FORUM INCOGNITA

Борьба с киберпреступностью: возможна ли разработка универсального механизма?

Татьяна Тропина*

Эффективная борьба с киберпреступностью требует гармонизации уголовного законодательства на международном уровне и выработки комплекса процессуальных мер для сотрудничества при расследовании преступлений. В настоящей статье автор анализирует международные подходы к гармонизации законодательства в этой сфере, а также причины отсутствия международного инструмента, регулирующего борьбу с киберпреступностью, который был бы принят большинством государств мира.

Киберпреступность, компьютерная преступность, информационная безопасность

The transborder nature of cybercrime problem calls for harmonisation of substantive legal frameworks on the international level and for the development of a set of procedural measures allowing effective cooperation in crime investigation in digital environment. This article analyses existing international approaches to harmonisation of cybercrime legislation and examines the reasons why there is still no universally accepted international treaty on cybercrime.

Cybercrime, computer crime, cybersecurity

Введение

Анонимность, простота использования, быстрота передачи информации, возможность быстрого охвата широкой аудитории — информационно-коммуникационные технологии изменили общество, открыв новые возможности для ведения бизнеса и для повседневных коммуникаций. В своём развитии современное общество полагается на глобальные информационные сети, и, как следствие, зависит от них. Вместе с зависимостью растёт уязвимость общества[1].

Когда сеть Интернет создавалась как неиерархическая структура без «головного» центра управления, разрушив который можно было бы парализовать её работу, вряд ли кто-то мог представить масштабы развития проекта, изначально использовавшегося в военных и научных целях[2]. Основной целью создания Интернета была устойчивость к атакам извне, и разработчики не могли предвидеть, что с ростом использования информационных технологий неразработанные механизмы контроля и защиты от атак внутри сети станут одной из глобальных проблем

* *Тропина Татьяна Львовна* — старший научный сотрудник Института зарубежного и международного уголовного права им. Макса Планка (г. Фрайбург, Германия), кандидат юридических наук (e-mail: tatiana.tropina@gmail.com).

[1] *Bekkers V., Thaens M.* Interconnected networks and the governance of risk and trust // Information Polity. 2005. Vol. 10. P. 37–48.

[2] *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff.* A Brief History of the Internet. URL: www.isoc.org/internet/history/brief.shtml (дата обращения: 05.01.2013).

информационного сообщества[3], что децентрализованная структура сети и отсутствие национальных границ в киберпространстве предоставит возможности для роста преступности и будет сдерживать разработку механизмов социального и правового контроля в сфере использования информационных сетей для совершения преступлений.

С момента, когда сеть Интернет стала доступна широкому кругу пользователей и до момента, когда уязвимость информационных технологий стала очевидной, прошло достаточно времени, чтобы разрыв между развитием цифровых технологий и разработкой механизмов их регулирования создал правовой вакуум. Этот разрыв не уменьшается и по сей день, обусловливая появление новых проблем защиты информации и пользователей от посягательств, новых способов совершения киберпреступлений, а также их рост. При этом проблема киберпреступности состоит из двух компонентов. Во-первых, появляются новые преступления, такие как нарушение целостности, доступности и конфиденциальности электронных данных, объектом которых являются новые охраняемые законом интересы, возникшие в связи с развитием информационных технологий. Во-вторых, глобальные информационные сети используются для совершения деяний, ответственность за которые уже предусмотрена уголовным законодательством многих государств, таких как хищение имущества, распространение детской порнографии, нарушение тайны частной жизни, и др.[4]

В последние годы информационные сети развиваются слишком быстро, чтобы существующие механизмы контроля успевали реагировать на новые проблемы. К основным угрозам, связанным с развитием информационных технологий и распространением сети Интернет, в настоящее время эксперты относят «облачную» обработку данных[5], автоматизацию атак, использование мобильных устройств для подключения к сети Интернет, уязвимость персональной информации в социальных сетях[6], распространение так называемого «информационного оружия», примером которого является вирус Stuxnet, разработанный, по мнению специалистов, для атак на ядерную промышленность Ирана, но при этом причинивший немалый ущерб инфраструктуре многих других стран[7]. И это далеко не полный перечень последних тенденций в области развития глобальной информационной сети, на которые правовое регулирование пока не может найти адекватного ответа.

Киберпреступность как явление возникла всего несколько десятилетий назад, однако за короткое время с развитием информационных технологий феномен противоправных деяний в киберпространстве успел превратиться в глобальную проблему, поставив под угрозу не только отдельных пользователей, но и информационную безопасность целых государств. С того момента, как государство включается в информационный обмен посредством сети Интернет, оно само и его граждане становятся уязвимыми для посягательств из любой точки земного шара. Более того, как показывает пример атак на ядерное производство Ирана, даже отключение особо важных для государства объектов от глобальных информационных сетей не защищает их от возможных атак: вирус Stuxnet, например, распространялся через портативные накопительные устройства, подключаемые к компьютеру через порт USB[8].

---

[3] *Gercke M.* Understanding Cybercrime: Guide for Developing Countries. ITU, 2011.

[4] *Goodman M.* International Dimensions of Cybercrime // Ed. by S. Ghosh and E. Turrini. Cybercrimes: A Multidisciplinary Analysis. Berlin, Heidelberg, 2010.

[5] Облачная обработка данных, или облачные вычисления – так называемый "*Cloud Computing*" включает систему обработки данных, при которых доступ к файлам, программному обеспечению и вычислительным сервисам производится через Интернет, а не с локального персонального компьютера. Иными словами, все данные хранятся не на локальном диске пользователя, а в «облаке». Преимущество этого способа обработки данных для пользователей в том, что доступ к ним можно получить с любого компьютера, а также в том, что пространство и ёмкость для хранения данных не ограничено возможностью локального компьютера. С точки зрения расследования киберпреступлений, облачные вычисления создают проблемы при расследовании, поскольку иногда даже операторы "облачного" сервиса не могут точно сказать, на каком сервере и в какой стране находятся данные.

[6] См.: *McAfee*. Threats Predictions, 2011. URL: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf (дата обращения: 05.01.2013).

[7] *Kerr P. , Rollins J., Theohary C.* The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, CRS Report for Congress. URL: http://www.fas.org/sgp/crs/natsec/R41524.pdf (дата обращения: 05.01.2013).

[8] *Orrey K.* A Survey of USB Exploit Mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective. URL: http://www.vulnerabilityassessment.co.uk/education/whitepaper.pdf (дата обращения: 05.01.2013).

Единственный способ полностью обезопасить особо важные объекты для функционирования общества — это полностью отключить сеть Интернет не только от объектов защиты, но и во всём государстве в целом. Разумеется, это невозможно, поскольку информационные технологии играют важнейшую роль в функционировании общества. Но, учитывая транснациональный характер сети Интернет и отсутствие внутри неё государственных границ, меры по предотвращению, расследованию и пресечению киберпреступлений не могут работать в глобальной информационной среде только на национальном уровне. Именно поэтому борьба с киберпреступностью изначально является международной проблемой.

Преступность в глобальных информационных сетях: факторы риска и проблемы борьбы

Преступность в информационных сетях, в частности, в сети Интернет — комплексная проблема, понимание которой невозможно без анализа технологических и правовых проблем регулирования информационных сетей. Именно анализ взаимосвязи между техническими характеристиками сети и обусловленными этими характеристиками правовыми сложностями, с которыми сталкиваются законодатели и правоохранительные органы, является первым шагом к возможной выработке механизмов адекватного реагирования на развитие и рост киберпреступности.

Популярность сети Интернет в сочетании с появлением доступных и дешёвых технологий для развёртывания сети передачи данных не только в индустриальных государствах, но и в развивающихся странах, привела к росту пользователей до 2,3 миллиардов в 2011 году[9]. С увеличением числа пользователей возрастают, в первую очередь, два фактора риска. Во-первых, как уже было сказано выше, увеличивается зависимость общества от информационных технологий, что, в свою очередь, обусловливает его уязвимость к различного рода информационных посягательствам. Во-вторых, с ростом количества тех, кто использует Интернет, растёт потенциальная возможность стать жертвой использования информационных технологий в преступных целях[10]. При этом совершение преступления в сети Интернет не требует больших усилий и затрат — достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. В настоящее время не требуется даже глубоких технических познаний: в Интернете существуют специальные форумы, на которых можно приобрести программное обеспечение для совершения преступлений, украденные номера кредитных карт и идентификационные данные пользователей, а также воспользоваться услугами по помощи в совершении электронных хищений и атак на компьютерные системы как в целом, так и на отдельных стадиях совершения преступлений[11].

Компьютерные данные за несколько секунд могут быть переданы из одной точки мира в другую посредством глобальных компьютерных сетей. Более того, практически любая передача данных в сети обычно включает несколько стран, поскольку трансфер Интернет-данных обычно строится на принципе оптимального маршрута, когда информация разбивается на части и идёт по наиболее удобным и доступным каналам[12]. Контролировать передачу данных, с учётом их объёма и количества пользователей, очень трудно, если не невозможно[13]. Преступник, потерпевший, сервер с необходимой информацией могут находиться в разных странах и на разных континентах, что требует сотрудничества правоохранительных органов нескольких стран при расследовании преступления.

---

[9] См.: ITU ICT Facts and Figures 2011. Page 1. URL: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf (дата обращения: 05.01.2013).

[10] *Gercke M.* Understanding Cybercrime: Guide for Developing Countries. ITU, 2011.

[11] См.: *Ben-Itzhak Y.* Organized Cybercrime // ISSA Journal. October 2008. URL: https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf (дата обращения: 05.01.2013); ESET, 2010, Cybercrime Coming of Age white paper, January 2010. URL: http://go.eset.com/us/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf (дата обращения: 05.01.2013).

[12] *Comer D.* Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture. Purdue University, 1995.

[13] *Sieber U.* Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law // Delmas-Marty M, Pieth M & Sieber U. (eds). Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de legislation comparée, 2008. P. 127–202.

Развитие автоматизации позволяет увеличить скорость передачи данных и совершать множественные преступления без особых финансовых и временных затрат[14]. Более того, автоматизация позволяет преступникам аккумулировать большую финансовую прибыль путём хищения небольших сумм у тысячи пользователей, что создаёт проблемы обнаружения преступлений (владелец банковского счета может просто не заметить исчезновение финансовых средств) и возбуждения уголовных дел. Например, если тот же владелец банковского счета обратится с заявлением о пропаже незначительной суммы, правоохранительным органам достаточно трудно оценить масштаб деятельности тех, кто совершил хищение, поскольку ущерб, причинённый одному потерпевшему, очень мал, в то время как правонарушители путём аккумуляции этих небольших сумм могут добиться внушительной прибыли[15].

Анонимность сети Интернет, уязвимость беспроводного доступа и использование прокси-серверов дают возможность существенно затруднить обнаружение преступников: для совершения преступления может использоваться «цепочка» серверов[16], преступления могут быть совершены путём выхода в Интернет через точки общего доступа, такие, как Интернет-кафе, технологии позволяют также «взломать» доступ в чужую беспроводную сеть Wi-Fi. Таким образом, существует достаточно способов затруднить расследование преступлений[17].

Расследование преступлений в глобальной сети обычно требует быстрого анализа и сохранения электронных данных, которые очень уязвимы по своей природе и могут быть быстро уничтожены. В этой ситуации традиционные механизмы правовой взаимопомощи и принцип суверенитета, одним из проявлений которого является то, что только правоохранительные органы государства могут производить следственные действия на его территории, требуют множество формальных согласований, делая расследование транснациональных киберпреступлений проблематичным. Помимо сотрудничества правоохранительных органов, которое требует временных затрат и соблюдения множества формальностей, встаёт также вопрос о соблюдении фундаментального принципа *nullum crimen, nulla poena sine lege*[18], когда необходима двойная криминализация деяния как в стране, с территории которой действовал правонарушитель, так и в государстве, где находится потерпевший. Разница в криминализации деяний, различия в определении тяжести совершенного деяния, особенно в сфере религиозных преступлений и преступлений против общественного порядка, в области нелегального контента, значительно затрудняют процесс сотрудничества правоохранительных органов, иногда делая его невозможным[19].

Таким образом, эффективный контроль негативных явлений в кибепространстве, таких как преступность, требует гораздо более интенсивного международного сотрудничества, чем существующие меры по борьбе с любыми другими формами транснациональной преступности. Именно поэтому помимо гармонизации уголовно-правовых норм требуется гармонизация процессуальных инструментов и выработка новых механизмов международного сотрудничества.

Законодательство по борьбе с киберпреступностью: проблемы гармонизации и универсального похода

Гармонизация уголовного и уголовно-процессуального законодательства, а также соз-

---

[14] *Gercke M.* Understanding Cybercrime: Guide for Developing Countries. ITU, 2011.

[15] *Wall D. S.* Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace // Police Practice and Research, 8:2, 1, 2007. P. 191.

[16] *Lovet G.* Fighting Cybercrime: Technical, Juridical and ethical Challenges. Virus Bulletin Conference [online]. September, 2009. P. 63–76. URL: http://www.fortiguard.com/sites/default/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf (дата обращения: 05.01.2013).

[17] См. Casey, Error, Uncertainty, and Loss in Digital Evidence // International Journal of Digital Evidence. 2002. Vol. 1. Issue 2. URL: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDEC80B5E5B306A85C4.pdf (дата обращения: 05.01.2013).

[18] *Hall.* Nula Poena sine Lege // Yale Law Journal. 1937. Vol. 47. P. 165.

[19] *Sieber U.* Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law // Delmas-Marty M., Pieth M. & Sieber U. (eds). Les chemins de l'HarmonisationPénale/Harmonising Criminal Law, Collection de L'UMR de DroitComparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008.

дание эффективной системы правовой взаимопомощи путём принятия универсального соглашения, регулирующего борьбу с киберпреступностью на глобальном уровне, в настоящее время становится все более затруднительным. И, как ни странно, одним из препятствий являются уже существующие региональные и международные механизмы гармонизации законодательства в области борьбы с киберпреступностью, точнее, их фрагментарность и «конкуренция» между уже существующими региональными подходами и попытками выработать инструменты, которые выйдет за пределы регионального охвата.

«Мозаичность» развития международных инструментов в этой области особенно явно заметна в настоящее время, через десять лет после принятия первого соглашения, призванного установить глобальные стандарты в борьбе с преступностью в информационном пространстве — Конвенции Совета Европы по киберпреступности (ETS № 185), подписанной в Будапеште 23 ноября 2001 года[20]. К сожалению, документ, который был призван стать эталоном для национальных законодателей и выйти на глобальный уровень, поскольку являлся первым международным документом в этой области, справился лишь до определённой степени с первой из задач, но при этом не только не стал универсальным решением проблемы объединения усилий в борьбе с киберпреступностью в силу ряда недостатков, но ещё и привёл к разрозненности подходов к гармонизации законодательства.

Конвенция Совета Европы о киберпреступности

Следует оговориться, что значение Конвенции Совета Европы в борьбе с преступностью в кибепространстве трудно переоценить — именно этот документ заложил основные принципы и механизмы международного сотрудничества, определил границы криминализации, установил универсальные рамки для развития национальных норм и международных инструментов в этой области. Однако Конвенция Совета Европы страдает серьёзными недочётами, которые делают невозможным применение этого инструмента для гармонизации законодательства о киберпреступности на общемировом уровне. В частности, проблемы Конвенции заключаются в следующем:

— *отсутствие эффективного механизма имплементации и отсутствие мониторинга имплементации*

Конвенция предусматривает необходимость имплементации её положений на национальном уровне. Логично было бы предполагать, что более 30 стран, ратифицировавших Конвенцию, должны иметь сравнимые нормы, регулирующие ответственность за кибепреступления, а также процессуальные механизмы, позволяющие расследовать данный вид преступлений. Однако анализ законодательства участников Конвенции показывает, что этого до сих пор не произошло[21]. Более того, Совет Европы никогда не проводил полную оценку имплементации норм документа в национальное законодательство стран и его соответствия правовых норм обязательствам по конвенции.

Когда оценка имплементации отдельных положений Конвенции всё-таки была произведена в 2009 году, исследования показали, что принятые меры значительно разнятся. Например, не все государства — участники создали подразделения по борьбе с кибепреступностью, так называемые «контакт-центры 24/7», способные быстро реагировать на запросы правоохранительных органов других стран и оказывать взаимопомощь при расследовании киберпреступлений, несмотря на обязательства, принятые в соответствии со статьёй 35 Конвенции[22].

— *«региональность» инструмента, фокус на развитых странах*

В то время, когда Конвенция о киберпреступности находилась в процессе разработки, количество пользователей сети Интернет в развитых государствах превышало число тех, кто использовал информационные сети в странах развивающихся. Однако в 2005 году развивающиеся страны обогнали страны с

[20] Текст документа: Convention on Cybercrime. URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (дата обращения: 05.01.2013).

[21] *Gercke M.* Ten Years Convention on Cybercrime // Computer Law Review International. 2011. Vol. 15. Issue 5.

[22] См. Council of Europe. The Functioning of 24/7 Contact Points for Cybercrime. Discussion Paper. URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/567_24_7report4public_april09a.pdf (дата обращения: 05.01.2013).

развитой инфраструктурой по количеству пользователей Интернета[23]. С точки зрения развивающихся государств, Конвенция о киберпреступности ориентирована больше на страны с развитой инфраструктурой.

Развивающиеся государства, которые в настоящее время активно приглашаются присоединиться к Конвенции, разумеется, не были привлечены к процессу разработки её положений. Эта проблема имеет скорее политический, чем правовой характер, но информационная безопасность является не только юридическим, но и политическим вопросом. Совет Европы позиционирует Конвенцию о киберпреступности как подход, который выходит за пределы Европы и уже является глобальным (тот факт, что Конвенция подписана странами Азии и Америки, конечно, свидетельствует об этом). Однако то, что за 10 лет существования Конвенции ни одна развивающаяся страна не ратифицировала это соглашение, а также то, что только семь государств из 146 стран-членов ООН, не подписавших Конвенцию, присоединились к Соглашению, свидетельствует об ограниченных возможностях евроцентристского подхода[24]. Неудивительно, что именно развивающиеся страны делают заявления о необходимости именно универсального, а не регионального инструмента, разработка которого должна осуществляться под эгидой ООН и включать в процесс согласования все государства-члены. Так, в процессе подготовки XII Конгресса ООН по Предотвращению преступности и обращению с правонарушителями, страны Латинской Америки[25], Западной Азии[26], Африки и других развивающихся регионов заявили о необходимости принятия универсального соглашения по вопросам борьбы с киберпреступностью.

– отсутствие комплексного подхода, пробелы и спорные нормы

Одной из основных задач, которую ставили перед собой разработчики Конвенции Совета Европы о киберпреступности, была разработка подхода, охватывающего все возможные области борьбы с киберпреступностью. Однако по сравнению с другими региональными соглашениями, такими как Модельный Закон о компьютерных преступлениях Содружества Наций 2002 года[27], документами Европейского Союза (например, Директива ЕС 2000/31/ЕС об электронной коммерции[28]) Конвенция Совета Европы не охватывает важные области регулирования, включающие, например, сбор и представление электронных доказательств, ответственность Интернет-провайдеров. Процессуальные инструменты, предлагаемые Конвенцией, не решают также такие проблемы, как перехват коммуникаций в области передачи голосовых данных через сеть Интернет (Voice-over-IP) и использование программного обеспечения удалённого отслеживания при расследовании преступлений, что создаёт правовые лакуны и различия между подходами в использовании данных инструментов[29].

Кроме того, Конвенция не решает ни один из спорных вопросов юрисдикции, поскольку не создаёт новых подходов отнесения расследования и преследования преступлений в информационных сетях к компетенции того или иного государства, ограничиваясь традиционными положениями об установлении юрисдикции. С учётом трансграничности сети Интернет традиционные подходы к проблеме юрисдикции достаточно проблематичны в реальном расследовании преследовании компьютерных посягательств. До сих пор идут споры, с учётом каких факторов решается

---

[23] Development Gateway's Special Report, Information Society – Next Steps? 2005. URL: http://topics.developmentgateway.org/special/informationsociety (дата обращения: 05.01.2013).

[24] *Gercke M.* Ten Years Convention on Cybercrime // Computer Law Review International. 2011. Vol. 15. Issue 5.

[25] Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress. P. 10. URL: http://www.unodc.org/documents/treaties/Congress12RPM/2009-RPM-LatinAmerica/V0984371_E.pdf (дата обращения: 05.01.2013).

[26] Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. P. 10. URL: http://www.unodc.org/documents/treaties/Congress12RPM/2009-RPM-WesternAsia/V0984377e.pdf (дата обращения: 05.01.2013).

[27] Commonwealth Model Law on Computer and Computer Related Crime. URL: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (дата обращения: 05.01.2013).

[28] Directive 200/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT (дата обращения: 05.01.2013).

[29] *Gercke M.* Ten Years Convention on Cybercrime // Computer Law Review International. 2011. Vol. 15. Issue 5.

вопрос территориальной «привязки» для киберпреступлений в случае, если затронуто несколько стран: местонахождение данных, место наступления последствий преступления, умысел преступника на наступление последствий в определённой стране, или, как в случае нелегального контента, язык контента и его смысл[30]. При том, что развитие информационных технологий, например, в области облачных вычислений, создаёт новые юрисдикционные проблемы, например, даже администраторы облачных сетей не всегда могут ответить на вопрос, на территории какой страны находится сервер с данными, уже имеющиеся недостатки в регулировании юрисдикционных вопросов создают огромный пробел, устранить который становится все сложнее.

Помимо всего вышеперечисленного, Конвенция Совета Европы содержит спорные нормы, противоречащие, по мнению некоторых государств, фундаментальным принципам международного права. Такой нормой являются положения пункта "b" статьи 32 Конвенции, позволяющие правоохранительным органам получать доступ к компьютерным данным, находящимся на территории другого государства с добровольного согласия лица, имеющего полномочия раскрыть информацию, без согласования с компетентными властями государства, означает отступление от принципа национального суверенитета при расследовании преступлений. Фактически участники Конвенции частично отказываются от данного принципа в пользу эффективного расследования кибепреступлений. При этом Конвенция не предлагает никаких механизмов обеспечения прозрачности соответствующих процедур. Положения Конвенции, регулирующие проведение следственных действий на территории другого государства без официального согласования с ним, являются камнем преткновения для некоторых государств, в том числе и Российской Федерации[31].

Иные инструменты

Упомянутые выше проблемные аспекты Конвенции Совета Европы являются одной из причин того, что в различных регионах мира началась разработка альтернативных подходов в сфере гармонизации законодательства. Такими инструментами являются решения Совета Европейского Союза[32], Модельный Закон Содружества Наций о компьютерных преступлениях 2002 года, Модельный Закон стран Карибского Бассейна о киберпреступности (проект HIPCAR)[33], совместный проект Европейского союза и Международного Союза Электросвязи для государств Тихоокеанского региона (проект ICB4PAC)[34], проект ООН по разработке законодательства в области киберпреступности для стран Африки (проект ESCWA)[35] и др.

При этом в течение последних лет предпринимались попытки создать иные «компромиссные» инструменты, не имеющие никакой региональной привязки, никак не связывающие государства юридически, и являющиеся в большей степени документами, объясняющие законодательную технику в области криминализации электронных посягательств. Одной из таких попыток является, например, разработка Международным Союзом Электросвязи (*далее* – МСЭ) для развивающихся государств модельного документа[36], содержащего законодательные «формулы» для возможного использования их развивающимися странами в процессе изме-

---

[30] *Sieber U.* Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law // Delmas-Marty M, Pieth M & Sieber U. (eds.) Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008.

[31] T-CY (2008) 01, Compilation of responses to questionnaire for the Parties concerning the practical implementation of the Convention on Cybercrime. Strasbourg, March, 2008, P.28. URL: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2008)%2001%20E.PDF (дата обращения: 05.01.2013).

[32] Например, рамочный документ по атакам на информационные системы: Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[33] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts, HIPCAR. URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (дата обращения: 05.01.2013).

[34] См.: ITU-ICB4PAC. URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis (дата обращения: 05.01.2013).

[35] Models for Cybercrime Legislation in ESCWA member countries. URL: http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf (дата обращения: 05.01.2013).

[36] ITU Toolkit for Cybercrime Legislation. ITU, 2009.

нения законодательства о киберпреступности. Подобные попытки вряд ли можно признать успешными. Например, нет сведений о применении модельного документа МСЭ в какой-либо из стран; более того, документ через несколько лет после разработки удалён из списка рекомендуемых МСЭ. Это неудивительно, поскольку он страдал серьёзными недостатками, такими, как отличие формулировок от общепризнанных международных стандартов, введение криминализации таких деяний, как кибертерроризм при отсутствии согласованного определения терроризма на международном уровне, отсутствие моделей для криминализации детской порнографии[37]. Кроме того, разработка этого документа Ассоциацией американских юристов явилась дополнительным фактором критики по тем же основаниям, по которым критикуют Конвенцию Совета Европы, а именно создание подходов для развивающихся стран без их участия и учёта их нужд.

Наиболее успешными для последующей гармонизации в рамках группы стран являются региональные подходы. Например, Модельный закон Содружества Наций о киберпреступности, который способствовал принятию нового «сопоставимого» законодательства в области киберпреступности в странах Содружества Наций. Также успешным можно признать уже упомянутый проект HIPCAR – совместная работа Европейского Союза и МСЭ по созданию модельного документа, гармонизирующего законодательство в области киберпреступности в странах Карибского региона[38]. Этот документ, который по своей сути не связывает страны юридически, сыграл большую роль в добровольной гармонизации законодательства в государствах-участниках проекта, поскольку к его разработке и имплементации были привлечены все заинтересованные стороны – от правоохранительных органов и парламентов стран до частного сектора (операторов, провайдеров сети Интернет и др.).

Однако региональный фокус, при всей его успешности в деле гармонизации уголовного законодательства в рамках группы стран, будь оно обязательным или добровольным, ведёт к дальнейшей фрагментации усилий, поскольку обновление национального уголовного законодательства выходит на первый план. Это заслоняет собой проблему процессуального сотрудничества, для которого в трансграничном киберпространстве необходим именно глобальный, а не региональный подход.

Одной из трудностей при реализации глобального подхода к решению проблем борьбы с киберпреступностью является «медлительность» ООН – единственной организации, способной разработать и принять документ универсального характера. Время, увы, безнадёжно упущено, ведь ООН по не вполне понятным причинам начала заниматься вопросом противодействия киберпреступности лишь почти через десять лет после начала разработки Конвенции Совета Европы. В настоящее время в качестве одного из этапов подготовки некоего глобального механизма борьбы с киберпреступностью ООН проводит всестороннее исследование соответствующего законодательства государств-участников, которое планируется завершить к апрелю 2013 года[39]. Как предполагаемый глобальный механизм будет согласовываться с уже существующими региональными подходами, пока неясно, как и то, будет ли вообще разработан этот механизм и когда это произойдёт, а также сколько времени понадобится на его согласование. Учитывая темпы развития информационных технологий, возможно, что вырабатывать актуальные решения новых проблем киберпреступности придётся уже в процессе создания универсального документа ООН.

Законодательные механизмы: на пути от региональных решений к глобальным?

С учётом существующего количества наднациональных решений, основная проблема гармонизации законодательства о киберпре-

---

[37] *Gercke M., Tropina T.* From Telecommunication Standardization to Cybercrime Harmonization // Computer Law Review International. 2009. Issue 5.

[38] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts, HIPCAR. URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (дата обращения: 05.01.2013).

[39] UNODC, Comprehensive study on the problem of and response to cybercrime. URL: http://www.unodc.org/cybercrime-study (дата обращения: 05.01.2013).

ступности на международном уровне в настоящее время заключается не в отсутствии моделей для разработки законодательства, а в том, что все увеличивающееся количество этих моделей никоим образом не приводит к широте охвата и сотрудничеству на глобальном уровне. Инструменты, выработанные Европейским Союзом, Советом Европы, Содружеством Наций, странами Карибского региона обусловили криминализацию электронных посягательств в национальном законодательстве стран и гармонизацию общей части уголовного законодательства на уровне регионов мира. Однако в области процессуального сотрудничества, взаимной правовой помощи, а также в вопросах юрисдикции эти инструменты пока не смогли создать правовой базы для эффективного сотрудничества на оперативном уровне. Даже при всей фрагментарности имплементации международных стандартов в национальные правовые системы, законодательство большинства стран мира уже имеет нормы, предусматривающие ответственность за киберпреступления. Однако остаются актуальными вопрос о соответствии этих норм друг другу и проблема процессуального взаимодействия правоохранительных органов при расследовании киберпреступлений.

На первый взгляд, усилия различных международных организаций в области гармонизации законодательства по борьбе с киберпреступностью кажутся взаимодополняющими. Однако сотрудничество между этими организациями в настоящее время либо неэффективно, либо практически отсутствует. Таким образом, главная проблема эффективного сотрудничества заключается в том, что нет единого подхода к международным стандартам а также к вопросу о том, кто должен заниматься их разработкой и регулированием процесса их имплементации.

Заключение. От международного соглашения к международному трибуналу?

Несмотря на разрозненность и фрагментарность подходов к борьбе с киберпреступностью, в последнее время появляются новые предложения о создании глобальных инструментов, требующих гораздо более высокого уровня международного сотрудничества, чем гармонизация законодательства. Например, предложение о создании международного трибунала по преступлениям, совершенным в киберпространстве, внесённое председателем группы по борьбе с киберпреступностью Института «Восток-Запад» С. Шолбергом[40], в настоящее время широко обсуждается на уровне международных организаций, а также в академических кругах. Действительно, идея создания трибунала, ответственного, по словам её автора, за «мир и безопасность в киберпространстве» может показаться весьма привлекательной. Однако насколько своевременна эта идея в настоящей ситуации? Как уже было сказано выше, международное сообщество, несмотря на усилия региональных и наднациональных организаций, так и не достигло консенсуса по основным вопросам борьбы с киберпреступностью. Насколько эффективным может быть подобное международное судебное учреждение и есть ли разумные предпосылки к его созданию?

С одной стороны, в условиях, когда как уголовное, так и уголовно-процессуальное законодательство о кибепреступности ещё очень далеко от гармонизации, когда неясна ситуация с решением вопроса о юрисдикции, когда правовая взаимопомощь по вопросам кибепреступлений находится в периоде становления, дискуссии о создании международного трибунала по киберпреступности выглядят преждевременными. С другой стороны, современное общество уже столкнулось с проблемой, когда развитие информационных технологий значительно опередило развитие инструментов правового регулирования. Упущенное время и невозможность спрогнозировать последствия повсеместного применения информационных сетей привели к ситуации, когда законодателям приходится заполнять уже существующие пробелы, что в условиях необходимости международной гармонизации подходов к борьбе с киберпреступностью и отсутствии чётких международных стандартов является достаточно сложной задачей.

[40] Текст документа: *Schjolberg S.* Proposals for new legal mechanisms on combatting cybercrime and global cyberattacks. An International Criminal Court or Tribunal for Cyberspace (ICTC). URL: http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf (дата обращения: 05.01.2013).

При этом информационная безопасность уже рассматривается государствами как одна из приоритетных задач в сфере национальной безопасности и международной политики. Компьютерные атаки на компании и даже на государства, такие как вирус Stuxnet, показывают, что если информационное оружие и не станет в ближайшее время реальной угрозой, то в любом случае может причинить серьёзные проблемы экономике и военной безопасности государств[41]. Вероятно, дискуссии о создании международного трибунала по киберпреступности необходимо начинать уже сейчас. Однако для создания и эффективного функционирования этого института необходима твёрдая правовая основа, которая в настоящее время отсутствует, а именно:

– гармонизированное на международном уровне уголовное законодательство, набор минимальных стандартов, которые будут имплементированы во всех государствах-членах соглашения о международном трибунале;

– разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять доказательства с учётом международной составляющей проблемы киберпреступности;

– эффективные механизмы правовой взаимопомощи в области расследования киберпреступлений, отлаженное сотрудничество правоохранительных органов на оперативном уровне;

– механизм решения юрисдикционных вопросов в киберпространстве.

Международное сотрудничество является ключевым моментом для сдерживания такого комплексного явления, как киберпреступность. Совместная работа государств и международных организаций, выработка новых механизмов контроля и управления – единственный путь к информационной безопасности, которая в настоящее время представляется труднодостижимой целью, но в то же время является насущной необходимостью.

[41] *Farwell J.P., Rohozinski R.* Stuxnet and the Future of Cyber War // Survival. 2011. Vol. 53. No. 1.