Л.В. Иванова,
доцент кафедры уголовного права и процесса Тюменского государственного университета, кандидат юридических наук, доцент

Уголовно-правовое противодействие киберпреступности в странах БРИКС

В Московской декларации XII саммита БРИКС, состоявшегося 17 ноября 2020 г.[1], признается проблема все возрастающего использования информационно-коммуникационных технологий в преступных целях и отмечается важность разработки единой нормативно-правовой базы для противодействия этому.

Несмотря на общность интересов в противодействии киберпреступности, подходы к криминализации нарушений в цифровом пространстве в рамках конкретного государства существенно различаются как по форме, так и по содержанию. Рассмотрим особенности закрепления уголовной ответственности за киберпреступления в законодательстве стран, входящих в БРИКС (Федеративная Республика Бразилия, Российская Федерация, Республика Индия, Китайская Народная Республика и Южно-Африканская Республика).

Единственным источником уголовной ответственности в Российской Федерации является УК РФ, из содержания которого можно сделать вывод о наличии двух групп киберпреступлений: специальные киберпреступления (преступления в сфере компьютерной информации) и общеуголовные киберпреступления (все иные, совершаемые с использованием информационных технологий)[2].

В Уголовном кодексе Бразилии[3] статьи о киберпреступлениях содержатся в разных главах. При этом в последние годы законодатель стремится установить наказание за новые виды пре-

[1] URL: https://brics-russia2020.ru/images/114/83/1148395.pdf (дата обращения: 25.01.2021).
[2] См. подробнее: *Иванова Л.В.* Виды киберпреступлений по российскому уголовному законодательству // Юрид. исслед. 2019. № 1.
[3] Código Penal (Decreto-Lei № 2.848, de 7 de Dezembro de 1940). URL: http://www.planalto.gov.br/CCIVIL_03/Decreto-Lei/Del2848.htm#art334 (дата обращения: 20.01.2021).

ступлений, совершаемых с использованием информационных технологий.

Так, 26 декабря 2019 г. в ст. 122 УК Бразилии были внесены изменения[1], предусматривающие усиление ответственности в случае побуждения, подстрекательства, содействия самоубийству или членовредительству, осуществленного через компьютерную сеть, социальную сеть или передачу в реальном времени.

С 2018 г. установлена уголовная ответственность за распространение материалов порнографического содержания через средства массовой информации, компьютерную или телекоммуникационную систему.

С 2013 г. УК Бразилии устанавливает ответственность за прерывание или нарушение работы телематических или информационных служб общественного пользования. Ранее закон защищал только телеграфные или телефонные связи.

При этом любое преступление, совершенное в киберпространстве, может быть наказано так же, как если бы оно было совершено вне такого контекста. Кроме того, иногда в статьях конкретно не упоминаются информационные и телекоммуникационные сети как способ совершения преступления, но это может подразумеваться в тексте закона, поскольку в статье упоминается публичное совершение преступления.

Помимо Уголовного кодекса в Бразилии действуют и специальные законы, в которых может устанавливаться ответственность за соответствующее преступление в киберпространстве. Например, Закон о промышленной собственности[2] закрепляет ответственность за публикацию любым способом ложной информации в ущерб конкуренту с целью получения преимущества. Использование любых средств публикации включает использование и информационных технологий.

В Индии можно выделить три группы киберпреступлений. Первая группа преступлений выделяется в соответствии с Законом об информационных технологиях[3], вторая группа – в соот-

[1] Lei n 13.718, de 24 de setembro de 2018. URL: http://www.planalto.gov.br/ccivil_03/_Ato 2015-2018/2018/Lei/L13718.htm (дата обращения: 20.01.2021).
[2] Industrial Property Law. 9,779/96. URL: https://www.jpo.go.jp/e/system/laws/gaikoku/document/index/brazil-e_industrial_property_law.pdf (дата обращения: 20.01.2021).
[3] The Information Technology Act, 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf (дата обращения: 20.01.2021).

ветствии с Уголовным кодексом Индии[1], а третья группа преступлений – в соответствии со специальными и местными законами.

Закон об информационных технологиях является основным законодательным актом Индии, касающимся киберпреступлений, в гл. XI которого содержится обширный и подробный перечень киберпреступлений и наказаний за них (ст. 65–74). Единственным преступлением, за которое может грозить пожизненное лишение свободы, является кибертерроризм.

Уголовный кодекс Индии содержит несколько киберпреступлений, например киберпреследование, сексуальные домогательства в электронном виде, фейковые новости в социальных сетях.

Иногда формулирование способа совершения преступления указывает на возможность совершения преступления посредством информационно-телекоммуникационных сетей. Среди таких преступлений можно назвать подстрекательство к мятежу, клевету и др.

Если в законе информационные технологии не указываются в составе конкретного преступления, но фактически преступление было совершено в сети «Интернет», то в статистике такое преступление отражается как киберпреступление. Например, подстрекательство к самоубийству может происходить в сети, и в этом случае оно становится киберпреступлением.

Последняя группа киберпреступлений – это преступления, предусмотренные специальными законами: Законом об азартных играх[2], Законом о лотереях[3] и др. Уголовная ответственность одновременно возможна в соответствии как с Уголовным кодексом Индии, так и со специальным законом.

В Уголовном кодексе Китайской Народной Республики[4] установлена ответственность за такие киберпреступления, как незакон-

[1] The Indian Penal Code, 1860. URL: https://www.indiacode.nic.in/handle/123456789/2263?locale=en (дата обращения: 20.01.2021).

[2] The Public Gambling Act, 1867. Digital Repository of All Central and State Acts. URL: https://www.indiacode.nic.in/handle/123456789/2269?view_type=browse&sam_handle=123456789/1362 (дата обращения: 20.01.2021).

[3] The Lotteries (Regulation) Act, 1998. Digital Repository of All Central and State Acts. URL: https://www.indiacode.nic.in/handle/123456789/1994?view_type=browse&sam_handle=123456789/1362 (дата обращения: 20.01.2021).

[4] Criminal Law of the People's Republic of China. URL: http://www.chnlawyer.net/law/subs/xingfa.html (дата обращения: 20.01.2021).

ное вторжение в компьютерную информационную систему, уничтожение компьютерных информационных систем, невыполнение обязательств по управлению безопасностью информационной сети, незаконное использование информационных сетей. В ряде статей использование информационных технологий не упоминается, но подразумевается в способе совершения преступления.

Поскольку киберпреступления разнообразны, трудно предвидеть, какие конкретные деяния будут совершены с помощью телекоммуникационных сетей. Для этих целей представляется важной ст. 287 УК Китая, согласно которой «кто использует компьютеры для совершения финансового мошенничества, кражи, растраты, растраты государственных средств, кражи государственной тайны или других преступлений, должен быть осужден и наказан согласно соответствующим положениям этого кодекса».

В Южно-Африканской Республике положения об уголовной ответственности за киберпреступления содержатся в различных нормативных актах, охраняющих определенную область цифровой среды. Действующее право представляет собой гибрид различных законодательных актов и общего права.

Например, действует Закон о защите критической инфраструктуры[1], в котором предусмотрена ответственность за предоставление, распространение или публикацию любым способом информации, относящейся к мерам безопасности, применяемым в критической инфраструктуре или в отношении нее.

Однако термин «киберпреступления» называется в Законе об электронных коммуникациях и сделках[2], гл. VIII которого включает такие преступления, как несанкционированный доступ, перехват или вмешательство в данные, а также компьютерное вымогательство, мошенничество и подделка.

Следует отметить, что сейчас государство находится в процессе совершенствования законодательства о киберпреступлениях. В конце 2015 г. была выпущена Национальная политика в об-

[1] The Critical Infrastructure Protection Act № 8, 2019. URL: https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000 (дата обращения: 20.01.2021).

[2] The Electronic Communications and Transactions Act № 25, 2002. URL: https://www.gov.za/documents/electronic-communications-and-transactions-act (дата обращения: 20.01.2021).

ласти кибербезопасности[1], за которой последовали проекты закона о киберпреступности и кибербезопасности[2].

Положения законопроекта раскрывают широкий круг киберпреступлений: незаконное обеспечение доступа, незаконное получение данных, незаконные действия в отношении программного или аппаратного обеспечения, незаконное вмешательство в данные или компьютерную программу, незаконное вмешательство в компьютерный носитель данных или компьютерную систему, незаконное получение, владение, предоставление, получение или использование пароля, кодов доступа и др.

Таким образом, в каждой стране есть свои особенности в установлении уголовной ответственности за киберпреступления. Чтобы эффективно противодействовать киберпреступности на межгосударственном уровне, БРИКС желательно принять единый документ, который содержал бы общее понимание киберпреступлений и их видов.

Р.А. Забавко,
доцент кафедры уголовного права Юридического института Иркутского государственного университета, кандидат юридических наук

О готовности российского уголовного права к использованию искусственного интеллекта при квалификации преступлений

Искусственный интеллект, лишенный многих ограничений человеческого разума, эффективно решает различные задачи не только в науке, иных высокотехнологичных отраслях, но и в тех сферах, где, как считалось долгое время, принимать решения может только человек. Все более распространенными становятся

[1] The National Cybersecurity Policy Framework for South Africa. № 609, 2015. URL: http://cybercrime.org.za/docs/National_Cybersecurity_Policy_Framework_2012.pdf (дата обращения: 20.01.2021).

[2] The Cybercrimes and Cybersecurity Bill, 2017. URL: https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6b-2017-7-nov-2018-0000 (дата обращения: 20.01.2021).