**МЕЖДУНАРОДНАЯ БОРЬБА С ПРЕСТУПНОСТЬЮ**

DOI: https://doi.org/10.24833/0869-0049-2020-2-77-87

Исследовательская статья
Поступила в редакцию: 12.02.2020
Принята к публикации: 19.05.2020

**Екатерина Александровна АРХИПОВА**
Университет прокуратуры Российской Федерации
Азовская ул., д. 2-1, Москва, 117638, Российская Федерация
e.arkhipova@bk.ru
ORCID: 0000-0002-0358-3438

**Вячеслав Николаевич ДОДОНОВ**
Университет прокуратуры Российской Федерации
Азовская ул., д. 2-1, Москва, 117638, Российская Федерация
2596619@mail.ru
ORCID: 0000-0001-8923-2286

# МЕЖДУНАРОДНО-ПРАВОВЫЕ ПРОБЛЕМЫ СОТРУДНИЧЕСТВА ПРИ ВЫЯВЛЕНИИ, РАССЛЕДОВАНИИ И ПРЕДУПРЕЖДЕНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**ВВЕДЕНИЕ.** *В настоящей работе на основе анализа международных актов, а также практики их применения рассматриваются проблемы международно-правового регулирования взаимодействия при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации.*

**МАТЕРИАЛЫ И МЕТОДЫ.** *Материал для исследования включает соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. и в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г., а также другие международно-правовые документы в рассматриваемой сфере. В работе использованы сравнительно-правовой, сравнительно-исторический и другие научные методы познания общего и частного характера.*

**РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ.** *Результатом проведенного исследования является общая оценка состояния международно-правовой базы взаимодействия государств при выявлении, рас-*

*следовании и предупреждении преступлений в информационно-телекоммуникационной сфере, а также анализ той ее части, которая имеет юридическую силу для Российской Федерации. Раскрыты структура, проблемные моменты и направления развития международно-правового регулирования в указанной сфере.*

**ОБСУЖДЕНИЕ И ВЫВОДЫ.** *На основе проблемного анализа современного опыта международно-правового регулирования сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации, авторы пришли к выводу, что существующая международно-правовая база для такого сотрудничества носит недостаточный характер и нуждается в совершенствовании как на универсальном, так и на региональном уровне.*

**КЛЮЧЕВЫЕ СЛОВА:** *информационно-телекоммуникационные сети, киберпреступность, компьютерная информация, компьютерные преступления, борьба с преступлениями в сфере высоких технологий, международное сотрудничество, СНГ*

**ДЛЯ ЦИТИРОВАНИЯ:** Архипова Е.А., Додонов В.Н. 2020. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации. – *Московский журнал международного права.* № 2. С. 77–87. DOI: https://doi.org/10.24833/0869-0049-2020-2-77-87

*Авторы заявляют об отсутствии конфликта интересов.*

**INTERNATIONAL CRIMINAL LAW**

DOI: https://doi.org/10.24833/0869-0049-2020-2-77-87

Research article
Received 12 March 2020
Approved 19 May 2020

**Ekaterina A. ARKHIPOVA**
University of Prosecutor's Office of the Russian Federation
2-1, ul. Azovskaya, Moscow, Russian Federation, 117638
e.arkhipova@bk.ru
ORCID: 0000-0002-0358-3438

**Vyacheslav N. DODONOV**
University of Prosecutor's Office of the Russian Federation
2-1, ul. Azovskaya, Moscow, Russian Federation, 117638
2596619@mail.ru
ORCID: 0000-0001-8923-2286

# INTERNATIONAL LEGAL PROBLEMS OF COOPERATION IN THE DETECTION, INVESTIGATION AND PREVENTION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS AND IN THE FIELD OF COMPUTER INFORMATION

**INTRODUCTION.** *Based on the analysis of international acts, as well as the practice of their application, the authors consider the international legal problems of interaction in the detection, investigation and prevention of crimes committed using information and telecommunication networks and in the field of computer information.*

**MATERIALS AND METHODS.** *The materials for the study include the Agreement on cooperation of the CIS member States in the fight against crimes in the field of computer information of June 1, 2001, the Agreement on cooperation of the CIS member States in the fight against crimes in the field of information technology of September 28, 2018, as well as other international legal documents in this area. The paper uses comparative, comparative-historical and other scientific methods of research, general and particular ones.*

**RESEARCH RESULTS.** *The result of the study is a general assessment of the state of the international legal framework for the interaction of countries in the detection, investigation and prevention of crimes in the information and telecommunication sector, as well as an analysis of the part of it that has legal force for the Russian Federation. The structure, problems and directions of development of international legal regulation in this area are revealed.*

**DISCUSSION AND CONCLUSIONS.** *Based on the problematic analysis of the current experience of international legal regulation of cooperation in the fight against crimes committed using information and telecommunication networks and in the field of computer information, the authors concluded that the existing international legal framework for such cooperation is insufficient and needs to be improved both at the universal and regional level.*

**KEYWORDS:** *information and telecommunication networks, cybercrime, computer information, computer crimes, fighting crimes in the field of high technologies, international cooperation, CIS*

**FOR CITATION:** Arkhipova E.A., Dodonov V.N. International Legal Problems of Cooperation in the Detection, Investigation and Prevention of Crimes Committed Using Information and Telecommunication Networks and in the Field of Computer Information. – *Moscow Journal of International Law.* 2020. No. 2. P. 77–87. DOI: https://doi.org/10.24833/0869-0049-2020-2-77-87

*The authors declare the absence of conflict of interest.*

## 1. Введение

Компьютерная преступность является одним из самых специфических, сложно устроенных и динамично развивающихся видов преступности. Современная киберпреступность – серьезная угроза как для отдельных государств, так и для всего мирового сообщества [Бессонов 2013:232; Волеводз 2002:47].

Преступления в сфере высоких технологий имеют глобальный характер и элементы транснациональности, что делает международное сотрудничество ключевым фактором принятия эффективных мер противодействия.

Основными целями международного сотрудничества являются:

1) совершенствование международно-правового регулирования в соответствующей области;

2) гармонизация национальных законодательств на основе международных норм и рекомендаций;

3) достижение единства (координации) действий государств в лице национальных правоохранительных органов при выявлении, расследовании и предупреждении преступлений.

Как и в других сферах, сотрудничество государств в борьбе с рассматриваемым видом преступности базируется на конвенциальном (договорно-правовом) и институциональном (в рамках международных организаций) механизмах.

## 2. Международно-правовая база сотрудничества

Современное состояние международного сотрудничества в борьбе с киберпреступлениями характеризуется следующими особенностями:

- тенденцией к фрагментации сотрудничества в рамках региональных организаций и интеграционных объединений, создающих свои механизмы сотрудничества [Волеводз 2001:29];
- отсутствием четкого понимания явления и общих определений основных используемых понятий, в том числе в научном дискурсе;
- наличием правового вакуума, при котором развитие законодательной базы суще-

ственно отстает от эволюции информационно-коммуникационных технологий (далее – ИКТ), состоящей в том числе в появлении новых форм киберпреступности;

– противоречиями между государствами по вопросам процедур сотрудничества, затрагивающих принцип суверенитета [Шматкова 2016:720].

Универсальными международными документами в рассматриваемой области выступили Конвенция Совета Европы о киберпреступности, заключенная в Будапеште 23 ноября 2001 г. (далее – Будапештская конвенция), а также Протокол к ней от 28 января 2003 г., добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающей к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности[1].

Несмотря на название указанных документов, к их реализации присоединились также более 20 государств, не являющихся членами Совета Европы, таких как Австралия, Аргентина, Израиль, Маврикий, Канада, США, ЮАР, Япония и др. Таким образом, по состоянию на 1 апреля 2019 г., Конвенцию и протокол к ней ратифицировали 65 государств.

Россия в этом договоре не участвует в силу распоряжения Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»»[2]. Хотя при его подписании Россия оставляла за собой право определиться с участием в Конвенции при условии возможного пересмотра положений п. «b» ст. 32 данного документа, которые «могут причинить ущерб суверенитету и безопасности государств – участников Конвенции и правам их граждан». Согласно этому пункту договаривающаяся сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему.

Таким образом, в настоящий момент Россия не имеет единого специального договора с ведущими зарубежными странами о борьбе с компьютерными преступлениями, несмотря на тот факт, что наше государство последовательно выступает с инициативой разработки универсальной конвенции по международному противодействию информационной преступности под эгидой ООН[3]. Тем не менее перспективы принятия такого акта остаются пока крайне туманными из-за противодействия западных государств.

В этих условиях в качестве правовой основы для международного взаимодействия при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей, в том числе в сфере компьютерной информации, можно рассматривать узкопрофильные документы договорного характера, которые могут быть применимы в случаях, когда данные виды преступлений совершены с использованием ИКТ. К таким конвенциям можно отнести, к примеру, Конвенцию Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 г. (ст. 7)[4]; Конвенцию ООН против транснациональной организован-

[1] Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. Доступ: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580 (дата обращения: 19.12.2019); Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного акта ксенофобии при помощи информационных систем от 28 января 2003 г. Доступ: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081611 (дата обращения: 19.12.2019).

[2] Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»». Доступ: http://www.kremlin.ru/acts/bank/27059 (дата обращения: 15.12.2019).

[3] Проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» был подготовлен Россией как альтернатива Будапештской конвенции и передан в Генассамблею ООН.

[4] Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 г. – *Справочно-правовая система «Гарант»*. Доступ: http://base.garant.ru/2570351/ (дата обращения: 15.12.2019).

ной преступности от 15 ноября 2000 г. (ст. 29)[5]; Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющий Конвенцию ООН против транснациональной организованной преступности (принят 15 ноября 2000 г. Резолюцией 55/25 Генеральной Ассамблеи ООН)[6].

В рамках СНГ договорно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий базируется на Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. (далее – СПКИ)[7], которое вступило в силу для России 17 октября 2008 г. Договаривающимися сторонами являются Азербайджан, Армения, Беларусь, Казахстан, Киргизия, Молдова, Россия, Таджикистан, Узбекистан, Украина.

В СПКИ определены четыре состава преступления, которые государства – участники Соглашения обязуются закрепить в своем уголовном законодательстве, если они совершены умышленно: (1) неправомерный доступ к охраняемой законом компьютерной информации; (2) создание, использование или распространение вредоносных программ; (3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети; (4) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторских прав.

Наиболее детальную регламентацию в СПКИ получила процедура направления и исполнения запроса об оказании содействия (ст. 6–8).

СПКИ основано на традиционном представлении о правовой помощи. Так, В.П. Талимончик справедливо относит данный факт к числу недостатков указанного Соглашения. Он пишет: «Вызывает удивление, что система электронных запросов на оказание правовой помощи не нашла своего применения в рамках СНГ. Поразительным является тот факт, что СПКИ... основано также на традиционном представлении о правовой помощи. Оно вкратце упоминает о новых технологиях при направлении запроса о правовой помощи, не упоминая о них при ответе» [Талимончик 2008:29].

В научной литературе отмечены и другие явные недочеты СПКИ:

1) в договоре, координирующем международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации, не учтена природа данного вида преступлений, хотя такой документ должен содержать нормы, закрепляющие специальные процессуальные формы сотрудничества;

2) не называются компетентные органы для работы с запросами. В ч. 1 ст. 4 СПКИ говорится, что сотрудничество между сторонами в рамках настоящего Соглашения осуществляется между компетентными органами непосредственно. В то же время установление четкого списка уполномоченных для сотрудничества органов могло бы упростить применение Соглашения ;

3) в ст. 7 СПКИ, которая посвящена процедуре исполнения запросов, во-первых, не содержится четко определенных случаев, когда исполнение запроса может быть приостановлено. Во-вторых, несмотря на специфику преступлений в сфере высоких технологий, ст. 6 требует обязательного письменного подтверждения запроса;

4) соглашением не рассматривается такая перспективная процессуальная форма сотрудничества, как создание совместных следственных групп;

5) наконец, СПКИ не предусматривает положений для решения ряда вопросов, затрагивающих суверенитет государства (вопросы конкурирующей юрисдикции, передачи уголовного производства) [Мороз 2016:12].

Как видно, договорно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках СНГ нуждалось в улучшении. Учитывая правовые недочеты СПКИ, 28 сентября 2018 г. государства – участники СНГ заключили Соглашение о сотрудничестве в борь-

[5] Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г. – *Справочно-правовая система «Гарант»*. Доступ: http://base.garant.ru/2561303/ (дата обращения: 15.12.2019).

[6] Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности от 15 ноября 2000 г. – *Справочно-правовая система «Гарант»*. Доступ: http://base.garant.ru/12126241/ (дата обращения: 15.12.2019).

[7] Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. – *Собрание законодательства РФ*. 2009. № 13. Ст. 1460.

[8] В соответствии с Нотой МИД России от 3 августа 2015 г. № 6839/1дснг и Нотой Исполнительного комитета СНГ от 10 августа 2015 г. № 3-1/919 Следственный комитет Российской Федерации является компетентным органом.

бе с преступлениями в сфере информационных технологий (далее – Соглашение 2018 г.)[9]. Договаривающимися сторонами в данном Соглашении выступают Армения, Беларусь, Казахстан, Киргизия, Россия, Таджикистан, Узбекистан. Отметим существенно суженный состав участников по сравнению с СПКИ.

В настоящее время в Российской Федерации проходит процедура ратификации данного Соглашения. С момента вступления в силу этого документа для ратифицировавших его государств утратит силу СПКИ (в отношениях между государствами – участниками Соглашения).

В новом Соглашении устранен ряд недостатков предыдущего документа: название акта более точно отражает предмет регулирования; более полно даны определения всех значимых понятий; расширен круг уголовно наказуемых деяний в сфере информационных технологий. Так, согласно ч. 1 ст. 3 нового Соглашения стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния в сфере информационных технологий, если они совершены умышленно:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

Сохраняя общее правило о письменной форме запроса об оказании содействия, Соглашение 2018 г. все же допускает, что «запрос и материалы исполненного запроса могут передаваться по техническим каналам связи в случае, если об этом есть двусторонняя договоренность между компетентными органами Сторон либо эти каналы определены иными международными договорами, участниками которых являются Стороны» (ч. 2 ст. 6).

Перспективным для России является развитие международного сотрудничества в борьбе с компьютерными преступлениями в формате Шанхайской организации сотрудничества (далее – ШОС). В связи с этим можно упомянуть Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.). В числе основных направлений сотрудничества в этом документе названы противодействие угрозам использования информационно-коммуникационных технологий в террористических целях и противодействие информационной преступности (ст. 3 Соглашения). После вступления Соглашения в силу стороны приступили к его практической реализации: была начата работа по выстраиванию комплексного механизма взаимодействия шести

[9] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. – *Справочно-правовая система «Гарант»*. Доступ: http://base.garant.ru/72087644/#help (дата обращения: 15.09.2019).

стран-участников (помимо России, это Соглашение подписали Казахстан, Китай, Кыргызстан, Таджикистан, Узбекистан).

В 2018 г. страны – участники ШОС договорились об организации мониторинга террористических угроз в Интернете в рамках работы Совета региональной антитеррористической структуры (РАТС).

Международное взаимодействие России с иностранными государствами по вопросам сотрудничества в борьбе с преступлениями в сфере высоких технологий осуществляется также на основании двусторонних межправительственных соглашений. К числу таких документов можно отнести Соглашение между Правительством РФ и Правительством Французской Республики о сотрудничестве в борьбе с преступностью и в области внутренней безопасности от 10 февраля 2003 г., в ст. 1 которого прямо предусмотрено техническое и оперативное сотрудничество в борьбе с преступлениями в сфере компьютерной информации, в том числе связанными с использованием Интернета и других средств связи[10].

Сотрудничество в области информационной безопасности и вопросов, касающихся киберпреступности предусмотрено Соглашением между Правительством РФ и Правительством Малайзии о сотрудничестве в области информационных и коммуникационных технологий от 5 августа 2003 г.[11]

Отмечая значительный прогресс, достигнутый в развитии и внедрении новейших информационно-коммуникационных технологий, Российская Федерация и Республика Индия заключили в 2016 г. межправительственное соглашение о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий[12].

Сотрудничество в правоохранительной области в целях расследования дел, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях, закреплено также в Соглашении между Правительством РФ и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 6 сентября 2018 г.[13]

Взаимодействие компетентных органов иностранных государств в борьбе с преступлениями в сфере компьютерной информации предусмотрено также Соглашением между Правительством РФ и Правительством Королевства Бельгии о сотрудничестве в борьбе с преступностью от 20 декабря 2000 г.[14] К сожалению, до настоящего времени это Соглашение не вступило в силу в соответствии со ст. 19, предусматривающей направление и получение сторонами уведомлений о выполнении внутригосударственных процедур, необходимых для его вступления в силу. Соглашение между Правительством РФ и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 14 мая 2010 г., разработанное сторонами в русле реализации положений резолюции Генеральной Ассамблеи ООН от 2 декабря 2009 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[15], а также в целях противостояния угрозам международной информационной и коммуникационной без-

[10] Соглашение между Правительством РФ и Правительством Французской Республики о сотрудничестве в борьбе с преступностью и в области внутренней безопасности от 10 февраля 2003 г. – *Бюллетень международных договоров.* 2005. № 8. С. 62.

[11] Соглашение между Правительством РФ и Правительством Малайзии о сотрудничестве в области информационных и коммуникационных технологий от 5 августа 2003 г. – *Бюллетень международных договоров.* 2004. № 1. С. 77.

[12] Соглашение между Правительством РФ и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий от 15 октября 2010 г. – *Бюллетень международных договоров.* 2017. № 4. С. 83–88.

[13] Соглашение между Правительством РФ и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 6 сентября 2018 г. – *Официальный интернет-портал правовой информации.* Доступ: http://publication.pravo.gov.ru/Document/View/0001201904290008 (дата обращения: 22.12.2019).

[14] Соглашение между Правительством РФ и Правительством Королевства Бельгии о сотрудничестве в борьбе с преступностью от 20 декабря 2000 г. – *Справочно-правовая система «Гарант».* Доступ: http://base.garant.ru/71672372/ (дата обращения: 26.12.2019).

[15] Резолюция, принятая Генеральной Ассамблеей ООН на 64-й сессии 2 декабря 2009 г. (по докладу Первого комитета (A/64/386)), 64/25 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Доступ: https://undocs.org/ru/A/RES/64/25 (дата обращения: 17.11.2019).

опасности, не вступило в силу по тем же основаниям (ст. 11).

В правовом пространстве международного взаимодействия государств в борьбе с преступлениями в сфере высоких технологий важное место занимают и межведомственные договоренности с компетентными органами иностранных государств. В их числе можно упомянуть следующие документы:

– Соглашение между Правительством РФ и Правительством Греческой Республики о сотрудничестве МВД России и Министерства общественного порядка Греческой Республики в области борьбы с преступностью (Афины, 6 декабря 2001 г.)[16];

– Меморандум о взаимопонимании между Следственным комитетом РФ и Полицией Государства Израиль (Тель-Авив, 15 ноября 2012 г.)[17];

– Меморандум о взаимопонимании между Следственным комитетом при прокуратуре РФ и Министерством внутренней безопасности США в лице Службы иммиграционных и таможенных расследований США (Вашингтон, 26 марта 2010 г.)[18].

В первом из этих договоров предусмотрено, что компетентные органы сторон будут осуществлять взаимодействие в предупреждении, выявлении, пресечении и раскрытии «преступлений в сфере высоких технологий, включая компьютерные преступления». В втором и третьем в качестве одной из областей, в которой стороны выражают стремление к сотрудничеству, названа борьба с «мошенничеством, совершаемым с использованием компьютерной техники».

Несмотря на вариативность правовых норм, сегодня назрела необходимость принятия международного правового акта, направленного на уголовно-правовую охрану информационной безопасности, содержащего классификацию преступлений против информационной безопасности и рекомендации государствам по криминализации деяний против информационной безопасности в национальном законодательстве[19].

### 3. Институциональная база сотрудничества

Международные организации, такие как ОЭСР, Совет Европы, РАТС, Европейский союз, ООН и Интерпол, играют важную роль в выработке единого подхода, координации международных усилий и выстраивании международного сотрудничества в борьбе с преступлениями в сфере высоких технологий. Так, например, первое всестороннее исследование проблемы киберпреступности и уголовно-правовых мер по борьбе с ней в международном масштабе было предпринято ОЭСР, которая проанализировала возможности гармонизации норм, предусматривающих уголовную ответственность за киберпреступления, а также представила криминологическое определение компьютерного преступления[20].

Интерпол ввел в обиход кодификатор компьютерных преступлений и способов их совершения, которым присвоил каждому компьютерному преступлению определенный буквенный индекс, расположив их в порядке уменьшения общественной опасности совершенного деяния [Русскевич 2018:113].

Большое значение для взаимодействия государств — участников Европейского союза имеет деятельность Европола и Евроюста, принимающих непосредственное участие в борьбе с киберпреступностью на пространстве Европейского союза [Шматкова, Волеводз 2017:156]. В работе Европола используется система аналитических рабочих картотек (analysis work files), формируемых из сосредоточенных в его информационной системе данных в целях анализа, определяемого как обработка или использование данных для поддержки уголовных расследований [Волеводз, Дамирчиев 2011:118-119]. Система действующих аналитических картотек включает картотеку по киберпреступности *Cyborg* [Якимова, Нарутто 2016:371].

---

[16] См.: Соглашение между Правительством РФ и Правительством Греческой Республики о сотрудничестве Министерства внутренних дел РФ и Министерства общественного порядка Греческой Республики в области борьбы с преступностью от 6 декабря 2001 г. – *Бюллетень международных договоров.* 2004. № 12. С. 61–66.

[17] Меморандум о взаимопонимании между Следственным комитетом РФ и Полицией Государства Израиль от 15 ноября 2012 г. – *Справочно-правовая система «Гарант».* Доступ: http://base.garant.ru/71679482/ (дата обращения: 11.12.2019).

[18] Текст документа не опубликован в открытых источниках.

[19] Ефремова М.А. Уголовно-правовая охрана информационной безопасности: Автореф. дис. ... докт. юрид. наук. М. 2018. С. 12.

[20] Computer-Related Crime: Analysis of Legal Policy. Paris: OECD. 1986.

Формирование единого решения проблемы компьютерной преступности на региональном уровне было реализовано Комитетом министров Совета Европы[21], который определил минимально необходимый к включению в национальное законодательство список киберпреступлений. Кроме того, в рамках Совета Европы успешно действуют Европейская группа по обучению и борьбе с киберпреступностью и Европейский комитет по проблемам преступности, основными задачами которых являются оказание содействия государствам-участникам в гармонизации законодательств в сфере киберпреступности и получении электронных доказательств, расширение возможностей для эффективного международного сотрудничества в этой области.

Деятельность Межправительственной группы экспертов открытого состава по киберпреступности в рамках ООН, созданной по инициативе Российской Федерации по итогам XII Конгресса ООН по предупреждению преступности и уголовному правосудию (Салвадор, 2010 г.) [Волеводз, Тарасенко 2010:4], также направлена на наращивание потенциала в борьбе с киберпреступностью путем информационной и консультативной поддержки национальных компетентных органов и их взаимодействия с зарубежными партнерами. Вместе с тем Управление ООН по наркотикам и преступности использует свой специализированный опыт в области реагирования систем уголовного правосудия для оказания технической помощи в предупреждении киберпреступлений и повышении осведомленности о них, международном сотрудничестве, а также в сборе данных, исследованиях и анализе в области киберпреступности.

## 4. Заключение

В свете вышеизложенного представляется, что основные меры по борьбе с преступностью в сфере высоких технологий, принимаемые на международном уровне, должны быть связаны с действиями по реформированию законодательства на национальном уровне. Национальные и международные усилия должны дополнять друг друга, обеспечивая тем самым координацию шагов по борьбе с киберпреступностью и гармонизацию национальных законодательств.

Впрочем, на этом пути остается пока немало нерешенных проблем. Как справедливо отмечает Т.Л. Тропина, имеющиеся международные инструменты, направленные на обеспечение кибербезопасности, характеризуются мозаичностью, являются фрагментарными и, скорее, конкурируют между собой, что не способствует гармонизации уголовного и уголовно-процессуального законодательств государств [Тропина 2012:86].

Следует также согласиться с утверждением, что международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Именно поэтому требуется, «чтобы на решение вопросов кибербезопасности были обращены совместные усилия различных субъектов, как государственных, так и частных» [Huey, Nhan, Broll. 2013:81]. На сегодняшний день большинство государств вынуждены ««на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам»[22].

Таким образом, можно констатировать, что международно-правовая база для борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации, сегодня носит недостаточный, фрагментарный характер и нуждается в совершенствовании как на универсальном, так и на региональном уровне. Основным препятствием на этом пути является несогласованность позиций государств по ряду вопросов, наиболее существенным из которых является допустимая степень ограничения национального суверенитета в сфере регулирования киберпространства. При этом следует учитывать, что традиционные механизмы международного сотрудничества, включая запросы, взаимопомощь и другие подобные инструменты, применявшиеся в XIX в. и ранее, являются не-

[21] 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). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f1094 (accessed 12.12.2019).

[22] Пункт 17 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203. Доступ: http://www.kremlin.ru/acts/bank/41919/page/3 (дата обращения: 10.05.2019).

подходящими в эру, когда преступления могут совершаться из любой точки земного шара со скоростью света [Smith, Grabosky, Urbas 2004:60].

Вместе с тем 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%. 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» [Карпова 2014:46].

**Список литературы**


1. Бессонов С.А. 2013. История и зарубежный опыт правовой регламентации компьютерных преступности. – *Территория науки*. № 2. С. 231–237.
2. Волеводз А.Г. 2002. *Противодействие компьютерным преступлениям: правовые основы международного сотрудничества.* М.: ООО Издательство «Юрлитинформ». 496 с.
3. Волеводз А.Г. 2001. Международно-правовые основы международного сотрудничества в обнаружении, отслеживании, сохранении и изъятии компьютерной информации. – *Международное публичное и частное право.* № 4. С. 28 – 41.
4. Волеводз А., Дамирчиев Э. 2011. Европейская полицейская организация в свете Лиссабонского договора. – *Уголовное право.* № 2. С. 114-120.
5. Волеводз А.Г., Тарасенко С.М. 2010. К итогам XII Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. – *Международное уголовное право и международная юстиция.* № 4. С. 3 - 5.
6. Карпова Д.Н. 2014. Киберпреступность: глобальная проблема и ее решение. – *Власть*. № 8. С. 46–50.
7. Мороз Н.О. 2016. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ. – *Международное уголовное право и международная юстиция*. № 3. С. 12–14.
8. Мысина А.И. 2019. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий. – *Международное право.* № 1. С. 18–27. DOI: 10.25136/2306-9899.2019.1.29027
9. Ревин В.П. 2017. Актуальные проблемы сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий. – *Международное сотрудничество Евразийских государств: политика, экономика, право.* № 1. С. 83–91.
10. Русскевич Е.А. 2018. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. – *Международное уголовное право и международная юстиция.* № 3. С. 10–13.
11. Талимончик В.П. 2008. Конвенция о киберпреступности и унификация законодательства. – *Информационное право.* № 2. С. 27–30.
12. Тропина Т.Л. 2012. Борьба с киберпреступностью: возможна ли разработка универсального механизма? – *Международное правосудие.* № 3. С. 86–95.
13. Шматкова Л.П. 2016. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы. – *Молодой ученый.* № 28. С. 720–723.
14. Шматкова Л.П., Волеводз А.Г. 2017. Формирование и современный этап совершенствования правового регулирования противодействия киберпреступлениям в Европейском союзе. – *Библиотека уголовного права и криминологии.* № 3. С. 154-159.
15. Якимова Е.М., Нарутто С.В. 2016. Международное сотрудничество в борьбе с киберпреступностью. – *Криминологический журнал Байкальского государственного университета экономики и права.* Т. 10. № 2. С. 369–378. DOI: 17150/1996-7756.2016.10(2).369-378
16. Huey L., Nhan J., Broll R. 2013. 'Uppity Civilians' and 'Cyber-Vigilantes': The role of the general public in policing cyber-crime. – *Criminology and Criminal Justice.* Vol. 13. No. 1. P. 81–97. DOI: 10.1177/1748895812448086.
17. Smith R.G., Grabosky P., Urbas G. 2004. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press. 263 p. DOI: https://doi.org/10.1017/CBO9780511481604


**References**


1. Bessonov S.A. Istoriya i zarubezhnyi opyt pravovoi reglamentatsii komp'yuternykh prestupnosti [History and Foreign Experience in the Legal Regulation of Computer Crime]. – Territoriya nauki. 2013. No. 2. P. 231–237. (In Russ.)
2. Huey L., Nhan J., Broll R. Uppity Civilians and Cyber-Vigilantes: The role of the general public in policing cybercrime. – *Criminology and Criminal Justice.* 2013. Vol. 13. No. 1. P. 81–97. DOI: 10.1177/1748895812448086.
3. Karpova D.N. Kiberprestupnost': global'naya problema i ee reshenie [Cybercrime: A Global Challenge and Its Solution]. – *Vlast'*. 2014. No. 8. P. 46–50. (In Russ.)
4. Moroz N.O. Aktual'nye voprosy mezhdunarodnogo sotrudnichestva v bor'be s prestupnost'yu v sfere vysokikh tekhnologii v ramkakh SNG [Topical Issues of International Cooperation in Crime Prevention in the Field of High Technologies within the Framework of the Commonwealth of Independent States (CIS)]. – *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiya.* 2016. No. 3. P. 12–14. (In Russ.)
5. Mysina A.I. Mezhdunarodno-pravovye osnovy sotrudnichestva gosudarstv po protivodeistviyu prestupleniyam v sfere informatsionnykh tekhnologii [International Legal Framework for Cooperation between States in Combating Crimes in the Field of Information Technology]. – *Mezhdunarodnoe pravo.* 2019. No. 1. P. 18–27. (In Russ.) DOI: 10.25136/2306-9899.2019.1.29027

6. Revin V.P. Aktual'nye problemy sotrudnichestva gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v bor'be s prestupleniyami, sovershaemymi s ispol'zovaniem informatsionnykh tekhnologiy [Actual Problems of Cooperation of States – Participants of the Commonwealth of Independent States in Fight against Crimes Committed Using Information Technologies]. – *Mezhdunarodnoe sotrudnichestvo Evraziiskikh gosudarstv: politika, ekonomika, pravo.* 2017. No. 1. P. 83–91. (In Russ.)
7. Russkevich E.A. Mezhdunarodno-pravovye podkhody protivodeistviya prestupleniyam, sovershaemym s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologii [International Law Approaches to Combating Crimes Committed Using Information and Communication Technology]. – *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiya.* 2018. No. 3. P. 10–13. (In Russ.)
8. Shmatkova L.P. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupleniyami: sostoyanie i perspektivy [International Cooperation in the Fight against Cybercrime: state and prospects]. – *Molodoi uchenyi*. 2016. No. 28. P. 720–723. (In Russ.)
9. Shmatkova L.P., Volevodz A.G. Formirovanie i sovremennyi etap sovershenstvovaniya pravovogo regulirovaniya protivodeistviya kiberprestupleniyam v Evropeiskom soyuze. [Formation and current stage of improving legal regulation of countering cybercrimes in the European Union]. – *Biblioteka ugolovnogo prava i kriminologii*. 2017. No. 3. P. 154-159. (In Russ.)
10. Smith R.G., Grabosky P., Urbas G. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press. 2004. 263 p. DOI: https://doi.org/10.1017/CBO9780511481604
11. Talimonchik V.P. Konventsiya o kiberprestupnosti i unifikatsiya zakonodatel'stva [Convention on Cybercrime and the Unification of Legislation]. – *Informatsionnoe pravo*. 2008. No. 2. P. 27–30. (In Russ.)
12. Tropina T.L. Bor'ba s kiberprestupnost'yu: vozmozhna li razrabotka universal'nogo mekhanizma? [Addressing the Problem of Cybercrime: is it possible to develop universal legal framework on the international level?]. – *Mezhdunarodnoe pravosudie*. 2012. No. 3. P. 86–95 (In Russ.)
13. Volevodz A.G. *Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva* [Countering computer crimes: legal framework for international cooperation]. Moscow: OOO Izdatel'stv0o "Yurlitinform" Publ. 2002. 496 p. (In Russ.)
14. Volevodz A.G. Mezhdunarodno-pravovye osnovy mezhdunarodnogo sotrudnichestva v obnaruzhenii, otslezhivanii, sokhranenii i iz"yatii komp'yuternoi informatsi [International legal framework for international cooperation in the detection, tracking, preservation and seizure of computer information]. – *Mezhdunarodnoe publichnoe i chastnoe pravo.* 2001. No. 4. P. 28 – 41. (In Russ.)
15. Volevodz A.G., Tarasenko S.M. K itogam XII Kongressa Organizatsii Ob"edinennykh Natsii po preduprezhdeniyu prestupnosti i ugolovnomu pravosudiyu [Towards the end of the XII United Nations Congress on Crime Prevention and Criminal Justice]. – *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiy.* 2010. No. 4. P. 3 - 5. (In Russ.)
16. Volevodz A., Damirchiev E. Evropeiskaya politseiskaya organizatsiya v svete Lissabonskogo dogovora. [European police organization in the light of the Lisbon Treaty]. – *Ugolovnoe pravo*. 2011. No. 2. P. 114-120. (In Russ.)
17. Yakimova E.M., Narutto S.V. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu [International Cooperation in Cybercrime Counteraction]. – *Criminology Journal of Baikal National University of Economics and Law*. 2016. Vol. 10. No. 2. P. 369–378. (In Russ.) DOI:.17150/1996-7756.2016.10(2).369-378

**Информация об авторах**

**Екатерина Александровна Архипова,**
кандидат юридических наук, старший научный сотрудник отдела научного обеспечения международного сотрудничества прокуратуры и сравнительного правоведения, Университет прокуратуры Российской Федерации

117638, Российская Федерация, Москва, Азовская ул., д. 2-1

e.arkhipova@bk.ru
ORCID: 0000-0002-0358-3438

**Вячеслав Николаевич Додонов,**
кандидат юридических наук, ведущий научный сотрудник отдела научного обеспечения международного сотрудничества прокуратуры и сравнительного правоведения, Университет прокуратуры Российской Федерации

117638, Российская Федерация, Москва, Азовская ул., д. 2-1

2596619@mail.ru
ORCID: 0000-0001-8923-2286

**About the Authors**

**Ekaterina A. Arkhipova,**
Cand. Sci. (Law), Senior Researcher at the Department of Scientific Support for International Cooperation of the Prosecutor's Office and Comparative Law, University of Prosecutor's Office of the Russian Federation

2-1, ul. Azovskaya, Moscow, Russian Federation, 117638

e.arkhipova@bk.ru
ORCID: 0000-0002-0358-3438

**Vyacheslav N. Dodonov,**
Cand. Sci. (Law), Leading Researcher at the Department of Scientific Support for International Cooperation of the Prosecutor's Office and Comparative Law, University of Prosecutor's Office of the Russian Federation

2-1, ul. Azovskaya, Moscow, Russian Federation, 117638

2596619@mail.ru
ORCID: 0000-0001-8923-2286