Научная статья
УДК 343.346
DOI: 10.47475/2311-696X-2024-42-3-96-101

С. 96–101

МЕЖДУНАРОДНЫЕ УСИЛИЯ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Денис Валентинович Пучков
Уральский государственный юридический университет им. В. Ф. Яковлева, Екатеринбург, Россия
d.puchkov@loys.law
https://orcid.org/0000-0002-5318-0338

Аннотация. Изучение преступлений, совершаемых в сфере информационно-коммуникационных технологий, позволяет сделать однозначный вывод об их совершении в неограниченном физическими барьерами информационном пространстве и, как следствие, зачастую за пределами национальных юрисдикций. Данные проявления носят обобщенный характер, затрагивая интересы не отдельного государства или группы государств, а всего мирового сообщества, что актуализирует борьбу с такого рода преступлениями на международном уровне.

Однако в силу различных причин, прежде всего экономических и политических, отдельные страны не имеют надлежащей правовой базы для противодействия преступным посягательствам в данной сфере, в связи с чем юрисдикция данных стран используется для совершения анализируемого вида преступлений, что в условиях отсутствия единого механизма противодействия им нивелирует усилия стран в сфере противодействия преступности в общем и преступлениям в сфере информационно-коммуникационных технологий в частности.

В этой связи актуализируется необходимость разработки унифицированных подходов к формированию нормативной базы и взаимодействию государств в данной сфере, в том числе на основе разработанных для этого международно-правовых соглашений. В статье анализируется развитие международного сотрудничества на примере Организации Объединенных Наций, в связи с рассмотрением проекта всеобъемлющей конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях.

Ключевые слова: преступления в сфере информационно-коммуникационных технологий, трансграничность, конвенционность, юрисдикция, киберпреступность, кибербезопасность, информационная безопасность

Для цитирования: Пучков Д. В. Международные усилия по борьбе с преступлениями в сфере информационно-коммуникационных технологий // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 96–101. DOI: 10.47475/2311-696X-2024-42-3-96-101

Research article

INTERNATIONAL EFFORTS TO COMBAT CRIMES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Denis V. Puchkov
Ural State Law University name after V. F. Yakovlev, Yekaterinburg, Russia
d.puchkov@loys.law
https://orcid.org/0000-0002-5318-0338

Abstract. The study of crimes committed in the field of information and communication technologies allows us to draw an unambiguous conclusion that they are committed in an information space unlimited by physical barriers and, as a result, often outside national jurisdictions. These manifestations are of a generalized nature, affecting the interests not of a single state or a group of states, but of the entire world community, which actualizes the fight against this type of crime at the international level.

However, due to various reasons, primarily economic and political, some countries do not have an appropriate legal framework for countering criminal attacks in this area, and therefore the jurisdiction of these countries is used to commit the type of crimes under analysis, which, in the absence of a unified mechanism for countering them, is leveled out countries' efforts to combat crime in general and crimes in the field of information and communication technologies in particular.

In this regard, the need to develop unified approaches to the formation of a regulatory framework and interaction between states in this area is becoming urgent, including on the basis of international legal agreements developed for this purpose. The article analyzes the development of international cooperation using the example of the United Nations, in connection with the consideration of the draft Comprehensive Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes.

Keywords: crimes in the field of information and communication technologies, transnationality, conventionality, jurisdiction, cybercrime, cybersecurity, information security

For citation: Puchkov DV. International efforts to combat crimes in the field of information and communication technologies. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(3):96-101. (In Russ.) DOI: 10.47475/2311-696X-2024-42-3-96-101

Введение

Наряду с крайне положительным влиянием технологий на человечество в различных сферах его жизнедеятельности, включая социальную, экономическую, культурную и даже религиозную, следует признать и негативные аспекты их развития. С этих позиций актуализируется задача по изучению преступного поведения в сфере информационно-коммуникационных технологий и проблем противодействия преступности в данной сфере.

Одной из таких проблем стала доступность и анонимность информационного пространства, включая глобальную сеть Интернет, что фактически привело к отсутствию какого-либо контроля в данной среде со стороны государств. В тоже время трансграничность данного вида преступности на фоне различия уголовно-правового потенциала противодействия ей со стороны отдельных государств акцентно смещает киберпреступность в юрисдикции с наименее развитой нормативно-правовой базой, хотя последствия совершенных киберпреступлений распространяются далеко за пределы этих юрисдикций. В этой связи преступления в сфере информационно-коммуникационных технологий приобретают международный (конвенционный) характер как посягающие на интересы всего мирового сообщества.

Отсутствие же единого подхода к преступным проявлениям, относимым к заявленной тематике, порождает появление правовых лагун, используемых, в первую очередь, организованной преступностью, что лишь повышает характер и степень их общественной опасности, препятствует эффективной борьбе с преступлениями в данной сфере и говорит о необходимости унификации как понятийного аппарата, так и подходов к межгосударственному взаимодействию по противодействию преступлениям в сфере информационно-коммуникационных технологий.

Материалы и методы

В статье использованы международные и национальные нормативно-правовые акты, регламентирующие вопросы уголовно-правового противодействия преступлениям в сфере информационно-коммуникационных технологий, специальная литература по предмету исследования. Основу исследования составили общенаучные и частнонаучные методы научного познания, анализ теоретических и нормативных правовых источников, статистический, герменевтический методы.

Описание исследования

Необходимость усиления борьбы с преступностью и объединения всех заинтересованных сторон стали одними из основных тем на проходивших в 2005 г. XI и в 2010 г. XII конгрессах Организации Объединенных Наций, посвященных вопросам предупреждения преступности. Подобная активность ознаменовалась принятием на XII Конгрессе ООН Резолюции Генеральной Ассамблеи от 21 декабря 2010 г. № 65/230, содержащей Сальвадорскую декларацию о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире[1].

Помимо этого, одним из итогов работы XII Конгресса по предупреждению преступности и уголовному правосудию явилось также принятие решения о формировании межправительственной группы экспертов с открытым составом, целью которой было определено исследование проблемы киберпреступности, создание ответных мер международным сообществом, государствами — членами ООН и частного сектора [5, с. 176].

Одним из промежуточных итогов заявленных ООН целей по противодействию киберпреступности явилось разработка в 2011 г. Конвенции ООН об обеспечении международной информационной безопасности, представленной на конференции по киберпространству в Лондоне, состоящей из преамбулы, 23 статей, объединенных в основную часть, и заключительных положений. Несомненно важным моментом данного документа явилось закрепление в ст. 4 основных угроз международному миру и безопасности, возникающих в информационном пространстве, включающих в себя:

— использование информационных технологий и средств для осуществления враждебных действий и актов агрессии;

— трансграничное распространение информации, противоречащей принципам и нормам как международного права, так и национальному законодательству государства;

— целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства»[2].

Несмотря на позитивную оценку данного документа, можно отметить его исключительно общий характер, в то время как каждое государство сталкивается

[1] Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире : принята резолюцией 65/230 Генеральной Ассамблеи от 21 декабря 2010 г. // Организация Объединенных Наций : Декларации. URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml (дата обращения: 07.03.2024).

[2] Конвенция ООН об обеспечении международной информационной безопасности (концепция) // Совет Безопасности Российской Федерации : [сайт]. URL: http://www.scrf.gov.ru/security/information/Inf_conc/ (дата обращения: 07.03.2024).

с конкретными проявлениями использования информационно-коммуникационных технологий при совершении преступлений, связанных с оборотом наркотических средств и психотропных веществ, изготовлением и оборотом порнографии, включая детскую и пр.

Другим значимым международным актом, направленным на противодействие киберпреступлениям, стала Будапештская конвенция Совета Европы от 23 ноября 2001 г. «О преступлении в сфере компьютерной информации»[1]. Указанную Конвенцию можно отнести к одной из наиболее строгих мер международного противодействия компьютерным преступлениям. Ратифицируя Конвенцию или присоединяясь к ней, государства соглашаются обеспечить криминализацию действий в их национальном законодательстве, описанных в разделе основ уголовного права. Государства должны оценить целесообразность внедрения стандартов и принципов Конвенции и использовать Конвенцию в качестве ориентира или в качестве справочного пособия для разработки своего внутреннего законодательства. Но при этом следует учитывать, что Конвенция основана на криминальном киберповедении, сложившемся в конце 1990-х гг., что на фоне его существенной трансформации к настоящему моменту, несомненно, отражается и на позитивном потенциале данного документа.

Международные стандарты кибербезопасности еще далеки от идеальных и четких понятий и стандартов, что говорит о необходимости актуализации работы в данном направлении [1; 2; 3]. В этой связи безусловно положительно можно оценить усилия РФ и КНР, еще в 2010 г. предложивших проект глобальной конвенции по борьбе с киберпреступностью, несмотря на то, что по многим, в том числе и конъюнктурным причинам, в последующем проект был отклонен.

Но, осознавая насущность объединения усилий государств в противодействии киберпреступности, уже в 2017 г. Россией в адрес Генерального секретаря Организации Объединенных Наций был направлен проект концепции конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, включающий в том числе и перечень преступных посягательств, предлагаемых к криминализации[2].

Такого рода предложения Российской Федерации были направлены на разрешение фундаментальных проблем в выработке единых уголовно-правовых моделей защиты телекоммуникации, таких как различия в терминологическом и понятийном аппарате; непонимание отграничения одного явления от другого (это важно при определении механизма взаимодействия); отсутствие доверительных отношений между странами.

На практике все эти факторы приводят к попыткам лишь на техническом уровне защитить телекоммуникации от преступных посягательств, зачастую оставляя без внимания правовые аспекты. В Доктрине информационной безопасности РФ в связи с этим отмечено: «Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства. Следовательно, государства на национальном уровне вынуждены самостоятельно формировать границы кибербезопасности для защиты своих информационных ресурсов»[3]. При этом, например, стремление развивающихся стран сократить цифровое отставание через инвестиции только лишь в инфраструктуру, без учета необходимости обеспечения правовой, в том числе и уголовно-правовой защиты кибертехнологий, приведет к созданию разрыва в информационно-телекоммуникационной сфере как наносящего ущерб развивающимся странам в качестве специального фактора [6, с. 6]. Таким образом, необходимо, чтобы страны не только вводили меры для борьбы с киберпреступностью и контролировали безопасность своей инфраструктуры и информационных технологий, но и осуществляли это в соответствии с интересами всего мирового сообщества и в рамках правил и процедур, обеспечивающих это, что в очередной раз говорит о необходимости их разработки и принятия мировым сообществом.

В этой связи крайне важным документом является доклад Генерального секретаря ООН от 30 июля 2019 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[4], в котором страны-участницы высказались о существующих уголовно-правовых проблемах регулирования киберпреступности в их странах, отразивший во многом сходные риски, а именно: повышение уровня подготовки киберпреступников, в том числе повышение уровня анонимности пользователей (Австрия, Аргентина, Чехия и др.); потребность пересмотра действующего уголовного и уголовно-процессуального законодательства (Боливия, Китай, Чехия, Франция и др.); сложности в проведении

[1] О преступлении в сфере компьютерной информации : заключена в Будапеште 23 ноября 2001 г. // СПС «Гарант».URL: http://base.garant.ru/4089723/ (дата обращения: 07.03.2024).

[2] Письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций от 11 октября 2017 г. на имя Генерального секретаря : пункт 107 повестки дня, 72-й сессия Генеральной Ассамблеи ООН. 16 октября 2017 г. URL: https://undocs.org/ru/A/C.3/72/12 (дата обращения: 07.03.2024).

[3] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[4] Противодействие использованию информационно-коммуникационных технологий в преступных целях : доклад Генерального секретаря ООН : 74-я сессия Генеральной Ассамблеи ООН 30 июля 2019 г. URL: http://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 07.03.2024).

уголовных расследований в ситуациях, не охватываемых международными соглашениями (Австралия, Бразилия, Эстония, Гана и др.); ограниченная эффективность взаимной правовой помощи (Швейцария, Тайланд, США, Австралия и др.); недостаточная доступность электронных доказательств и (или) их безопасность (Аргентина, Китай, Германия и др.); недостаточная квалификация сотрудников правоохранительных органов, не обладающих специальными познаниями в сфере ИКТ (Индия, Венгрия, Малайзия, Саудовская Аравия и др.) [5, с. 169–170].

Тем не менее можно говорить о том, что нормативное правовое регулирование возникающих в сфере реализации кибернетических технологий отношений с позиции уголовно-правовой сферы постоянно стремится достичь существующего уровня развития кибернетических технологий, демонстрируя тем самым свою неадекватность. Установленная в настоящее время в уголовном законе ответственность за совершение киберпреступлений не способна в полной мере отразить динамику технологических перемен и возможностей, вызванных ускоренным ростом информационного развития человечества. Уголовное законодательство осуществляет регулирование возникающих в сфере реализации кибертехнологий отношений на более низком уровне, чем требует социальный и технологический прогресс современного общества, вследствие чего не реализуются его охранительная и предупредительная функции. Более того, имеются различные подходы в определении родового объекта киберпреступлений, в разных странах им определены сфера экономической деятельности, собственности, информационной безопасности и компьютерной информации.

Генеральная Ассамблея ООН

— отмечая данные обстоятельства, и что информационно-коммуникационные технологии, имея огромный потенциал для развития государств, создают новые возможности для преступников и могут способствовать повышению уровня и сложности преступности,

— отмечая также потенциальный риск злоупотребления новыми технологиями [4], включая искусственный интеллект,

— признавая при этом их потенциал в предотвращении и борьбе с использованием информационно-коммуникационных технологий в преступных целях и обеспокоенность ростом и разнообразием преступлений, совершенных в цифровом мире, и их влиянием на стабильность критической инфраструктуры государств и предприятий и на благополучие отдельных лиц,

— признавая, что различные преступники, в том числе торговцы людьми, пользуются информацией и коммуникационными технологиями для осуществления преступной деятельности,

— подчеркивая необходимость укрепления координации и сотрудничества между государствами в борьбе с использованием информационно-коммуникационных технологий в уголовных целях, в том числе путем предоставления технической помощи развивающимся странам по их просьбе для улучшения национального законодательства

на 74 сессии постановила учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, принимая во внимание полный учет существующих международных инструментов и усилий на национальном, региональном и международном уровнях по борьбе с использованием информационных и коммуникационных технологий в преступных целях, в частности работы и результатов межправительственной экспертной группы открытого состава по проведению комплексного исследования киберпреступности[1].

Следует признать данное решение историческим, учитывая сам факт отражения на международном уровне всех обозначенных проблем.

Однако, учитывая последствия пандемии COVID-19, Генеральная Ассамблея в своем решении 74/567 от 14 августа 2020 г., а затем 75/555 от 15 января 2021 г. решила отложить организационное заседание специального комитета на 10–12 мая 2021 г. Специальный комитет в мае 2021 года в ходе трехдневной организационной сессии в Нью-Йорке согласовал план и условия своей дальнейшей деятельности. А уже 26 мая 2021 года Генеральная Ассамблея приняла резолюцию 75/282 «Противодействие использованию информационных и коммуникационных технологий в преступных целях»[2].

В этой резолюции Генеральная Ассамблея среди прочего постановила, что начиная с заключительной сессии в Нью-Йорке в январе 2022 года, Специальный комитет созовет не менее шести сессий по 10 дней каждая и завершит свою работу, чтобы представить проект конвенции Генеральной Ассамблее на ее 78-й сессии; далее она постановила, что комитет проведет первую, третью и шестую сессии переговоров в Нью-Йорке, вторую, четвертую и пятую сессии — в Вене, будет руководствоваться правилами процедуры Генеральной Ассамблеи.

Заключительная сессия Специального комитета проходила в Нью-Йорке с 29 января по 9 февраля 2024 года. На этой сессии комитет постановил приостановить свою работу и рекомендовать Генеральной Ассамблее принять решение о проведении возобновленной заключительной сессии позднее, чтобы позволить комитету завершить свою работу и представить проект конвенции Генеральной Ассамблее на ее семьдесят восьмой сессии, что нашло свое отражение в документе Генеральной Ассамблеи A/78/L.46[3].

[1] Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 г. [по докладу Третьего комитета (A/74/401)] 74/247. Противодействие использованию информационно-коммуникационных технологий в преступных целях : 74-я сессия Генеральной Ассамблеи ООН. URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 17.02.2024).

[2] URL: https://documents.un.org/doc/undoc/gen/n21/133/54/pdf/n2113354.pdf (дата обращения: 17.02.2024).

[3] URL: https://documents.un.org/doc/undoc/ltd/n24/051/03/pdf/n2405103.pdf (дата обращения: 17.02.2024).

Решение о приостановлении работы Специального комитета является неслучайным: несмотря на однозначную общую проблематику в сфере противодействия преступлениям в сфере информационно-коммуникационных технологий следует признать ряд не решенных государствами-участниками проблем в данной сфере.

Так, в опубликованном драфте проекта Концепции по итогам работы шестой сессии Специального комитета в главе II «Криминализация» подлежали криминализации множество преступных деяний, включая вышеуказанные предложения Российской Федерации, а также преступления с использованием информационно-коммуникационных технологий против половой неприкосновенности: в том числе связанные с детской порнографией и сексуальным насилием над детьми либо домогательство ребенка (ст. 13, 14, 15); вовлечение несовершеннолетних в совершение противоправных действий (ст. 15 bis); поощрение самоубийства или принуждение к нему (ст. 15 ter); против общественной безопасности, здоровья населения и общественной нравственности: подстрекательство к подрывной или вооруженной деятельности (ст. 15 quater); преступления, связанные с экстремизмом (ст. 15 quinquies); отрицание, одобрение, оправдание или реабилитация геноцида или преступлений против мира и человечности (ст. 15 sexies); преступления, связанные с терроризмом (ст. 15 septies); преступления, связанные с распространением наркотических средств и психотропных веществ (ст. 15 octies); преступления, связанные с незаконным оборотом оружия (ст. 15 novies)[1].

Однако на заключительной сессии, где автору посчастливилось принять личное участие, множество из обоснованно подлежащих криминализации деяний были предложены к исключению, что повлекло обоснованные возражения со стороны стран — участниц Специального комитета.

Так, 10-е заседание Специального комитета озаботилось проблемами криминализации. Ряд стран, в частности страны исламского мира, указали на очень короткий список преступлений, которые охватывает Конвенция, и предложили включить в него преступления, связанные с терроризмом, экстремизмом, торговлей людьми и т. д. Также вновь встал вопрос о необходимости соблюдения прав человека, который сомнения не вызывал ни у кого, за исключением того, что в ст. 5 Конвенции шла ссылка на соблюдении всеми странами — участниками Специального комитета положений Конвенции, которые ими не были ратифицированы.

Если по правам человека консенсус был близок в связи с взятием формулировок из других конвенций, то с криминализацией деяний консенсус придется еще найти, что планируется сделать на специальном заседании Специального комитета.

Несмотря на наличие существенных противоречий, которые привели к приостановлению работы Специального комитета, следует признать, что развитие международного сотрудничества в области информационной безопасности на примере Организации Объединенных Наций, особенно в контексте рассмотрения проекта всеобъемлющей конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях, представляет собой важный этап в борьбе с киберпреступностью и обеспечении кибербезопасности на глобальном уровне.

Заключение и вывод

Проведенный анализ показывает, что ООН служит форумом для освещения проблем информационной безопасности и киберпреступности, а также для обмена лучшими практиками и опытом между государствами. Несмотря на отсутствие всеобъемлющей конвенции, уже само обсуждение ее проекта стимулирует дальнейший диалог и обсуждение важных вопросов, таких как определение стандартов поведения в киберпространстве и разработка механизмов сотрудничества, что способствует гармонизации законодательства различных стран и укреплению международного правового порядка в киберпространстве.

Предлагаемая Конвенция послужит значимым средством преодоления проблем, связанных с юрисдикционными разногласиями в киберпространстве, обеспечит реализацию механизмов межгосударственного сотрудничества в расследовании и преследовании киберпреступлений, пересекающих национальные границы, а также механизмов для сотрудничества в области правоприменения, включая экстрадицию преступников и обмен информацией о киберпреступлениях, что улучшит эффективность расследований киберпреступлений и судебного преследования киберпреступников.

Всеобъемлющая конвенция ООН по киберпреступности является важным инструментом в борьбе с киберугрозами и обеспечении кибербезопасности на международном уровне. Ее роль и значение продолжают расти в условиях быстрого развития информационных технологий, и дальнейшее совершенствование международного сотрудничества в этой области остается ключевой задачей для обеспечения кибербезопасности в будущем.

[1] Обновленный проект текста конвенции : от 23.05.2024 A/AC.291/22/Rev.3. URL: https://documents.un.org/symbol-explorer?s=A/AC.291/22/REV.3&i=A/AC.291/22/REV.3_1719848612226 (дата обращения: 17.02.2024).

Список источников

1. Ефремова М. А. Международно-правовые основы уголовно-правовой охраны информационной безопасности // Правосудие. 2020. Т. 2, № 1. С. 82–98. DOI:10.37399/issn2686-9241.2020.1.82-98

2. Кильмаматова Э. Р. Международное регулирование преступлений в сфере кибертерроризма // Современные вопросы государства, права, юридического образования : сборник научных трудов по материалам XV Международной научно-практической конференции, Тамбов, 22 декабря 2019 года. Тамбов : ИД «Державинский», 2020. С. 334–340.

3. Кузнецов А. Г. Международное сотрудничество в борьбе с киберпреступностью // Научный портал МВД России. 2023. № 1 (61). С. 131–136.

4. Пучков Д. В. Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8, № 4. С. 382–391.

5. Пучков Д. В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики : дис. … д-ра юрид. наук. Екатеринбург, 2022. 474 с.

6. Scholberg S., Ghernaouti-Helie S. A Global Protocol on Cybersecurity and Cybercrime. An Initiative for Peace and Security in Cyberspace. Oslo, 2009. URL: https://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (дата обращения: 17.02.2024).

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 25.04.2024.
Дата рецензирования статьи / Revised: 16.05.2024.
Дата принятия статьи к публикации / Accepted: 15.07.2024.