ISSN 1996-7756

УДК 343.375
DOI 10.17150/1996-7756.2016.10(2).369-378

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Е.М. Якимова[1], С.В. Нарутто[2]
[1] Байкальский государственный университет, г. Иркутск, Российская Федерация
[2] Московский государственный юридический университет им. О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация

Информация о статье
Дата поступления
28 мая 2015 г.

Дата принятия в печать
23 марта 2016 г.

Дата онлайн-размещения
29 июня 2016 г.

Ключевые слова
Защита информации; Интернет; информация; киберпреступление; киберпространство; международное сотрудничество

Финансирование
Государственное задание № 29.1247.2014/К на выполнение научно-исследовательских работ в сфере научной деятельности в рамках проектной части, проект № 1247 «Пределы ограничения прав личности в уголовном судопроизводстве в целях обеспечения национальной безопасности государства: уголовно-процессуальный и криминалистический анализ»

Аннотация. В настоящее время постиндустриальное общество трансформируется в общество информационное, что, с одной стороны, упрощает взаимодействие между участниками общественных отношений, с другой стороны, повышает риск нарушения конфиденциальности контрактов. Изменение структуры и объема передачи информации требует как от самих субъектов социальных отношений, которые имеют личный интерес в обеспечении максимально возможного уровня безопасности передаваемых данных, так и от государства в целом как от гаранта стабильности правового поля общественных отношений выстраивания четкой архитектуры безопасного распространения информации. Очевидно, что национальная безопасность значительным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость только возрастает. Информация, выступая в качестве экономической и социальной гарантии стабильности существования и развития общества и государства, является объектом пристального внимания и воздействия со стороны государства. Введение полноценного электронного документооборота и создание интероперабельных информационных ресурсов сделали информационную материю достаточно уязвимой для вмешательства извне. Правовые основы режима конфиденциальности информации в международном праве включают следующие его составляющие: базовые принципы в сфере privacy; порядок трансграничного оборота конфиденциальной информации; защиту конфиденциальной информации; статус международных органов, осуществляющих выработку единой правовой политики в сфере privacy и ее реализацию. Исходя из обобщенного анализа нормативно-правовой базы как международного, так и национального законодательства, существующих взглядов на данную проблему и высказанных авторских замечаний, предлагается концептуально новый подход к реализации международного сотрудничества в сфере борьбы с киберпреступлениями, предполагающий бóльшую скоординированность действий всех государств как минимум по двум направлениям: совершенствование правовой основы взаимодействия и имплементация выработанных норм в национальное законодательство, улучшение организационной основы обмена информацией.

INTERNATIONAL COOPERATION IN CYBERCRIME COUNTERACTION

Ekaterina M. Yakimova[1], Svetlana V. Narutto[2]
[1] Baikal State University, Irkutsk, the Russian Federation
[2] Kutafin Moscow State Law University (MSAL), Moscow, the Russian Federation

Article info
Received
2015 May 28

Accepted
2016 March 23

Available online
2016 June 29

Abstract. The post-industrial society is now transforming into the informational one, which, on the one hand, simplifies social relations and, on the other hand, increases the risk of violating the confidentiality of contracts. The changes in the structure and volume of transmitted information require that a rigorous procedure of safe transmission of information should be maintained by both the subjects of social relations, which have a personal interest in ensuring the maximum possible level of security for the transmitted data and the state as a whole as a guarantor of social relations' legal stability. It is evident that national security greatly depends of ensuring information security, and that technological progress increases this dependence. Information, acting as economic and social guarantee of stable existence and development of the society

ISSN 1996-7756

Keywords
Information protection; Internet; information; cybercrime; cyberspace; international cooperation

Financing
Governmental order No. 29.1247.2014/K for research work within the framework of the project No. 1247 «The boundaries of limiting individual rights in criminal proceedings to ensure national security: criminal procedure and forensic analysis» (registration No. 114091140016 in FGANU TsITiS)

and the state, is an object of close attention and influence from the state. The introduction of full-scale electronic documentation processing and the creation of inter-operational information resources made information rather vulnerable to external influence. The legal basis of information protection in international law includes the following components: basic privacy principles; the procedure of trans-border transmission of confidential information; protection of confidential information; status of international bodies working on developing a unified legal policy in the sphere of privacy and its implementation. Using the generalized analysis of both the international and the national legal bases, the existing views on this issues and the authors' considerations, the paper presents a conceptually innovative approach to international cooperation in the sphere of counteracting cybercrimes, which presupposes a greater coordination of the actions of all states in at least two directions: the enhancement of the legal background of counteraction and the implementation of the devised norms into the national legislation, the improvement of the organizational basis of information exchange.

Каждое государство постоянно балансирует между принципами соблюдения прав и свобод человека и гражданина, интеграцией в международное сообщество, необходимостью обеспечения экономического роста и национальной безопасности, в том числе посредством ограничения прав и свобод человека и гражданина, установления административных форм ограничения предпринимательской деятельности, защиты собственных интересов на международной арене. Выбор осуществляет и население, и органы публичной власти, однако в ряде сфер никакие внутренние причины не должны перевешивать необходимость международного сотрудничества в борьбе с преступлениями, которое должно строиться на принципах открытости, взаимопомощи, активности в разработке новых форм взаимодействия. Как представляется, международное сотрудничество в борьбе с киберпреступностью необходимо осуществлять на основе участия всех стран, что предопределяется как свойством самой информации в качестве объекта посягательства, так и характером совершаемых преступлений. Как заметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шьольберг (Stein Schjolberg), «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне» [1]. Действительно, в современном мире все сферы жизнедеятельности находятся в прямой зависимости от работы вычислительных и информационных сетей. Вместе с тем «широкое использование для обработки информации средств вычислительной техники с программным обеспечением, позволяющим сравнительно легко модифицировать, копировать и разрушать информацию» [2, с. 4] повышает уязвимость информационного пространства. Пользователи информационных систем «без достаточных к тому оснований верят в отсутствие кибератак, используя информационное пространство с незнанием ограничений и угроз безопасности системы» [3, p. 193].

В современном мире информация выступает важнейшим компонентом развития общества. Превращение постиндустриального общества в общество информационное означает, что информация приобретает глобальный характер, становится значимой как для человека лично, так для государства и общества в целом, каждый может искать, получать, передавать, производить и распространять информацию любым законным способом, не существует границ для ее потока. В настоящий момент информация признается одной из важнейших ценностей, соответственно, ее защита представляет собой не менее важную деятельность, чем ее получение и передача, следовательно, в «дигитализированном обществе начала XXI в. сфера проявления риска меняется» [4, с. 46]. Например, «революционные события так называемой Арабской весны в мировом экспертном, медийном и политическом дискурсе оказались неразрывно связаны с ролью информационно-коммуникационных технологий. …Беспрецедентная скорость распространения информации через интернет (в основном через социальные сети) сыграла против режимов, стремившихся скрыть свои репрессивные акции от международного сообщества и не владевших адекватными навыками ведения информационной борьбы» [5, с. 129]. В настоящее время тенденции глобализации усиливаются, причем всё очевиднее те

ISSN 1996-7756

проблемы, к которым она приводит. В этих условиях актуализируется вопрос об участии всех партнеров системы мирового правопорядка в борьбе с негативными проявлениями, вызванными глобализационными процессами, в том числе транснациональной киберпреступностью.

Очень важно понимать глобальность проблемы киберпреступности. Так, уже сейчас кибератаки парализуют работу не только частных структур, но и государственных органов, в мире не существует государства, которое было бы защищено от подобного рода атак. В качестве вероятных источников киберугроз рассматриваются не только хакеры или их группы, но также отдельные государства, террористические, преступные группировки.

При выработке средств и методов борьбы с киберпреступностью следует помнить о латентности данного вида преступлений. По оценкам экспертов, латентность «компьютерных преступлений» в США достигает 80 %, в Великобритании — 85 %, в ФРГ — 75 %, в России — более 90 % [6, с. 15]. По данным международной службы по обеспечению безопасности в области киберугроз Symantec Security, «каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд дол. США» [4, с. 46].

Киберпреступность может нарушать интересы как государства, так и отдельного человека. Бесспорно, особенности функционирования информационных систем, прежде всего сети Интернет, «требуют, чтобы на решение вопросов кибербезопасности были обращены совместные усилия различных субъектов, как государственных, так и частных» [7, p. 81], однако именно государство может и должно, а главное, только оно способно эффективно осуществлять полномасштабное противодействие совершению киберпреступлений, создавать условия для того, чтобы те, кто в наибольшей мере подвержен нападению киберпреступников (например, банки, физические лица), могли выстраивать более надежную систему информационной защиты.

В мире есть примеры достаточно эффективных систем противодействия совершению киберпреступлений. В настоящее время ведущие страны мира активно расширяют и создают в вооруженных силах и спецслужбах подразделения, которые должны обеспечивать развитие наступательных возможностей в киберпространстве (табл.).

Особенности обеспечения кибербезопасности в ряде стран
Details of Cybersecurity Practices in Some Countries

Страна / Country	Участие в Конвенции о киберпреступности / Participation in Cybercrime Convention	Разработка Конвенции ООН «Об обеспечении международной информационной безопасности» / Development of UN Convention «On International Information Security»	Основные организации в области кибербезопасности / Key agencies responsible for cybersecurity
Великобритания / Great Britain	+	–	Группа безопасности электронной коммуникации при Центре правовой связи при МИД; подразделение Министерства обороны по защите от виртуальных угроз
Германия / Germany	+	–	Специальная группа при МВД ФРГ
Индия / India	+	–	Аналитический и исследовательский отделы внешней разведки и разведывательное бюро внутренней разведки
Китай / China	–	+	Реализация программы защиты от несанкционированного подключения к компьютеру
Россия / Russia	–	+	Управление «К» МВД и отделы «К» региональных управлений МВД; Национальный контактный пункт при БСТМ МВД России
США / USA	+	–	Центр национальной кибербезопасности; Объединенное кибернетическое командование Вооруженных сил США

ISSN 1996-7756

Например, в США наряду с уже функционирующим Центром национальной кибербезопасности (National Cyber Security Center) в составе Вооруженных сил сформировано Объединенное кибернетическое командование (Unified U.S. Cyber Command), которое в глобальном масштабе должно координировать усилия всех структур Пентагона в ходе ведения боевых действий, оказывать соответствующую поддержку гражданским федеральным учреждениям, а также взаимодействовать с аналогичными по задачам ведомствами других стран [8, с. 26]. Вместе с тем указанные организации — отчасти подконтрольные ведомства, поскольку «верховной контролирующей структурой является Совет национальной безопасности со специальными комитетами, в сферу ответственности которых входит реализация информационной стратегии» [9, с. 36], в том числе по борьбе и с киберпреступностью. В Великобритании реализуются программы по созданию кибероружия, которые обеспечат способность властей противостоять растущим угрозам из киберпространства [10, с. 70]. В Австралии создана группа координации безопасности электронной почты (ESCG). «Основной задачей этой группы является создание безопасного и надежного электронного оперативного пространства как для общественного, так и для частного секторов» [11, с. 84].

Деятельность по противодействию совершению киберпреступлений осуществляют не только отдельные государства, но и их блоки, в частности НАТО. Так, важность данной проблемы находит отражение во всех руководящих документах блока, принятых в последние годы. В стратегическую концепцию НАТО впервые включено положение о киберпространстве как новой сфере военной деятельности альянса [12, с. 13].

Иными словами, в борьбе с трансграничными преступлениями, к которым можно отнести и значительную часть киберпреступлений, особая роль отведена государствам, и только при хорошо скоординированной работе правоохранительных органов различных стран возможно снизить количество совершаемых правонарушений в рассматриваемой сфере.

Международное сотрудничество осуществляется по нескольким направлениям и предполагает прежде всего создание нормативных актов и выработку общих рекомендаций, а также внедрение эффективных моделей организационного взаимодействия между государствами. При этом следует учитывать, что традиционные механизмы международного сотрудничества, включая запросы, взаимопомощь и другие подобные инструменты, применявшиеся в XIX в. и ранее, являются неподходящими в эру, когда преступления могут совершаться из любой точки земного шара со скоростью света [13, p. 60].

Правовое регулирование вопросов борьбы с киберпреступлениями представляет собой базис всей системы противодействия киберпреступности. Сложность выработки международных актов в целом в рассматриваемой ситуации осложняется еще и тем, что «существующие законы трудно применять, когда речь идет о не поддающихся локализации атаках в планетарных масштабах, доказательства которых разбросаны и виртуальны» [14, с. 144].

Международное сообщество на различных уровнях выработало ряд актов, имеющих значение для борьбы с киберпреступностью, причем особую роль играют региональные акты, поскольку общемировой документ в настоящее время создать затруднительно. Вместе с тем нельзя не отметить попытки государств распространить нормы глобальных международных договоров на борьбу с киберпреступностью или заключить новые договоры. Например, так как в киберпространстве наряду с отдельными лицами могут действовать и организованные преступные группы, существует возможность применения к ним международных договоров, направленных на борьбу с организованной преступностью, в частности Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г.

Кроме того, разработана концепция Конвенции ООН об обеспечении международной информационной безопасности[1], которая была представлена международному сообществу в ноябре 2011 г. на конференции по киберпространству в Лондоне и включает преамбулу, 23 статьи, объединенные в основную часть, и заключительные положения. Основная часть документа состоит из пяти глав, содержание которых находится в единой композиционной целостности. Немаловажно, что в ст. 4 Конвенции закреплены основные угрозы международ-

[1] Конвенция об обеспечении международной информационной безопасности (концепция). URL : http://www.scrf.gov.ru/documents/6/112.html.

ISSN 1996-7756

ному миру и безопасности в информационном пространстве, из которых выделено 11 базовых и 4 дополнительных. Среди базовых названы, например, использование информационных технологий и средств для осуществления враждебных действий и актов агрессии; целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства; трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств. Опять же в документе не указаны такие реальные угрозы международной безопасности, как совершение киберпреступлений, распространение наркотических и психотропных средств, их аналогов, а также порнографии, в том числе и детской.

Помимо этого, концепция Конвенции содержит ст. 5, посвященную основным принципам обеспечения международной информационной безопасности. Анализ представленных принципов позволяет сделать вывод о том, что их можно разделить на четыре группы: принципы участия государства в системе международной информационной безопасности как члена международного сообщества; принципы, позволяющие государству сохранить свой суверенитет в процессе международного сотрудничества в борьбе с киберпреступностью; принципы обеспечения свободного информационного обмена между странами. Четвертая группа принципов устанавливает характер взаимодействия государства и частных субъектов в рассматриваемых отношениях. Вместе с тем опять же приходится констатировать, что в концепции Конвенции детально не прописаны принципы международного сотрудничества в борьбе с киберпреступлениями, кроме направленного против действий террористического характера.

Позитивным следует признать включение в концепцию Конвенции гл. 5 «Международное сотрудничество в сфере международной информационной безопасности», однако меры международного сотрудничества в рассматриваемой сфере представляются явно недостаточными для эффективного функционирования системы международной экономической безопасности, поскольку предполагают лишь «обмен национальными концепциями обеспечения безопасности в информационном пространстве, оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации», «консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера». Вместе с тем данные формы не учитывают необходимость удовлетворения потребности в оперативном взаимодействии правоохранительных органов по широкому кругу вопросов.

Таким образом, положения концепции Конвенции ООН об обеспечении международной информационной безопасности носят достаточно компромиссный характер и ориентированы прежде всего на предупреждение информационных войн, терроризма.

Нельзя не отметить, что бóльшую часть специализированных актов по борьбе с киберпреступлениями составляют акты Европейского союза, который обладает одной из наиболее развитых в мире систем обеспечения информационной безопасности. Так, в октябре 1999 г. в ходе Тамперского совещания Европейского совета им было принято решение о целесообразности включения преступлений в области высоких технологий (high-tech crime) в число преступлений, по которым необходима выработка общего европейского подхода в части криминализации и санкций [15, с. 267; 16, с. 323]. В 2001 г. Европейская комиссия представила специальное сообщение «Создание безопасного информационного общества посредством повышения защищенности информационной инфраструктуры и борьбы с преступлениями с использованием компьютерных средств»[2], в котором содержались предложения правового и организационного характера по борьбе с киберпреступностью в Европейском союзе.

Как для Европейского союза, так и для всего мирового сообщества принципиальное зна-

[2] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions «Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computerrelated Crime». Brussels, 26.1.2001. COM (2000) 890fi nal. URL : http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html.

ISSN 1996-7756

чение имеет Конвенция о киберпреступности[3], регламентирующая глобальные меры борьбы с киберпреступностью, которая была принята Советом Европы в 2001 г. Россия не присоединилась к указанной Конвенции, поскольку положения ст. 32b противоречат российскому законодательству и нарушают суверенитет государства, так как предусмотренные в ней действия могут совершаться без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются. Кроме того, «в УК РФ отсутствуют нормы, устанавливающие уголовную ответственность юридических лиц за преступления в сфере компьютерной информации» [17, с. 27].

В преамбуле к Конвенции государства-участники обозначили цель ее принятия: выработка в приоритетном порядке общей политики в сфере уголовного права, ориентированной на защиту общества от киберпреступности, в том числе посредством принятия соответствующих законодательных актов и укрепления международного сотрудничества; сдерживание действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерной информации, а также против злоупотребления такими системами, сетями и информацией, путем обеспечения уголовной наказуемости таких деяний и предоставления полномочий, достаточных для эффективной борьбы с данными уголовными преступлениями, путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровне и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества.

Конвенция о киберпреступности предполагает осуществление действий на уровне государств-участников и на международном уровне. На национальном уровне мыслится развитие прежде всего материального уголовного права: разработка в национальных уголовных кодексах положений о преступлениях против конфиденциальности, целостности и доступности компьютерных систем, сетей и информации, о преступлениях, связанных с использованием компьютерных средств, с содержанием данных, с нарушением авторского права и смежных прав; определение дополнительных видов ответственности и санкций (включение в состав преступлений таких видов, как покушение на совершение преступления, соучастие в нем или подстрекательство к его совершению в рассматриваемой сфере); установление уголовной ответственности юридических лиц, что, однако, противоречит концепциям уголовной ответственности в ряде стран, например в Российской Федерации.

Так, в Конвенции о киберпреступности киберпреступления классифицируются следующим образом: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (offences against the confi dentiality, integrity and availability of computer data and systems): противозаконный доступ (illegal access); неправомерный перехват (illegal interception); воздействие на данные (data interference); воздействие на функционирование системы (system interference); противозаконное использование устройств (misuse of devices); 2) правонарушения, связанные с использованием компьютерных средств (computer-related offences): подлог с использованием компьютерных технологий (computer-related forgery); мошенничество с использованием компьютерных технологий (computerrelated fraud); 3) преступления, связанные с содержанием данных (content-related offences) — преступления, связанные с детской порнографией (offences related to child pornography); 4) правонарушения, связанные с нарушением авторского права и смежных прав (offences related to infringements of copyright and related rights).

Дополнительный протокол к Конвенции о киберпреступности[4] включает в указанный перечень следующие виды преступлений: 1) распространение расистских и ксенофобских материалов посредством компьютерных систем (dissemination of racist and xenophobic material through computer systems); 2) мотиви-

[3] Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) : заключена в Будапеште 23 нояб. 2001 г. URL : http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm.

[4] Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем (подписан в г. Страсбург 28 янв. 2003 г.). URL : http://mvd.gov.by/main.aspx?guid=4593.

ISSN 1996-7756

рованная угроза расизма и ксенофобии (racist and xenophobic motivated threat); 3) расистское и ксенофобское мотивированное оскорбление (racist and xenophobic motivated insult); 4) отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества (denial, gross minimisation, approval or justifi cation of genocide or crimes against humanity).

Конвенция предполагает также и развитие уголовно-процессуального законодательства, например необходимость законодательного закрепления оперативного обеспечения сохранности накопленных компьютерных данных, процедуры проведения обыска и выемки хранимых компьютерных данных.

Особое внимание в Конвенции уделяется международному сотрудничеству — данному вопросу посвящена гл. 3. Общими принципами международного сотрудничества названы: общие принципы взаимной помощи; возможность трансграничного доступа к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным, взаимной помощи в связи с оценкой хранящихся электронных данных, взаимной правовой помощи по сбору данных о потоках в режиме реального времени; создание сети 24/7).

Несмотря на наличие в рассматриваемой сфере других международных актов, «Конвенция является единственным признанным международным договором… содержит нормы материального и процессуального (процедурные) права в целях противодействия киберпреступности и защиты свободы, безопасности и прав человека в Интернете» [10, с. 66].

Положения Конвенции создают основу для взаимодействия государств, однако, как отмечает болгарский исследователь Р. Георгиева, «Конвенция не гарантирует безопасность виртуального пространства. Большое значение будет иметь ее координация с внутренним законодательством каждой страны» [18, с. 17].

В рамках Европейского союза реализуется ряд программ, способствующих борьбе с киберпреступлениями, вырабатываются совместные позиции по данному вопросу. В частности, Стокгольмская программа рекомендует подготовить стратегию внутренней безопасности для ЕС с целью улучшения защиты граждан и для борьбы с организованной преступностью и терроризмом.

На региональном уровне помимо Конвенции о киберпреступности принято также Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. Основной идеей данных документов является «определение единообразных составов компьютерных преступлений, которые государства должны включить в свое национальное законодательство, а также разработка мер борьбы с ними. Рассматриваемые договоры выполняют очень важную роль: они установили основы юрисдикции государств по уголовным делам в Интернете и правила международного сотрудничества, обеспечивающие согласованность действий государств в борьбе с компьютерными преступлениями. Несмотря на отдельные недостатки договоров, в целом они предусматривают системы взаимосвязанных международных и национальных мер борьбы с компьютерными преступлениями» [19, с. 39].

Важно отметить, что взаимодействие государств в сфере борьбы с киберпреступлениями требует обобщения правовых норм различных государств при регламентации действий сторон в процессе использования средств в борьбе с киберпреступлениями. В частности, Центром передового опыта НАТО в области компьютерной безопасности выпущен сборник рекомендаций «Таллинское руководство по применению международного права в кибервойне». Основными задачами предполагаются «адаптация существующих правовых норм в отношении вооруженных конфликтов под специфику враждебной деятельности в виртуальном пространстве» [12, с. 15] и попытка разработать дефиниции основных понятий в сфере компьютерной безопасности.

Второй формой сотрудничества государств в борьбе с киберпреступлениями является создание специализированных органов.

Поскольку информационная безопасность государства связана с его суверенитетом, то создание единого органа, который бы координировал взаимодействие государств по борьбе с киберпреступлениями, затруднительно, однако создаются вспомогательные органы, руководствующиеся едиными стандартами деятельности, обобщающими практику разных стран по вопросам борьбы с киберпреступлениями.

ISSN 1996-7756

Большое значение во взаимодействии государств — участников Европейского союза имеет деятельность Европола и Евроюста, принимающих «непосредственное участие в борьбе с киберпреступностью на пространстве Европейского союза» [15, с. 268]. В работе Европола используется система аналитических рабочих картотек (analys work files), формируемых из сосредоточенных в его информационной системе данных в целях анализа, определяемого как обработка или использование данных для поддержки уголовных расследований. Система действующих аналитических картотек включает картотеки по киберпреступности Cyborg и детской порнографии Twins [20, с. 88–89].

Что касается Евроюста, то его деятельность по обеспечению безопасности на территории Европы становится все более заметной: если в 2010 г. он расследовал 1 424 дела, то в 2015 г. — 2 214 дел[5]. Евроюст осуществляет в том числе координацию действий правоохранительных органов различных государств по вопросам расследования киберпреступлений, оказывает помощь в проведении расследований по запросу соответствующего органа публичной власти стран — участниц Европейского союза, предоставляет правоохранительным органам этих стран информацию о проводимых расследованиях в отношении киберпреступников. Полномочия Евроюста также распространяются на возбуждение уголовных расследований либо выдвижение предложения об их возбуждении правоохранительным органам стран — участниц ЕС и последующую координацию проводимых расследований.

Помимо указанных органов, обладающих юрисдикционной компетенцией в рассматриваемой сфере, Европейским союзом создаются и вспомогательные органы. Так, 18 января 2013 г. в Гааге официально открыт Европейский центр по борьбе с киберпреступностью. Целями его создания являются сбор и обработка данных по киберпреступлениям, проведение экспертных оценок интернет-угроз, разработка и внедрение передовых методов профилактики и расследования киберпреступлений, подготовка новых кадров, оказание помощи правоохранительным и судебным органам, а также координация совместных действий заинтересованных сторон, направленных на повышение уровня безопасности в европейском киберпространстве[6].

Военное взаимодействие государств также требует решения вопроса об их сотрудничестве в сфере организационной поддержки борьбы с киберпреступностью. Так, в 2008 г. «по инициативе Эстонии в Таллине был создан центр передового опыта НАТО, в настоящее время он является научно-исследовательским и учебным заведением альянса, занимающимся разработкой ключевых направлений развития коалиционных возможностей по действиям в киберпространстве» [12, с. 14].

Создание данного центра не являлось единственным направлением работы по организации борьбы с киберпреступлениями в Североатлантическом союзе: в 2013 г. было завершено развертывание единой системы НАТО по реагированию на компьютерные угрозы, включающей два центра по реагированию на угрозы в киберпространстве (в Брюсселе и Монсе). Помимо этого, предпринимаются шаги по проверке эффективности уже созданной системы отражения кибератак, например ежегодно проводятся учения «Киберкоалиция», «Защитный шар».

Иными словами, современной тенденцией международного противодействия киберпреступности является расширение сферы взаимодействия государств. Реальностью становится оперативное сотрудничество правоохранительных органов по борьбе с киберпреступлениями (Интерпол, Европол, Евроюст), создание и использование единой базы данных о киберпреступниках, о совершенных и планируемых киберпреступлениях (прежде всего работающей в режиме 24/7).

Отметим, что работа Интерпола в плане оперативности обработки информации менее эффективна, чем специализированных организаций меньшего масштаба. Так, российские правоохранительные органы чаще используют возможности Национального контактного пункта при БСТМ МВД России, который действует в формате 24/7 и предназначен обеспечивать вза-

[5] Eurojust fights serious, cross-border organised crime // Eurojust casework in 2015 (Eurojust infographics). URL : http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-03-04.aspx.

[6] Кибертерроризм: угроза национальной и международной безопасности. URL : http://www.arms-expo.ru/news/archive/kibertmezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/.

ISSN 1996-7756

имодействие с коллегами из ближнего и дальнего зарубежья. Офицер спецподразделения одной из стран в любое время суток может оперативно связаться с таким же пунктом в другом государстве и получить или передать нужные сведения, необходимые для проведения оперативно-розыскных мероприятий. Сегодня национальные контактные пункты действуют почти в 50 странах.

Таким образом, можно сделать следующие выводы. С учетом всей сложности и опасности киберпреступлений необходима выработка совместных действий ученых-юристов, прежде всего законодателей, и, конечно же, специалистов в области компьютерных информационных технологий, направленных на борьбу с преступлениями в глобальных информационных сетях. Поскольку внедрение нормативных актов как национального, так и международного характера — недостаточный шаг на пути решения проблемы борьбы с киберпреступностью, в данном случае необходимы специальные знания в области информационных технологий и программного обеспечения.

Единого глобального акта, регламентирующего порядок противодействия киберпреступлениям, не выработано, однако международное сообщество в рамках регионального сотрудничества предпринимает меры по законодательному регулированию действий субъектов в киберпространстве, по борьбе с киберпреступлениями.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Schjolberg S. A cyberspace treaty — A United Nations convention or protocol on cybersecurity and cybercrime [Electronic resource] / Stein Schjolberg // Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. — Mode of access : http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

2. Сачков Д.И. Обеспечение информационной безопасности в органах власти : учеб. пособие / Д.И. Сачков, И.Г. Смирнова. — Иркутск : Изд-во БГУЭП, 2015. — 122 с.

3. Forensic Investigation Processes for Cyber Crime and Cyber Space / K.K. Sindhu, R. Kombade, R. Gadge, B.B. Meshram // Proceedings of International Conference on Internet Computing and Information Communications. — 2012. — Vol. 16. — P. 193–206.

4. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. — 2014. — № 8. — С. 46–50.

5. Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы / О. Демидов // Индекс Безопасности. — 2013. — № 1 (104). — С. 129–168.

6. Варданян А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. — М. : Юрлитинформ, 2007. — 307 с.

7. Huey L. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and Criminal Justice. — 2013. — Vol. 13, № 1. — P. 81–97. — DOI : 10.1177/1748895812448086.

8. Берд К. Война со многими неизвестными / К. Берд // Компьютерра. — 2009. — № 20. — С. 26–29.

9. Завьялов С. Зарубежный опыт в области борьбы с пропагандой терроризма в интернете / С. Завьялов // Зарубежное военное обозрение. — 2014. — № 4. — С. 34–39.

10. Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации : дис. … канд. юрид наук : 12.00.13 / И.А. Химченко. — М., 2014. — 174 с.

11. Згадзай О.Э. Киберпреступность: факторы риска и проблемы борьбы / О.Э. Згадзай, С.Я. Казанцев // Вестник ГУ «Научный центр безопасности жизнедеятельности детей». — 2013. — № 4 (18). — С. 80–86.

12. Градов А. Деятельность Североатлантического союза в сфере кибербезопасности / А. Градов // Зарубежное военное обозрение. — 2014. — № 7. — С. 13–16.

13. Smith R.G. Criminals on Trial / R.G. Smith, P. Grabosky, G. Urbas. — Cambridge University Press, 2004. — 263 p.

14. Жилина И.Ю. Киберпреступность и борьба с ней (сводный реферат) / И.Ю. Жилина // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 2, Экономика : реф. журн. — 2003. — № 1. — С. 144–148.

15. Смирнов А.А. Система борьбы с киберпреступностью в Европейском Союзе / А.А. Смирнов // Библиотека криминалиста. — 2012. — № 2 (3). — С. 262–274.

16. Смирнов А.А. Международно-правовые аспекты борьбы с киберпреступностью и кибертерроризмом / А.А. Смирнов // Проблемы укрепления законности и правопорядка: наука, практика, тенденции : сб. науч. тр. / В.М. Хомич [и др.]. — Минск, 2012. — Вып. 5. — С. 323–329.

17. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. — 2015. — № 1 (59). — С. 21–31.

18. Георгиева Р. Конвенция за киберпрестъпността / Р. Георгиева // Общество и право (София). — 2001. — № 11. — С. 16–18.

19. Талимончик В.П. Международно-правовое регулирование отношений в сфере информации : автореф. дис. … д-ра юрид. наук : 12.00.14 / В.П. Талимончик. — СПб., 2013. — 52 с.

20. Волеводз А.Г. Учреждения и органы Европейского союза по судебному и полицейскому сотрудничеству : учеб. пособие / А.Г. Волеводз. — М. : Европ. учеб. ин-т при МГИМО(У) МИД России, 2010. — 303 с.

ISSN 1996-7756

REFERENCES

1. Schjolberg Stein. A cyberspace treaty — A United Nations convention or protocol on cybersecurity and cybercrime. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010*. Available at: http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

2. Sachkov D.I., Smirnova I. G. *Obespechenie informatsionnoi bezopasnosti v organakh vlasti* [Ensuring Information Security in the Bodies of Power]. Irkutsk, Baikal State University of Economics and Law Publ., 2015. 122 p.

3. Sindhu K.K., Kombade Rupali, Gadge Reena, Meshram B.B. Forensic Investigation Processes for Cyber Crime and Cyber Space. *Proceedings of International Conference on Internet Computing and Information Communications,* 2012, vol. 16, pp. 193–206.

4. Karpova D.N. Cybercrimes: a global issue and its solution. *Vlast'= The Power*, 2014, no. 8, pp. 46–50. (In Russian).

5. Demidov O. International information security and Russia's national interests. *Indeks Bezopasnosti = Security Index*, 2013, no. 1 (104), pp. 129–168. (In Russian).

6. Vardanyan A.V., Nikitina E.V. *Rassledovanie prestuplenii v sfere vyso-kikh tekhnologii i komp'yuternoi informatsii* [Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ., 2007. 307 p.

7. Huey L., Nhan J., Broll R. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime. *Criminology and Criminal Justice*, 2013, vol. 13, no. 1, pp. 81–97. DOI:10.1177/1748895812448086.

8. Berd K. A war with many unknown quantities. *Computerra*, 2009, no. 20, pp. 26–29. (In Russian).

9. Zav'yalov S. International experience in fighting the propaganda of terrorism in the Internet. *Zarubezhnoe voennoe obozrenie = Foreign Military Review*, 2014, no. 4, pp. 34–39. (In Russian).

10. Khimchenko I.A. *Informatsionnoe obshchestvo: pravovye problemy v usloviyakh globalizatsii. Kand. Diss.* [Information society: legal basis in the conditions of globalization. Cand. Diss.]. Moscow, 2014. 174 p.

11. Zgadzai O.E., Kazantsev S. Ya. Cybercrime: factors of danger and problems of struggle. *Vestnik GU «Nauchnyi tsentr bezopasnosti zhiznedeyatel'nosti detei» = Bulletin of «Research Center for the Security of Children»*, 2013, no. 4 (18), pp. 80–86. (In Russian).

12. Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. *Zarubezhnoe voennoe obozrenie = Foreign Military Review,* 2014, no. 7, pp. 13–16. (In Russian).

13. Smith R.G., Grabosky P., Grabosky G. *Criminals on Trial.* Cambridge University Press, 2004. 263 p.

14. Zhilina I.Yu. Cybercrimes and counteracting them (a summary). *Sotsial'nye i gumanitarnye nauki. Otechestvennaya i zarubezhnaya literatura. Seriya 2, Ekonomika = Sotsial'nye i gumanitarnye nauki. Russian and Foreign Literature. Series 2, Economics,* 2003, no. 1, pp. 144–148. (In Russian).

15. Smirnov A.A. EU System of Fight against Cybercrime. *Biblioteka kriminalista = Criminalist's Library*, 2012, no. 2 (3), pp. 262–274. (In Russian).

16. Smirnov A.A. International legal aspects of fighting cybercrimes and cyber-terrorism. In Khomich V. M. et al. *Problemy ukrepleniya zakonnosti i pravoporyadka: nauka, praktika, tendentsii* [Issues of Strengthening Law and Order: Science, Practice, Trends]. Minsk, 2012, iss. 5, pp. 323–329. (In Russian).

17. Evdokimov K.N. Topical issues of prevention of the crimes in the sphere of computer information in the Russian Federation. *Akademicheskii yuridicheskii zhurnal = Academic Juridical Journal*, 2015, no. 1 (59), pp. 21–31. (In Russian).

18. Evdokimov K.N. Konventsiya za kiberprest'pnostta. *Obshchestvo i pravo = Society and Law (Sofia),* 2001, no. 11, pp. 16–18. (In Bulgarian).

19. Talimonchik V.P. Mezhdunarodno-pravovoe regulirovanie otnoshenii v sfere informatsii. *Avtoref. Dokt. Diss.* [International legal regulation of relations in the sphere of information. Doct. Diss. Thesis]. Saint Petersburg, 2013. 52 p.

20. Volevodz A.G. *Uchrezhdeniya i organy Evropeiskogo soyuza po sudebno-mu i politseiskomu sotrudnichestvu* [Agencies and Bodies of the EU on court and police cooperation]. Moscow, European Studies Institute at MGIMO-University Publ., 2010. 303 p.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Якимова Екатерина Михайловна — доцент кафедры конституционного и административного права Юридического института Байкальского государственного университета, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: yakimova_katerin@mail.ru.

Нарутто Светлана Васильевна — профессор кафедры конституционного и муниципального права Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: svetanarutto@yandex.ru.

INFORMATION ABOUT THE AUTHORS

Yakimova, Ekaterina M. — Ass. Professor, Chair of Constitutional and Administrative Law, Law Institute, Baikal State University, Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: yakimova_katerin@mail.ru.

Narutto, Svetlana V. — Professor, Chair of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: svetanarutto@yandex.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Якимова Е.М. Международное сотрудничество в борьбе с киберпреступностью / Е.М. Якимова, С.В. Нарутто // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 2. — С. 369–378. — DOI : 10.17150/1996-7756.2016.10(2).369-378.

BIBLIOGRAPHIC DESCRIPTION

Yakimova E.M., Narutto S.V. International cooperation in cybercrime counteraction. *Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 369–378. DOI: 10.17150/1996-7756.2016.10(2).369-378. (In Russian).