УДК 343.9:007

Н. А. Зелинская

ПРЕСТУПНОСТЬ В КИБЕРПРОСТРАНСТВЕ: МЕЖДУНАРОДНО-ПРАВОВОЙ ДИСКУРС

На рубеже тысячелетий человечество, переживающее новую «информационную революцию», вступило в эпоху глобального информационного общества, технической базой которого является Интернет — глобальная информационная инфраструктура [1], создание которой открыло перед человечеством невиданные возможности, за которыми неизбежно следуют невиданные опасности. Информационная революция стремительно меняет мир, предоставляя человечеству принципиально новые решения и возможности во всех сферах его жизнедеятельности. Но вместе с очевидными благами информационная революция несет с собой и совершенно новые проблемы [2]. «В результате создания компьютерной сети и возникновения Интернета в конце XX — начале XXI века родился новый тип общества — общества информационного, в котором главным условием благополучия каждого человека и каждого государства становится знание, полученное благодаря беспрепятственному доступу к информации и умению работать с ней. Глобальная всемирная «паутина» — Интернет разрушила временные, пространственные и даже политические границы... тот факт, что ныне информационные потоки беспрепятственно преодолевают государственные границы, свободно циркулируют в информационном пространстве, а само это пространство значительно расширилось за счет эволюции вычислительной и информационной техники, позволяет сделать вывод о том, что воздействующий характер информации на различные сферы человеческой деятельности чрезвычайно увеличился. Таким образом, современное общество можно определить как общество, где происходит постоянное умножение, ускорение, уплотнение и глобализация информационных обменов» [3].

«Распространение по всему миру новых информационно-коммуникационных технологий породило множество различных преступлений, связанных с использованием компьютеров, что чревато угрозой не только для конфиденциальности, целостности или доступности компьютерных систем, но и для безопасности важнейших элементов инфраструктуры. Кроме того, технологические новшества порождают и непохожие друг на друга тенденции в области «криминальной инновации»; соответственно, несхожесть угроз, которые несут в себе преступления, связанные с использованием компьютеров, отражает различия, прослеживающиеся по всему спектру так называемого «разрыва в цифровых технологиях» [4].

В 2000 году Организация Объединенных Наций сообщила, что доступом к сетям располагало только примерно 4,5 % населения земного шара по сравнению с 44 % жителей Северной Америки и 10 % европейцев, в то время как в Азии, Африке и Южной Америке эти показатели колебались в пределах от 0,3 до 1,6 %. К 2005 году на региональном уровне более 98 % общемировых полос

АПДП. Вип. 67. 2 верстка. Іванова. 01.07.13

рабочих частот на базе интернет-протокола замкнуты на входе и выходе на Северную Америку. 99 % общемировых затрат на производство информационных технологий приходится на 55 стран [4, п. 18, 19].

Как отмечается в Докладе Генерального секретаря ООН «Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях» (2012), за последнее десятилетие произошел колоссальный рост в секторе информационно-коммуникационных технологий (ИКТ) и роли ИКТ в социально-экономическом развитии. Число абонентов мобильной телефонной связи во всем мире почти утроилось, достигнув 6 млрд. человек. Смартфоны превратили мобильные телефоны в универсальные устройства, дающие возможность работы с новыми приложениями и услугами. Во всем мире доля людей, пользующихся компьютером, как ожидается, вырастет с 1/50 в 2008 году до трети к 2020 году, в то время как число пользователей Интернета с 2005 года более чем удвоилось (до 2,5 млрд человек). Число подписчиков мобильной сотовой телефонной связи почти что сравнялось с числом жителей мира. Международный союз электросвязи (МСЭ) предсказывает, что к 2015 году мобильная сеть будет охватывать все населенные районы. Чуть меньше чем за десятилетие доступ к телефонии в большинстве развивающихся стран превратился из роскоши для богатых в факт жизни большинства [6, п. 3, 5].

Киберпреступность приобрела характер глобальной индустрии, доходы которой, согласно некоторым оценкам, превышают 1 триллион долларов США и быстро возрастают [7, 237]. По данным исследования, проведенного в 2011 году, глобальная киберпреступность каждый год обходится во всем мире в 114 млрд дол., а если учитывать вызываемые ею последствия — в два раза больше, что значительно превышает ущерб от международной торговли наркотиками [6].

Угрозы информационного общества, в том числе киберпреступность, воспринимаются как некий «информационный апокалипсис» [8]. Государственные и негосударственные субъекты с помощью информационно-коммуникационных технологий могут совершать действия против отдельных лиц, коммерческих предприятий, важнейшей промышленной инфраструктуры и правительств. Уникальные особенности информационной технологии облегчают ее использование в деструктивных целях. Слияние Интернета и других инфраструктур создает беспрецедентные возможности для выведения из строя телекоммуникационных сетей, электроснабжения, трубопроводов и нефтеперерабатывающих заводов, финансовых сетей. Применяемые для создания сбоев программные средства, по крайней мере, их базовые элементы доступны всем. Любой, кто обладает необходимыми навыками, может разработать более сложные подходы. Кроме того, эти средства быстро совершенствуются с учетом выявляемых новых уязвимых мест [9].

Мобильная телефония, социальные сети и сайты микроблогов существенно расширили круг информационных источников, доступных для людей, их воз-

можности выражать свое мнение и их способность координировать действия, в том числе политические протесты. Многие считают важной их роль в политических преобразованиях, которые произошли в ходе 2011 года, способствовав изменению отношений между гражданами и государством. Правительства многих государств уделяют серьезное внимание кибербезопасности, включая новые опасности, создаваемые киберпреступностью, включая подрыв социально-экономического порядка [6, п. 11, 13]. Преступность в киберпространстве не может не привлекать пристального внимания исследователей. Изучению этого феномена посвящены труды многих ученых, среди которых, в частности, могут быть названы Л. Азаров, Ю. Батурин, В. Быков, В. Вехов, А. Волеводз, В. Гавловский, В. Голубев, А. М. Дашян, Н. А. Жодзишский, В. Карчевський, А. Коновалов, В. Курушин, В. Машлыкин, В. Минаев, Л. Осипенко, Т. Тропина, В. Цимбалюк, И. Шинкаренко. Целью данной статьи является анализ актуальных аспектов проблемы противодействия киберпреступности, преимущественно в международно-правовом дискурсе.

Преступность информационного общества требует адекватного реагирования. Экспертами ООН отмечается, что происходящие изменения носят радикальный характер: технологические преобразования не только пронизывают среду, в которой мы живем, невиданным ранее образом связывая людей, объекты и информацию, но и представляют собой новое поколение угроз и факторов уязвимости в цифровой сфере, что вызывает необходимость кардинального пересмотра представлений о преступности в XXI веке [4, п. 15].

Глобальная доступность электронных и виртуальных услуг означает, что преступность в информационном пространстве естественным образом имеет транснациональное измерение [10]. В этих условиях нельзя не согласиться с тем, что важнейшим направлением информационной безопасности становится противодействие преступлениям, совершаемым в области использования электронно-вычислительных машин, систем и компьютерных сетей [11; 12]. Сдерживание киберпреступности является составной частью национальной кибербезопасности и стратегии зашиты важнейшей информационной инфраструктуры [13; 14]. На национальном уровне — это общая ответственность, требующая скоординированных действий со стороны правительственных организаций, частного сектора и граждан. На региональном и международном уровне это влечет за собой кооперацию и координацию усилий государств [15].

Проводимая в системе ООН интенсивная работа по концептуализации понятия «киберпреступность» и выработке согласованной политики сдерживания этой угрозы нашла отражение во многих документах, включая резолюции Генеральной Ассамблеи. С конца 80-х — начала 90-х годов прошлого века к этой проблеме неоднократно обращались «Группа Восьми», Совет Европы, Европейский Союз, Организация по безопасности и сотрудничеству в Европе, Содружество независимых государств, Содружество наций, Организация американских государств, Ассоциация государств Юго-Восточной Азии и Азиатско-Тихоокеанская ассоциация экономического сотрудничества (АТЭС), Шанхайская организация сотрудничества, Экономическое сообщество западноафриканских го-

сударств, Африканский союз, Интерпол, НАТО, ОДКБ, Международный союз электросвязи [16]. В частности, на саммите Организации по безопасности и сотрудничеству в Европе, состоявшемся в 2010 году в Астане, главы государств и правительств 56 стран — членов ОБСЕ приняли «Астанинскую юбилейную декларацию: на пути к сообществу безопасности», в которой подчеркнули необходимость добиться «большего единства целей и действий в противостоянии появляющимся транснациональным угрозам», назвав в их числе «киберугрозы» [17]. На Рабочем совещании ОБСЕ по всеобъемлющему подходу к повышению кибербезопасности и рассмотрению будущей роли ОБСЕ, которое проходило в Вене 9 и 10 мая 2011 года, обсуждались конкретные рекомендации по проведению последующей деятельности в рамках ОБСЕ. В резолюции «Общий подход ОБСЕ к укреплению кибербезопасности» Парламентской Ассамблеи ОБСЕ, принятой на двадцатой ежегодной сессии (Белград, 6–10 июля 2011 года) была признано, что угрозы, исходящие от киберпространства, и меры, направленные на повышение кибербезопасности, входят в число неотложных вопросов безопасности, волнующих государства и с озабоченностью отмечено, что угрозы, исходящие от киберпространства, постоянно эволюционируют и возрастают быстрыми темпами.

В рамках Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), которая прошла в два этапа: в Женеве в 2003 году и в Тунисе в 2005 году были приняты документы, которые оказали значительное влияние на формирование современной концепции «информационного общества». 12 декабря 2003 года в Женеве при проведении первого этапа Всемирной встречи была одобрена историческая Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» [18]. 16–18 ноября 2005 года в Тунисе во время проведения второго этапа Всемирной встречи на высшем уровне по вопросам информационного общества ее участники приняли «Тунисское обязательство», в котором говорится: «Мы …признаем необходимость эффективного противодействия проблемам и угрозам, возникающим в результате использования ИКТ, в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать негативное воздействие на целостность инфраструктуры в рамках отдельных государств в ущерб их безопасности. Необходимо предотвращать злоупотребление информационными ресурсами и технологиями в преступных и террористических целях и соблюдать права человека» [19]. В принятой 18 ноября 2005 года «Тунисской программе для информационного общества» подчеркивается важность уголовного преследования киберпреступности и содержится призыв к правительствам разработать необходимое законодательство [20].

Угрозы сетевым системам, образующим киберпространство, и передаваемой через них информации являются одной из серьезных глобальных проблем нашего времени. Известный украинский специалист в вопросах противодействия киберпреступности В. А. Голубев определяет «виртуальное пространство» — киберпространство — как «моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, собы-

тиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи» [21].

Как подчеркивает В. Н. Дремин, есть все основания утверждать, что современная информационная среда способствует воспроизводству преступности, а в связке явлений «информация — преступность» обнаруживается устойчивое системное взаимодействие. Существенным следствием развития информационной мегасреды является стремительно развивающийся процесс глобализации преступности. Несмотря на внешне различную природу этих социальных явлений, обнаруживаются их весьма жесткая связь и тенденция к ее укреплению [22–25].

В этих условиях особое значение приобретает вопрос о гармонизации национального материального уголовного права, поскольку взаимная правовая помощь, основывается, преимущественно, на принципе двойной криминализации, согласно которому преследуемое деяние должно быть уголовно наказуемым как в государстве, обращающемся за помощью, так и в государстве, оказывающем ее. Расследования в глобальных масштабах могут, как правило, проводиться лишь в отношении действий, влекущих за собой уголовную ответственность во всех затронутых ими странах [26]. Широко известен пример с компьютерным червем «Love Bug», созданным на Филиппинах в 2000 году, которым, как сообщалось, были заражены миллионы компьютеров по всему миру. При этом проведению следственных действий на месте мешало то, что на Филиппинах тогда отсутствовали надлежащие положения об уголовной ответственности за умышленную разработку и распространение вредоносного программного обеспечения [26].

Нельзя не принимать во внимание то обстоятельство, что уголовное законодательство развивалось на протяжении многих столетий, тогда как Интернет и киберпреступность — несколько десятилетий. Несмотря на то, что, как замечает А. Г. Волеводз, напоминающие компьютер устройства существуют со времен изобретения счетов, которые появились в 3500 году до нашей эры в Японии, Китае и Индии, а в 1623 году немецкий ученый Вильгельм Шикард создал первое аналоговое устройство, использовавшее ряд зубчатых колес, для арифметических исчислений [27, 13], очевидно, что компьютеры — порождение современности.

Принято считать, что история создания Интернета берет свое начало в 60-х годах. В 1962 году Дж. Ликлайдер изложил свою концепцию компьютерной сети «Galactic Network» (Галактическая сеть). Первым шагом к созданию Интернета стала коммуникационная сеть компьютеров ARPANet (Advanced Research Project Agency network — «Сеть Управления перспективных исследовательских программ»), созданная по заказу Министерства обороны США. В 1967 году Л. Робертс, глава компьютерного отдела ARPA, опубликовал предварительную схему структуры сети ARPAnet. В 1969 году выпущен первый документ Request for Comment (RFC) под названием «Host Software»

АПДП. Вип. 67. 2 верстка. Іванова. 01.07.13

(Программное обеспечение узла сети). Уже в 70-х годах прошлого века получил распространение термин «хакер», который позже стал применяться к компьютерным преступникам [28, 16–17, 20].

Эксперты выделяют несколько этапов развития компьютерной преступности. В 1960-х годах, когда появились первые транзисторные вычислительные системы и популярность компьютеров начала расти, уголовно наказуемым признавалось, главным образом, физическое повреждение компьютерных систем и хранящихся на них данных. В 1970-х годах произошел переход от традиционных имущественных преступлений к новым формам преступности, в частности, противоправному использованию компьютерных систем, способствовавший возникновению еще одной новой формы преступности — компьютерного мошенничества. В 1980-х годах популярность персональных компьютеров продолжала расти и впервые в истории управление многими важнейшими объектами инфраструктуры стало осуществляться при помощи компьютерных технологий. Одним из побочных эффектов распространения компьютерных систем стало повышение интереса к программному обеспечению и появление первых форм торговли «пиратскими» программными продуктами. Кроме того, появление компьютерных сетей позволило преступникам получать доступ к тем или иным компьютерным системам, не присутствуя при этом на месте преступления. Появление в 1990-е годы графического интерфейса (Всемирная сеть World Wide Web) и последовавший за этим стремительный рост числа пользователей Интернета привели к возникновению новых методов совершения преступных деяний. В первом десятилетии XXI века на передний план вышли новые, более изощренные методы совершения преступлений, такие как «фишинг», «атаки с использованием бот-сетей», а также новые методы использования технологий, в частности, речевая связь по Интернету (IP-телефония) (VoIP) и «облачные вычисления» («cloud computing»), которые затрудняют деятельность правоохранительных органов [29].

У. Зибер рассматривает шесть основных этапов формирования законодательства о борьбе с компьютерными преступлениями, принятого в разных странах начиная с 1970-х годов: a) защита данных и защита неприкосновенности частной жизни; b) уголовное законодательство о борьбе с экономическими преступлениями, связанными с использованием компьютеров; c) защита интеллектуальной собственности; d) защита от противозаконного и вредного контента; e) уголовно-процессуальное законодательство; и f) правовое регулирование защитных мер, таких как криптография и требования в отношении аутентификации [4, п. 37].

Компьютерные преступления многовариантны. «Мозаика противоправных деяний, которые связаны с Интернет и сферой высоких технологий, весьма обширна. Противоправный характер имеют как распространение вредоносных вирусов, взлом паролей, кража номеров кредитных карточек, так и распространение противоправной информации (от клеветы до материалов порнографического характера)» [30, 165]. Определение понятия «компьютерное преступление» или «преступление, связанное с использованием компьютеров» обсуж-

даются, как минимум, на протяжении последних 50 лет, однако до сих пор не имеет однозначной трактовки [31]. В интересующем нас контексте киберпреступностью, в самых общих чертах, называют преступность, которая имеет место в киберпространстве [30, 165]. Межправительственная группа экспертов, учрежденная Комиссией по предупреждению преступности и уголовному правосудию для проведения всестороннего исследования проблемы киберпреступности и ответных мер по борьбе с ней» отметила в своем Докладе (2011): «Компьютерная преступность и, более конкретно, киберпреступность — термины, используемые для обозначения конкретной категории преступных деяний. Связанные с этой категорией преступных деяний вызовы включают не только широкий круг уже подпадающих под эту категорию правонарушений, но и быстро формирующиеся новые методы совершения преступлений» [32, п. 10]. В материалах ООН эти термины охватывают любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде [33].

Исследования Т. Л. Тропиной показывают, что зарубежные ученые выделяют такие виды киберпреступлений, как «computer crimes», «computer-related crimes» и «computer-facilitated crimes». На основе этих исследований Т. Л. Тропина предложила следующую классификацию: 1) насильственные или иные потенциально опасные киберпреступления, посягающие на физическую безопасность, жизнь и здоровье человека; 2) преступления, посягающие на конфиденциальность информации — незаконный доступ к компьютерам или компьютерным системам без причинения ущерба информации; 3) деструктивные киберпреступления, заключающиеся в повреждении данных и посягающие на целостность данных и безопасность функционирования компьютерных систем; 4) преступления, посягающие на имущество, имущественные права, а также на право собственности на информацию и авторские права (Д. Деннинг объединяет эти преступления в группу с условным названием «хищения», хотя, как объясняет сам автор, хищение информации — это не хищение в традиционном смысле слова, поскольку информация при этом может остаться у ее владельца, и он не теряет возможности пользоваться ею); 5) преступления, посягающие на общественную нравственность; 6) преступления, посягающие на общественную безопасность; 7) иные киберпреступления — «computer-facilitated» (традиционные преступления, совершение которых компьютер или облегчает, или дает новые возможности для их совершения; в эту группу включено множество преступлений, таких как: реклама услуг проституции в сети Интернет (является преступлением не во всех государствах); незаконный оборот наркотиков с использованием сети Интернет; азартные игры в Интернете (как и проституция, не везде уголовно наказуемы); отмывание денег с помощью электронного перемещения; киберконтрабанда, или передача нелегальных товаров, например, шифровальных технологий, запрещенных в некоторых государствах, по сети Интернет и т.п. [34].

В предлагаемой классификации в первую группу выделены, как имеющие наибольшую опасность, насильственные киберпреступления, посягающие на физическую безопасность, жизнь и здоровье человека. Эта категория включает в себя: а) угрозу физической расправы; в) киберпреследование. Угроза физической расправы — действия, заключающиеся в давлении на психику жертвы путем передачи посланий, содержащих угрозы, посредством электронной почты. Цель преступления — причинение потерпевшему постоянного страха за его собственную жизнь или за жизнь дорогих ему людей (американские ученые иногда называют это правонарушение террористической угрозой, что, конечно, неверно). Киберпреследование — форма электронного преследования, которая зачастую сопряжена с явно выраженными или подразумеваемыми физическими угрозами, создающими чувство опасности у жертвы [34].

Деперсонализация преступного поведения в киберпространстве, создающая ощущение полной вседозволенности, нередко способствуют проявлению самых низменных побуждений у внешне социально благополучных людей, совершающих действия (угроза насилием, разращение детей и т.п.), на которые они не решились без той степени анонимности, которую дает Интернет. Криминализация угрозы физической расправы и других киберпреступлений, посягающих на физическую безопасность, жизнь и здоровье человека, с учетом способа совершения преступления как отягчающего обстоятельства, является существенным условием борьбы с безнаказанностью такого рода «респектабельных», но не менее опасных, чем уличные насильники, преступниками.

Совет Европы привлек внимание к транснациональному характеру компьютерных преступлений уже в 1976 году — на конференции по экономическим преступлениям. В 1989 году Европейский комитет по проблемам преступности одобрил Доклад экспертов по компьютерным преступлениям, в котором значительное внимание было уделено проблемам совершенствования материального уголовного права, связанным с новыми формами преступлений. В том же году Комитет министров принял рекомендацию № 89, признав важность гармонизации уголовного законодательства и практики в сфере борьбы с компьютерной преступностью (computer-related crime) [35]. За ней в 1995 году последовала вторая, касающаяся процессуальных аспектов проблемы. В феврале 1997 года Комитет Министров Совета Европы поручил новому комитету (Комитету экспертов по вопросам преступности в киберпространстве) подготовить свод юридических обязательств, рассмотрев в нем, в числе прочих, вопросы состава преступлений. Комитет подготовил 25 последовательных проектов текста. Через четыре года окончательный текст проекта был представлен Европейскому комитету по проблемам преступности, а затем передан на утверждение Комитету Министров Совета Европы [36]. Комитет Министров обратился в Парламентскую Ассамблею за заключением по проекту, который, с поправками, был принят на ее апрельской сессии 2001 года. Текст конвенции был одобрен на заседании Комитета Министров в ранге постоянных представителей 19 сентября 2001 года и принят министрами иностранных дел на заседании 8 ноября 2001 года.

23 ноября 2001 года в Будапеште Конвенция Совета Европы о киберпреступности (Convention on cybercrime) была открыта для подписания, а 1 июля 2004 года вступила в силу. Этот документ обязывает государства, являющиеся его сторонами, гармонизировать национальные законы в отношении определения основных преступлений. Согласно Конвенции, каждая сторона принимает меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву широкий круг деяний. В части 1 Конвенции («Материальное уголовное право») выделено четыре вида компьютерных преступлений: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; 2) правонарушения, связанные с использованием компьютерных средств; 3) правонарушения, связанные с содержанием данных; 4) правонарушения, связанные с нарушением авторского права и смежных прав, а также дополнительные виды ответственности и санкции (покушение, соучастие или подстрекательство к совершению преступления.

В 2007 году была открыта для подписания Конвенция Совета Европы о защите детей от эксплуатации и посягательств сексуального характера. Она содержит конкретные положения об уголовной ответственности за обмен детской порнографией, а также за умышленное получение доступа к детской порнографии с использованием информационных и коммуникационных технологий (п. 1(f) ст. 20). Поскольку в ходе переговоров по Конвенции не удалось достичь согласия о введении уголовной ответственности за расизм и распространение материалов ксенофобского содержания, в 2003 году был принят Дополнительный протокол к Конвенции о киберпреступности относительно криминализации деяний расистского и ксенофобского характера, совершаемых с помощью компьютерных систем (Additional protocol to the Convention on cibercrim, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems) [37]. Протокол содержит обязательства относительно криминализации следующих деяний: распространение расистских и ксенофобских материалов посредством компьютерных систем (ст. 3); мотивированная угроза расизма и ксенофобии через компьютерную систему совершения серьезного уголовного преступления, как определено ее внутренним правом, в отношении лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов (ст. 4); публичное расистское и ксенофобское оскорбление через компьютерную систему (ст. 5); распространение или обеспечение доступа для общественности через компьютерную систему материала, который полностью отрицает или чрезвычайно умаляет отрицательные последствия, одобряет или оправдывает действия, являющиеся геноцидом или преступлениями против человечества, как определено международным правом и как это признано окончательными и обязательными решениями Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 года, или любого другого международного суда, образованного согласно соответствующим междуна-

родным документам и юрисдикция которых признана стороной Протокола (ст. 6). Как видим, в рамках Совета Европы формируется значительный массив международно-правовых стандартов криминализации киберпреступлений. Законодательсво Украины должно быть приведено в полное соотвествие с формулировками договоров, участниками которых является наше государство.

Л. А. Осипенко справедливо подчеркивает: «Надгосударственный характер глобальных сетей объективно требует развития международно-правового регулирования в этой области. В глобальном информационном пространстве уголовно-правовая политика каждого государства оказывает непосредственное влияние на криминологическую ситуацию в целом. Присутствие в глобальных сетях национальных сегментов, в которых не криминализированы определенные действия, приводит к тому, что преступники активно «осваивают» эти сегменты» [38, 179].

Преступность в сфере киберпространства наглядно демонстрирует давно отмеченную закономерность, состоящую в том, что преступление следует за открывающимися возможностями, заполняя открывающиеся «ниши». В отношении киберпреступлений основная проблема для всех государств состоит в том, чтобы обеспечить соответствие уголовных законов постоянно меняющимся формам преступности [5, 3]. Как известно, одним из практических последствий сетевой архитектуры Интернета является то, что преступники далеко не всегда находятся в том месте, где ими совершаются киберпреступления. Вследствие транснационального характера киберпреступности борьба с этим явлением требует эффективных и скоординированных усилий всех стран. Одной из ключевых задач в деле борьбы с киберпреступностью является предотвращение создания «безопасных убежищ» для киберпреступников [32, п. 51].

Эффективное международное сотрудничество в целях предотвращения создания убежищ требует согласованного подхода к законодательству. Необходимо установление новых составов преступлений, если соответствующие деяния не были признаны уголовно наказуемыми в действующем законодательстве [32, п. 23, 24]. Принятие государствами соответствующего законодательства по борьбе со злоупотреблением информационными и коммуникационными технологиями в преступных целях, включая действия, призванные воздействовать на целостность важнейших национальных информационных инфраструктур, является центральным пунктом для достижения глобальной кибербезопасности. Поскольку угрозы могут исходить из любой точки мира, эта задача, по своей природе, является международной и требует международного сотрудничества. Чрезвычайно важно, чтобы страны гармонизировали свои правовые основы для борьбы с киберпреступностью [39].

Формирование соответствующего угрозе, эффективного и в достаточной мере унифицированного в соответствии международными стандартами национального уголовного законодательства в отношении киберпреступлений является, безусловно, сверхсложной задачей [40–42]. Специалисты отмечают, что «когда государства попытались адаптировать нормы, разработанные для вещественных объектов, к неосязаемому и эфемерному миру электронных объектов, воз-

ник целый ряд вопросов. При криминализации действий, связанных с компьютерными технологиями, следует проявлять осторожность, чтобы не допустить отнесения правомерных деяний к разряду криминальных. При модернизации уголовного законодательства необходима осмотрительность при отделении общего от частного. Возможно, что слишком конкретно сформулированные положения могут устареть с появлением новых технологий. Соответственно, желательно использовать «технологически нейтральные» термины» [43].

Потребность в международно-правовых стандартах криминализации обусловлена необходимостью стимулировать установление уголовно-правового запрета и гармонизировать национальное законодательство. Внутригосударственное право многих государств в целом имеет значительную степень сходства относительно большинства традиционных видов транснациональных преступлений, однако новые виды преступности требуют выработки четких согласованных определений. В вопросах борьбы с киберпрестностью вопрос гармонизации уголовно-правового запрета приобретает особую значимость.

Киберпространство по своей природе глобально. Обеспечение кибербезопасности, соблюдение прав человека и защита важнейшей информационной инфраструктуры требуют от государства значительных усилий как на национальном, так и на международном уровнях [44]. Адекватным ответом на угрожающие масштабы и прогрессирующий рост преступности в киберпространстве должна стать дальнейшая глобализация правового пространства. Несмотря на очевидную сложность разработки и принятия универсальной конвенции по борьбе с киберпреступностью, решение этой проблемы является приоритетной задачей мирового сообщества.

Литература

1. Рекомендации Международной академии связи по Глобальному информационному обществу // International Telecommunication Academy. WSIS-03/GENEVA/C/0003(2003).
2. Чернов А. А. Становление глобального информационного общества. Проблемы и перспективы / А. А. Чернов. — М. : Изд.-торг. корпорация «Дашков и К°», 2003. — С. 49, 82.
3. Рассолов И. М. Право и киберпространство / И. М. Рассолов. — М. : Моск. бюро по правам человека, 2007. — 248 с.
4. Организация Объединенных Наций. Одиннадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Семинар-практикум 6: Меры по борьбе против преступлений, связанных с использованием компьютеров : справочный документ. — Док ООН. A/CONF. 203/14.
5. Clough J. Principles of Cybercrime / J. Clough. — Cambridge : Cambridge University Press, 2010. — P. 5.
6. Организация Объединенных Наций. Генеральная Ассамблея. Экономический и Социальный Совет. Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях : докл. Ген. секретаря. 12 марта 2012. — Док. ООН. A/67/66-E/2012/49.
7. Kshetri N. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives N / N. Kshetri. — Heidelberg ; London : Springer, 2010. — 251 p.
8. Машлыкин В. Г. Реалии «информационного апокалипсиса»: киберпреступность, кибертерроризм, кибероружие / В. Г. Машлыкин, А. М. Коновалов // Доклады Института Европы. № 111. — М. : Рос. акад. наук, Ин-т Европы, 2003. — С. 28–35.
9. Организация Объединенных Наций. Генеральная Ассамблея. Достижения в сфере информа-

тизации и телекоммуникаций в контексте международной безопасности : докл. Ген. секретаря. 15 июля 2011. — Док. ООН A/66/152. — С. 18, 19.
10. Дефицит международного сотрудничества позволяет киберпреступности оставаться безнаказанной. Информационный бюллетень № 8 [Электронный ресурс] // Vienna International Centre. — Режим доступа : www.unis.unvienna.org.
11. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями : монография / В. А. Голубев. — Запорожье : ГУ «ЗИГМУ», 2003.
12. Голубев В. А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : учеб. пособие / В. А. Голубев, В. Д. Гавловский, В. С. Цимбалюк ; под общ. ред. Р. А. Калюжного. — Запорожье : ГУ «ЗИГМУ», 2002.
13. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. — М. : Юрид. лит., 1991.
14. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. — М. : Новый Юрист, 1998.
15. Понимание киберпреступности: руководство для развивающихся стран. Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратегии. Сектор развития электросвязи МСЭ. — Женева, 2009. — С. 11.
16. Азаров Л. С. Проблемы усовершенствования ответственности за «компьютерные» преступления: концептуальный подход // Уголовное право: стратегия развития в XX1 веке. — М. : Проспект, 2005. — С. 304–307.
17. Организация по безопасности и сотрудничеству в Европе 3 December 2010. Встреча на высшем уровне. Астана, 2010 год. Астанинская юбилейная декларация: на пути к сообществу безопасности. — Док. SUM.DOC/1/10. — П. 9.
18. First Phase of the WSIS (10–12 December 2003, Geneva). Geneva Declaration of Principles. WSIS-03/GENEVA/DOC/0004.
19. Second Phase of the WSIS (16–18 November 2005, Tunis) / Tunis Commitment WSIS-05/TUNIS/DOC/7. — Para. 15.
20. Second Phase of the WSIS (16–18 November 2005, Tunis) Tunis Agenda for the Information Society WSIS-05/TUNIS/DOC/6 (rev. 1) — Para. 40.
21. Голубев В. А. «Кибертерроризм» — миф или реальность? [Электронный ресурс] / В. А. Голубев ; Центр исслед. проблем компьютерной преступности. — 2001–2002. — Режим доступа : www.crime-research.org.
22. Дрёмин В. Н. Глобализация информационных систем как фактор глобализации преступности // Інформаційни технології та безпека : зб. наук. пр. — К., 2002. — Вип. 1. — С. 54–61.
23. Дрёмин В. Н. Интернет как предмет информационной криминологии и фактор воспроизводства преступности // Актуальні проблеми політики : зб. наук. пр. / голов. ред. С. В. Ківалов. — О., 2002. — Вип. 15. — С. 287–293.
24. Дрёмин В. Н. К вопросу о предмете информационной криминологии // Інформаційні технології та безпека : зб. наук. пр. — К., 2003. — Вип. 3. — С. 52–62.
25. Дрёмин В. Н. Информационная мегасреда в механизме криминализации общества // Актуальні проблеми держави і права : зб. наук. пр. / редкол.: С. В. Ківалов (голов. ред.) [та ін.]. — О., 2006. — Вип. 27. — С. 203–208.
26. Док. ООН. A/CONF.213/9. — П. 15, 16.
27. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. — М. : Юрлитинформ, 2001.
28. Дремлюга Р. И. Интернет-преступность : монография / Р. И. Дремлюга. — Владивосток : Изд. Дальневост. ун-та, 2008. — 240 с.
29. Док. ООН. UNODC/CCPCJ/EG.4/2011/2. — П. 12.
30. Дашян М. С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет / М. С. Дашян. — Wolters Kluwer Russia, 2007.
31. Тропина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов международной конференции «Информационные технологии и безопасность». — К. : Нац. акад. наук Украины, 2003. — Вып. 3. — С. 173–181.
32. Док. ООН. E/CN.15/2011/19. — П. 10.
33. Док. ООН. A/ CONF. 187/10.
34. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т. Л. Тропина. — Владивосток, 2007. — С. 8–17.
35. Council of Europe Committee of Ministers Recommendation No. R (89) 9 of the Committee of

Ministers to member states on Computer-related crime (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies) [Электронный ресурс]. — Режим доступа : wcd.coe.int/com.instranet.InstraServlet?command= com.instranet.CmdBlobGet&InstranetImage= 610660&SecMode=1&DocId=702280&Usage=2.
36. Док. ООН. E/CN.15/2001/4. — П. 4.
37. Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [Электронный ресурс]. — Режим доступа : www.conventions.coe.int/Treaty/EN/Treaties/Html/189.htm.
38. Осипенко Л. А. Борьба с преступностью в глобальных компьютерных сетях : международный опыт / Л. А. Осипенко. — М., 2004.
39. Понимание киберпреступности: руководство для развивающихся стран. Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратегии. Сектор развития электросвязи МСЭ. — Женева, 2009. — С. 4.
40. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : монография / И. Р. Шинкаренко, В. О. Голубев, Н. В. Карчевський, И. Ф. Хараберюш ; МВД Украины, Донец. юрид. ин-ту Луган. гос. ун-та внутр. дел. — Донецк : РВВ ЛДУВС, 2007.
41. Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошев, В. Черкасов // Уголовное право. — 2003. — № 3. — С. 9–11.
42. Вехов В. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. — 2004. — № 4. — С. 15–17.
43. Док. ООН. — П. 37, 39–41.
44. Док. ООН A/66/152. — С. 10.

Аннотация

Зелинская Н. А. **Преступность в киберпространстве: международно-правовой дискурс.** — Статья.

В статье рассматриваются актуальные проблемы международного сотрудничества в противодействии киберпреступности. Автор акцентирует внимание на том, что адекватным ответом на прогрессирующий рост преступности в киберпространстве должна стать дальнейшая глобализация правового пространства. Несмотря на очевидную сложность разработки и принятия универсальной конвенции по борьбе с киберпреступностью, решение этой проблемы является приоритетной задачей мирового сообщества.

Ключевые слова: международное сотрудничество, киберпреступность, киберпространство, глобализация правового пространства.

Анотація

Зелінська Н. А. **Злочинність у кіберпросторі: міжнародно-правовий дискурс.** — Стаття.

У статті розглядаються актуальні проблеми міжнародного співробітництва у протидії кіберзлочинності. Автор акцентує увагу на тому, що адекватною відповіддю на прогресуюче зростання злочинності у кіберпросторі повинна стати подальша глобалізація правового простору. Незважаючи на очевидну складність розробки й прийняття універсальної конвенції щодо боротьби з кіберзлочинністю, вирішення цієї проблеми є пріоритетним завданням світової спільноти.

Ключові слова: міжнародне співробітництво, кіберзлочинність, кіберпростір, глобалізація правового простору.

Summary

Zelinskaya N. A. **Crime in the cyberspace: international legal discourse.** — Article.

The actual issues of the international cooperation in cybercrime counteraction are approached in the article. The author emphasizes that further legal space globalization should become an adequate answer to the progressing growth of criminality in the cyberspace. Despite obvious complexity in developing and approving the universal convention on cybercrime counteraction, overcoming this challenge is a priority task of the global community.

Keywords: international cooperation, cybercrime, cyberspace, legal space globalization.

АПДП. Вип. 67. 2 верстка. Іванова. 01.07.13