–25 сентября 2018 г., где установили контакты с аналогичными организациями нескольких регионов России. На эпизодической основе студентами устанавливались контакты с международными волонтерскими организациями в сфере профилактики терроризма и кибертерроризма, в частности — с европейской сетью UNITED (United for Intercultural Action).

К работе в сфере профилактики кибертерроризма Юридический институт Алтайского государственного университета активно привлекает представителей среднего профессионального образования. Отметим, что среди российских вузов подобный опыт можно назвать уникальным. В частности, 25 февраля 2020 г. в колледже Алтайского государственного университета состоялась международ-

ная научно-практическая конференция «Социально-экономические, правовые аспекты в обеспечении информационной безопасности в эпоху цифровизации», которая прошла в режиме онлайн.

Конференция была организована в рамках соглашения о сотрудничестве колледжа Алтайского государственного университета и Профессионального колледжа Киргизского национального университета им. Ж. Баласагына. К участию в конференции присоединились и коллеги из Республики Казахстан, Учреждение «Innovative college», г. Семей.

По итогам конференции была принята резолюция, в рамках которой образовательные организации-участники договорились о дальнейшем тесном взаимодействии в ходе подготовки специалистов в области информационной безопасности и информационных технологий, а также экономики и правоведения.

Безусловно, подобные конференции стали традицией и в Юридическом институте, где с 2018 г. проводятся всероссийские научно-практические конференции по противодействию экстремизму и терроризму в России.

В рамках данной статьи предлагаем развивать указанные направления взаимодействия, в частности, с зарубежными сузами и вузами для преодоления региональной замкнутости образовательных учреждений. Считаем, что необходимо повышать роль образовательных учреждений в распространении культурных ценностей стран, их сохранении и обогащении с учетом высоких принципов культуры и взаимообогащении культур на постсоветском пространстве, в частности, содействовать сохранению и расширению применения русского языка как международного средства общения, осуществления образовательной и исследовательской деятельности, обмениваться опытом развития управления колледжами и вузами в условиях рыночных отношений и активной международной деятельности [12, с. 67].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анисимова И. А. Преступления террористической направленности: сравнительные аспекты. Барнаул : Изд-во Алт. ун-та, 2021. 122 с.

2. Абазов К. М. Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями // Вопросы безопасности. 2018. № 3. С. 1–9.

3. Овчинский В. С. Кибермафия становится глобальным игроком. URL: https://zavtra.ru/blogs/kibermafiya_stanovitsya_global_nim_igrokom.

4. Бутусова Л. И. К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. 2016. № 2. С. 48–52.

5. Чернядьева Н. А. Понятие «международный терроризм» в международных соглашениях ООН // Вестник СГЮА. 2012. № 4 (87). С. 1181–1187.

6. Greene A. Terrorism definition: one size fits all? // International and comparative law. 2017. № 66 (2). P. 411–440.

7. Рарог А. И. Уголовный кодекс России против терроризма // Lex Russica. 2017. № 4 (125). С. 155–178.

8. Абдулатипов А. М. Понятие информационного терроризма // Юридический вестник Дагестанского гос. ун-та. 2019. № 2. С. 105–111.

9. Авдеев В. А., Авдеева О. А. Преступность террористического характера и экстремистской направленности в РФ: состояние и тенденции правового регулирования // Российский судья. 2018. № 8. С. 18–23.

10. Обрывко Е. И., Стародубцева М. А., Саенко А. А. О некоторых аспектах повышения правовой культуры в вопросах профилактики экстремизма и идеологии терроризма в образовательной среде // Гуманитарные, социально-экономические и общественные науки. 2020. № 11. С. 81–84.

11. Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. № 1–1 (21). С. 41–45.

12. Цирлов В. Л. Правовые основы кибербезопасности Российской Федерации // Правовая информатика. 2013. № 4. С. 66–68.