ПРАВОВЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ: РОЛЬ МЕЖДУНАРОДНЫХ НОРМ И ДОГОВОРОВ

Крылов Д.Н., Пьянкова А.А.

Научный руководитель: Чурикова А.Ю.

Россия, г. Саратов,
Саратовская государственная юридическая академия

Аннотация. *В статье рассмотрены основные проблемы в сфере обеспечения кибербезопасности на международной арене. Кибербезопасность представляет собой целую область по защите компьютерных систем, программного обеспечения и данных от таких хакерских угроз, как фишинг, утечка данных, вирусов и других. Исследованы нормативно правовые акты разной юридической силы, касающиеся рассматриваемого вопроса. На основе ретроспективного анализа существующей законодательной базы был сделан вывод о несоответствии нормативного материала, регулирующего вопросы борьбы с киберпреступностью, а также о необходимости выработки международных норм, которые бы отвечали современным реалиям. Приведены доводы в пользу российского проекта Конвенции по борьбе с киберпреступностью. Авторами также были рассмотрены мнения компетентных ученых о необходимости регулирования киберпространства на международном уровне.*

Ключевые слова: *кибербезопасность, киберпреступность, киберпространство, информационная сфера, компьютерная информация, международное сотрудничество.*

В 21 веке – веке информационных технологий, остро стоит вопрос о регламентации киберпространства. Киберпреступность не имеет границ и может нанести существенный урон всему мировому сообществу. В связи с этим в целях нормативного урегулирования различными субъектами международного права был создан огромный пласт документов, направленных на противодействие киберпреступности.

Международное сотрудничество стран по вопросу защиты и противостояния киберпреступности базируется на заключении региональных, двусторонних, многосторонних соглашений.

В 1998 году Резолюция 53/70 положила начало изучению проблемы безопасности в информационной среде. В ней членам ООН предлагается «продолжить обсуждение вопросов информационной безопасности, дать конкретные определения угроз, предложить свои оценки проблемы, включая разработку международных принципов обеспечения безопасности глобальных информационных систем» [3].

ЕС и ООН принимают активное участие в разработке нормативно правовых актов, направленных на защиту киберпространства. В этой связи следует

выделять два документа: Закон о кибербезопасности 2019 года [4] и Директиву (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года [5]. В основе Директивы лежит целенаправленная деятельность по достижению высокого уровня безопасности информационных, а также сетевых систем в пределах Союза, используемых в ключевых секторах. Она отменяет ранее действующую Директиву [6] с целью расширения сферы влияния на услуги и сектора, которые играют ключевую роль в обеспечении важных экономических и социальных инфраструктур внутри одного государства. Закон о кибербезопасности имеет основополагающее значение, так как он вводит систему сертифицирования технологий, которая призвана снизить уровень киберугроз путём проверки на соответствие установленным критериям.

Огромную роль в обеспечении кибербезопасности играет Конвенция о преступности в сфере компьютерной информации 2001 г., принятая в Будапеште [7], в рамках которой предусматривается криминализация преступлений, связанных с информационной сферой, определяется сфера применения процессуальных норм, а также устанавливаются принципы и режим взаимодействия стран, чьи интересы были нарушены в результате деятельности киберпреступников. Однако большинство стран, среди которых Бразилия, Китай, Россия, осознавая масштаб проблемы, не ратифицировали Будапештскую конвенцию, так как данная конвенция вызывает ряд вопросов, которые в первую очередь обусловлены положениями статьи 32, предполагающей наличие возможности у различных спецподразделений осуществлять те или иные действия в компьютерных сетях стран-участников без предварительного официального уведомления, а также другими положениями, которые создают непосредственную угрозу безопасности и государственному суверенитету.

Среди ученых сформировалось весьма противоречивое мнение относительно значимости Конвенции. Одни считают её признанным договором международного характера по борьбе с киберпреступлениями, который включает в себя не только нормы материального, но и процессуального права [2; С. 86]. Другие исследователи, критикуя эту позицию, утверждают, что она неактуальна, так как закрепляет перечень понятий, противоправных деяний, который не охватывает большую часть киберпреступлений, что противоречит принципу законности, так как основания для криминализации есть, а нормы нет.

Мы придерживаемся мнения тех ученых, которые считают, что Будапештская конвенция потеряла свою актуальность. Ведь с момента её принятия прошло уже почти четверть века, за этот период произошел значительный скачок в развитии информационных технологий и смежных отраслей. Появился ряд новых технологий, часть из которых может быть использована для кибератак, а Будапештская конвенция никак не регулирует их использование.

Такое положение дел позволяет сделать вывод о том, что правовая база для регулирования рассматриваемой сферы есть, но она устарела. Следствием этого явления выступает неэффективное международное сотрудничество. В связи с этим в настоящее время существует острая необходимость в документе, который бы определял единые составы преступлений, категориальный аппарат, соответствующий современным реалиям.

В качестве возможного выхода из этой ситуации Российской Федерацией был предложен проект Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях [8].

По нашему мнению, Конвенция Российской Федерации является передовым документом, так как в ней представлен расширенный круг преступных деяний, обновленный понятийный аппарат, а также в нее не вошёл пункт о трансграничном доступе, против которого выступали некоторые государства. Также в этом документе большое внимание уделяется государственному суверенитету, защите несовершеннолетних, в частности, был исключен пункт, предоставляющий странам право самостоятельно выбирать между преступностью или не преступностью деяния по вопросу приобретения детской порнографии посредством использования информационно-коммуникационных технологий для себя или для другого лица и владения детской порнографией, находящейся в компьютерной системе или на электронно-цифровых носителях информации.

Однако российский проект был отрицательно встречен представителями международного сообщества. Такое положение дел обосновывалось тем, что большинство стран устраивала действующая система по организации безопасности в киберпространстве [1; С. 267]. Мы же считаем, что существующий механизм необходимо модернизировать для того, чтобы идти в ногу со временем, ведь с каждым днем появляется все больше и больше новых видов незаконных хакерских программ, при помощи которых можно получить доступ к конфиденциальной информации как отдельно взятой личности, так и целого государства. Также ведутся информационные войны, которые подвергают опасности психическое состояние людей, подрывают демографическую ситуацию, провоцируют массовые недовольства и в конечном итоге способствуют разжиганию конфликтов. Таким образом, киберпространство стало эпицентром различного рода диверсий. В связи с этим, некоторые ученые даже стали определять киберпространство как «пятое пространство» и включать его в перечень вместе с сушей, космосом, морским и воздушным пространством [1; С. 262]. Именно поэтому в современных реалиях стоит в срочном, незамедлительном порядке создать единый нормативный правовой акт международного уровня.

Исходя из всего вышесказанного, мы хотели бы отметить, что киберпреступления носят динамичный и трансграничный характер, а также являются латентными, что значительно усложняет возможность их незамедлительного пресечения, поэтому залогом успеха в обеспечении кибербезопасности являются вовлечение как можно большего количества стран и их чёткое, слаженное сотрудничество. В настоящее время отсутствует документ, который бы соответствовал сложившейся обстановке, унифицировал существующий порядок и был признан международным сообществом. Думается, что создание такого нормативно правового акта необходимо осуществлять на базе ООН, так как на данный момент это единственный орган, который мог бы объединить законодательство 193 стран в этом направлении и обеспечить единообразное понимание явлений информационного пространства, связанных с киберпреступлениями.

Также стоит отметить, что исключительно в рамках международного сотрудничества можно координировать усилия по борьбе с киберпреступностью.

Это предоставляется возможным путём своевременного обмена информацией о надвигающихся киберугрозах, что, в свою очередь, повысит эффективность защиты, ведь государства будут проводить совместное расследование и способствовать скорейшему раскрытию киберпреступлений. Всё это в совокупности поможет укрепить цифровое пространство, защитить данные и обеспечить стабильность.

Библиографический список

1. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261-269.

2. Кобец П.Н. Совершенствование межгосударственного сотрудничества в сфере информационной безопасности: основа противодействия международной киберпреступности // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 1. С. 83-89.

3. Международное сотрудничество в области информационной безопасности – Министерство иностранных дел Российской Федерации [Электронный ресурс]. URL: ttps://www.mid.ru/ru/foreign_policy/international_safety/1695468/ (дата обращения: 22.04.2024).

4. Regulation – 2019/881 – EN – EUR-Lex [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1709970545402 (дата обращения: 22.04.2024).

5. Directive – 2022/2555 – EN – EUR-Lex [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555 (дата обращения: 22.04.2024).

6. Directive – 2016/1148 – EN – EUR-Lex [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148&qid=1709971120712 (дата обращения: 24.04.2024).

7. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: https://base.garant.ru/4089723/ (дата обращения: 27.04.2024).

8. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях [Электронный ресурс]. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_R.pdf (дата обращения: 28.04.2024).

LEGAL ASPECTS OF CYBER SECURITY IN INTERNATIONAL RELATIONS: THE ROLE OF INTERNATIONAL NORMS AND TREATIES

Krylov D.N., Pyankova A.A.

Scientific adviser: Churikova A.Yu.

Saratov State Law Academy, Saratov, Russia

Abstract. *The article considers the important problems in the sphere of cyber security in the international arena. Cybersecurity is a whole area of protection of computer systems, software and data from hacker threats such as phishing, data leakage, viruses and others. The normative legal acts of different legal force concerning the issue under consideration have been studied. Based on a retrospective analysis of the existing legislative framework, it was concluded that the regulatory material governing the fight against cybercrime was inconsistent, as well as the need to develop international standards that would meet modern realities. The arguments in favour of the draft Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes put forward by the Russian Federation are presented. The authors also considered the opinions of competent scientists on the need to regulate cyberspace at the international level.*

Keywords: *cybersecurity, cybercrime, cyberspace, information sphere, computer information, international cooperation.*