МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

К. В. Шабуня

Научный руководитель: Е. Н. Мазаник, доцент кафедры международного экономического права, кандидат юридических наук, доцент

В современном мире международные отношения тесно связаны с цифровой средой, которая стремительно развивается и привносит свои изменения в сферу международного сотрудничества. Использование информационных технологий ставит вопрос о возникновении рисков и угроз, связанных с их внедрением и развитием.

Область информационной среды, которая обусловлена использованием цифровых технологий с целью создания, обмена и использования информации именуется киберпространством. В настоящее время возрастает количество преступлений, совершаемых в киберпространстве. В условиях непрерывного развития технологий возрастает и количество видов программного обеспечения, которые носят негативный характер и используются для достижения незаконных целей, в том числе в экономической сфере. Такие проблемы в информационной сфере требуют своевременной правовой защиты не только на региональном уровне, но и на универсальном. Единого подхода к решению данной задачи на международной арене пока не разработано, однако, международное сообщество заинтересованно в формировании многосторонней правовой регламентации и защиты киберпространства.

Многочисленные споры проводятся в отношении так называемого «поведения» в киберпространстве. Не редко государственные субъекты относят борьбу с киберпреступностью к компетенции негосударственных субъектов (международных организаций), таких как, например, Интерпол, Европол. На данный момент участники международного сообщества не пришли к какому-либо соглашению о статусе киберпространства, то есть является оно глобальным достоянием либо относится к физической территории государств и основано на их национальном происхождении. В результате чего возникают проблемы определения юрисдикции международного права в сфере киберпространства [1, с. 83].

Киберпространство тесно связано с киберпреступностью, которая в том числе является следствием отсутствия единых подходов в международно-правовом регулировании организации киберпространства. Киберпреступность включает в себя различные виды деятельности и используется для обозначения нарушений закона разного рода, при совершении которых или содействии в совершении которых используются электронные средства.

Международное сообщество стремится и принимает необходимые меры по борьбе с киберпреступностью. Многосторонним договором, регулирующим борьбу с преступной деятельностью в сфере информационных технологий,

является Конвенция о преступности в сфере компьютерной информации, принятая 23 ноября 2001 г. в Будапеште в рамках Совета Европы.

Изучив Конвенцию, можно выделить некоторые ее аспекты. Так, важно обратить внимание на четко сформулированную цель ее принятия и соблюдения, а именно выработку всеобъемлющей и гармоничной политики уголовного права, касающейся вопросов преступлений в сфере информационных технологий, которая бы защищала общество от киберпреступности как на внутригосударственном, так и на региональном уровне. Также, регламентированы некоторые понятия, например, «компьютерная система», «компьютерные данные» и иные. Это позволяет прийти к всеобщему четкому пониманию дефиниций терминологии.

Конвенция содержит классификацию основных встречающихся видов правонарушений в кибепространстве, среди которых мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией. При этом, в дополнительных протоколах, принятых в Страсбурге в 2003 году, уже существующая классификация дополняется некоторыми видами правонарушений, например, дискриминация, ксенофобия, распространение расистских взглядов.

Следующей особенностью Конвенции является то, что значительное внимание уделяется международному сотрудничеству. Очевидно, что такое направление развития в условиях роста киберпреступности является наиболее эффективным и значимым, так как такой вид преступности является трансграничным, а, значит, пострадать может любое государство. В силу этого, согласно ст. 48 данной Конвенции заверенные копии данного документа были направлены не только членам Совета Европы, но и не являющимся членам Совета Европы государствам, которые участвовали в разработке настоящей Конвенции, и любому государству, получившему предложение присоединиться к ней.

Также, странами-участницами Конвенции были приняты директивы, касающихся острых вопросов. Помимо данных директив, в рамках Конвенции создавались межгосударственные органы, которые помогают объединять усилия в борьбе с киберпреступностью, а также востребованы с целью координации и своевременного предоставления технической, экспертной и информационной помощи в процессе расследования киберпреступлений [2, с. 720].

В рамках международного сотрудничества разработано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г., которое было ратифицировано Законом Республики Беларусь от 16 июля 2019 года № 207-З «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий».

Данное соглашение содержит четко обозначенную цель - обеспечение предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий. В сравнении с соглашением

о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., новое соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. содержит уже более актуальные и обновленные положения. Важно, что в соглашении от 28 сентября 2018 г. подробно и конкретизировано определены права и обязанности сторон в различных направлениях взаимного сотрудничества. Так, регламентированы формы сотрудничества, компетентные органы, осуществление направления запроса об оказании содействия и исполнение запроса и так далее. Данное соглашение открыто для присоединения любого государства-участника СНГ. Следует отметить, что Республика Беларусь одной из первых ратифицировала данное Соглашение.

Обратим внимание, что с учетом интенсивности развития информационных технологий, в международные договоры своевременно вносить изменения и дополнения затруднительно. Так, такие виды сетевых угроз как «фишинг», «ботнет» еще не регламентированы в международных актах. Такие виды преступной деятельности на настоящем этапе развития информационных систем стали наиболее вредоносными и распространенными видами сетевых угроз, используемых злоумышленниками для достижения своих целей.

Республика Беларусь, в свою очередь, уделяет значительное внимание вопросам в сфере кибербезопасности и противодействия возможным террористическим угрозам. 18 марта 2019 года была утверждена Концепция информационной безопасности Беларуси, которая провозгласила информационный суверенитет, уважение цифрового суверенитета других стран и проведение мирной внешней информационной политики. В данной Концепции определяются стратегические задачи и приоритеты в области обеспечения информационной безопасности. Также, представители Республики Беларусь в 2019–2021 гг. принимали участие в заседаниях рабочей группы открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, учрежденной резолюцией Генеральной Ассамблеи ООН 73/27, и всемерно способствовали принятию консенсусом итогового доклада РГОС. В документе предусматривается перспектива разработки новых правил и норм. При этом Беларусь помимо поддержания инициативы Российской Федерации о создании новой РГОС по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ на 2021–2025 годы, принимает активное участие в ее работе и развитии [3].

Известный белорусский ученый А.А. Данилевич утверждает, что «наиболее эффективные результаты приносит взаимодействие, основанное на международных договорах и разработанном национальном законодательстве…» [4, с. 6]. С его точкой зрения следует согласиться, т.к. таким образом, формируется наиболее эффективная форма сотрудничества, при которой

возможна организация информационной безопасности как на региональном, так и на универсальном уровнях.

Вышеизложенное позволяет сделать следующие выводы.

Конвенция Совета Европы и Соглашение стран-участниц СНГ являются важными базовыми документами в сфере информационной безопасности и противодействия киберпреступности.

Однако, содержащиеся нормы в данных документах не в полной мере регулируют вопросы борьбы с киберпреступностью и организацией информационной безопасности. Поэтому строится система борьбы со всеми угрозами в целом, то есть без разработки конкретных подходов к определенному виду киберпреступности.

Необходимо стремиться к тому, чтобы как можно больше государств участвовало в подобного рода международных договорах, так как данный вид преступности является масштабным и ущерб может быть причинен любому государству с любой территории.

Республика Беларусь активно поддерживает международное взаимодействие в сфере обеспечения безопасности киберпространства, выступает за разработку правил и норм ответственного поведения в информационной сфере.

Список использованных источников:

1. Грязнов, С. А. Международное правовое регулирование киберпространства / С. А. Грязнов // Международный журнал гуманитарных и естественных наук. – 2021. – №1–3. – Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnoe-pravovoe-regulirovanie-kiberprostranstva. – Дата доступа 01.10.2023.

2. Шматкова, Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы [Электронный ресурс]. / Л. П. Шматкова // Молодой ученый. – 2016. – № 28 (132). – С. 720–723. – Режим доступа: https://moluch.ru/archive/132/37021/. – Дата доступа: 03.10.2023.

3. Международная информационная безопасность // Министерство иностранных дел Республики Беларусь [Электронный ресурс]. – Режим доступа: https://mfa.gov.by/mulateral/global_issues/inform. – Дата доступа: 04.10.2023.

4. Данилевич, А. А. Международная правовая помощь по уголовным делам: уголовно-процессуальный аспект / А. А. Данилевич, В. И. Самарин. — Минск: БГУ, 2009. — 127 с.