числе в процессе квалификации вовлечения несовершеннолетнего, необходимо обращать внимание на следующие аспекты:

1) наличие или отсутствие квалифицирующего признака – вовлечение несовершеннолетнего в совершение преступления родителем;

2) возраст, психологические и физические особенности несовершеннолетнего, вовлеченного в совершение преступления, а также факт нахождения последнего под возможным влиянием какой-либо социальной группы;

3) устанавливать и расследовать все преступные эпизоды в процессе которых могут быть выявлены факты вовлечения несовершеннолетнего в преступную деятельность;

4) при осуществлении процедуры доказывания давать правовую оценку каждому отдельному эпизоду вовлечения несовершеннолетнего в совершение преступления;

5) при определении способа вовлечения необходимо опираться на обстоятельства преступного деяния, совершенного взрослым лицом.

Список цитированных источников:

1. *Гулякевич, Д. Л.* Вовлечение несовершеннолетнего в совершение преступления: опыт уголовно-правовой оценки России и Беларуси / Д. Л. Гулякевич // Вестн. Моск. гос. ун-та. – 2011. – № 5. – С. 57–67.

2. *Щетинина, Н. В.* Некоторые вопросы квалификации вовлечения несовершеннолетнего в совершение преступлений или антиобщественных действий, совершенных родителем / Н. В. Щетинина // Вестн. Моск. ун-та МВД России. – 2017. – № 1. – С. 78–80.

3. Приговоры судов по ст. 150 УК РФ. Вовлечение несовершеннолетнего в совершение преступления [Электронный ресурс] // Судеб. практика. – Режим доступа : https://sud-praktika.ru/precedent/category/284.html. – Дата доступа : 11.11.2020

4. Вовлечение несовершеннолетнего в совершение преступления (кражи) путем обмана [Электронный ресурс] // Осиповичский районный исполнительный комитет. – Режим доступа : http://osipovichi.gov.by/uploads/files/vovlechenie-nesovershennoletnego-v-sovershenie-prestuplenija.pdf. – Дата доступа : 13.11.2020.

5. Вовлечение несовершеннолетнего в совершение преступления и антиобщественное поведение: эволюция уголовно-правовой оценки [Электронный ресурс]. – Режим доступа : http://e-edu.by/main/departments/law/staff/gulyakevich/publications/15.pda. – Дата доступа : 13.11.2020.

ВОПРОСЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

Расулев Абдулазиз Каримович,
профессор кафедры профилактики правонарушений
Академии Министерства внутренних дел Республики Узбекистан,
доктор юридических наук, профессор
rasuleff@mail.ru
Саъдуллаев Гайрат Абдужаббор угли,
преподаватель кафедры профилактики правонарушений
Академии Министерства внутренних дел Республики Узбекистан
sadullayev@mail.ru
(Республика Узбекистан, г. Ташкент)

В мире обеспечение информационной безопасности, противодействие киберпреступности, изучение криминологической характеристики преступлений в сфере информационных технологий и лиц, их совершивших, актуальность повышения эффективности международного сотрудничества требуют проведения глубоких исследований по рассматриваемой теме. Особое значение приобретают обеспечение защиты отношений в сфере информационных технологий и информационной безопасности от преступных посягательств, предупреждение преступлений в данной сфере, поиск научно-теоретических и практических решений уголовно-правовых проблем, имеющихся в национальном законодательстве, устанавливающем ответственность за подобные преступления, и правоприменительной практике. Эффективное решение проблемы борьбы с информационными преступлениями требует согласованных международных действий и сотрудничества. В процессе проведения расследований правоохранительные органы различных государств должны сотрудничать между собой, предоставляя потенциально полезную информацию непосредственно органам другого государства. Вместе с тем в зависимости от отношений между заинтересованными государствами, характера соответствующей информации и других факторов может также возникать потребность в разработке полномочий и процедур в международном соглашении. Это естественно, поскольку виновные или подозреваемые лица не могут быть арестованы, повестка не может быть подана, а полицейские или иные расследования не могут быть проведены на территории другого государства, за исключением действий в соответствии с условиями договора или иного соглашения [3, с. 306].

Генеральной Ассамблеей ООН, Советом Европы, ШОС, СНГ, Лигой арабских государств и иными организациями были приняты специальные акты, касающихся информационно-коммуникационных технологий, противодействию и профилактике преступного использования информационных технологий, предупреждению преступности в данной сфере на региональном и международном уровне [4, с. 40]. Однако, как справедливо указывает А.Г. Волеводз, «в ныне существующем виде механизмы международного сотрудничества не способствуют быстрому получению из иностранного государства доказательств в форме компьютерных данных» [5, с. 108]. Итак, в чем можно увидеть основные проблемы международного сотрудничества по уголовным делам, в частности по делам о преступлениях в сфере информационных технологий и безопасности?

Во-первых, наступил момент истины, когда мировое сообщество, национальные институты по борьбе и противодействию преступлениям в сфере информационных технологий и безопасности должны провести критический анализ и пересмотреть свои подходы, мировоззрения по вопросам унификации и гармонизации норм уголовного законодательства всех стран. Это связано с тем, что в глобальном информационном пространстве уголовно-правовая политика каждого государства оказывает непосредственное влияние на криминогенную характеристику уровня информационной преступности в целом. К сожалению, в глобальных сетях присутствуют национальные сегменты, где не криминализованы определенные преступные действия, что, в свою очередь, позволяет преступникам активно осваивать эти «островки беззакония и хаоса». Несмотря на то, что проходит второе десятилетие XXI в., до сих пор есть государства, где практически отсутствуют законы, устанавливающие ответственность за все существующие на практике виды информационных преступлений.

Существуют также процессуальные проблемы. Так, УПК Республики Узбекистан, как и многих других стран, предусматривает в качестве одного из важных условий удовлетворения запросов, связанных с производством уголовного дела, наличие в уголовном законодательстве запрашиваемого государства наказания в виде лишения свободы на срок не менее одного года (ч. 3 ст. 601 УПК Республики Узбекистан предусматривает исполнение запроса о выдаче лица, находящегося на территории Республики Узбекистан только, если УК Республики Узбекистан предусматривает за совершенное деяние наказание в виде лишения свободы на срок не менее одного года или более тяжкое наказание, когда выдача лица производится для привлечения к уголовной ответственности). При этом может возникнуть проблема при направлении запроса на территорию другого государства о выдаче лица, совершившего преступление против Республики Узбекистан. Например, при совершении несанкционированного доступа к информационным системам на территории Туркменистана, запрос не будет удовлетворен, так как УК Туркменистана вообще не предусматривает наказание в виде лишения свободы за указанное преступление. Особая опасность может возникнуть при несанкционированном доступе к информационным системам, имеющим стратегическое значение или составляющим государственные секреты. В свою очередь, аналогичная проблема по расследованию информационных преступлений может возникнуть при совершении преступления в Республике Беларусь, Кыргызстане, России (распространение вредоносных программ), Казахстане, Таджикистане (компьютерный саботаж), Индии (практически не предусматривается ответственность за преступления в сфере информационных технологий), Нидерландах (умышленное, с целью извлечения выгоды для себя или для третьего лица использование лицом технических устройств для перехвата или записи данных, идущих по телекоммуникационным системам или присоединенному оборудованию), Ирландии (лишение свободы не предусматривается).

Вышеуказанная проблема связана с таким институтом государственной юрисдикции и международного сотрудничества, как суверенитет. Суверенное равенство государств защищено нормами обычного международного публичного права, которые включают в себя обязательства государств не «вмешиваться в какой бы то ни было форме или по какой бы то ни было причине во внутренние и внешние дела других государств» [8, с. 6]. В этой связи вопросы правового обеспечения и уголовного правосудия попадают в эту исключительную прерогативу суверенитета государства, в результате чего уголовная юрисдикция традиционно имеет территориальную привязку. Поэтому государства должны воздерживаться от оказания давления на другие государства в отношении действий конкретных национальных органов, таких как правоохранительные органы или органы судебной власти [1, с. 53]. Одним из подходов к киберпреступности является признание того, что определение транснационального характера преступления максимально целесообразно, когда оно рассматривается с точки зрения юрисдикции и уголовных доказательств. Одним из способов, характеризующих любое правонарушение, например, является различие между составляющими элементами «деяния», «обстоятельства» и «результата» [2]. При возникновении одного или нескольких этих элементов или существенных последствий на территории другого государства преступление приобретает транснациональный характер.

Во-вторых, с учетом дальнейшего и неизбежного роста глобализации возник вопрос о необходимости рассмотрения проблемы по разработке глобального *общеобязательного* международного акта, предусматривающего общие принципы борьбы с информационными преступлениями, вопросы гражданской и уголовной ответственности, перечень уголовно наказуемых деяний, конкретные механизмы международного сотрудничества в области противодействия информационным преступлениям и повышения квалификации сотрудников правоохранительных органов, обмена данными и судопроизводства.

Так, за последние годы вопросы противодействия трансграничным преступлениям, в частности киберпреступности, на региональном уровне обсуждаются регулярно и системно. Можно отметить усилия авторитетной региональной организации ШОС, под эгидой которой в июне 2017 года в городе Ханты-Мансийске состоялась 1-я Международная конференция по информационной безопасности с участием стран БРИКС, ШОС и ОДКБ. В

работе конференции приняли участие представители Армении, Беларуси, Бразилии, Вьетнама, Казахстана, Малайзии, Российской Федерации и ЮАР. Кроме того, с 28 по 30 ноября 2017 года на 15-м заседании Генеральных прокуроров-членов ШОС в городе Санкт-Петербург были обсуждены вопросы консолидации усилий по противодействию новым вызовам и угрозам, в том числе преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий. В качестве одного из основных региональных документов, заложивших основы международно-правового сотрудничества в области борьбы с киберпреступностью, можно отметить Конвенцию Совета Европы о киберпреступности 2001 года [9].

В Стратегии развития ШОС до 2025 года особое внимание уделяется вопросу дальнейшего поэтапного реагирования на данную проблематику. В документе отмечено, что ШОС будет интенсивно и настойчиво добиваться принятия в ООН «Правил поведения в области обеспечения международной информационной безопасности», и в дальнейшем на этой основе совместно с другими членами мирового сообщества работать над формированием единого международного регулирования сферы информационно-коммуникационных технологий, развивать сотрудничество на этом направлении, в том числе в повышении квалификации профильных специалистов государств-членов в рамках Стратегии развития ШОС до 2025 года [10]. Отрадным фактором является то, что активную позицию в инициировании указанных Правил занимает Узбекистан. Это еще раз подчеркивает высокую обеспокоенность правительства ростом количества преступлений в области информационных технологий, усилением вызовов и угроз в сфере обеспечения международной информационной безопасности. В соответствии с принципом объективной территориальности, многие международные и региональные правовые документы устанавливают, что нет необходимости в том, чтобы все элементы преступления были совершены на одной территории для применения территориальной юрисдикции. В частности, в Пояснительной записке к Конвенции Совета Европы о компьютерных преступлениях разъясняется, что сторона может утверждать территориальную юрисдикцию в соответствии с принципом территориальности, если атаковавшее компьютерную систему лицо и система жертвы находятся на его территории, и если атакованная компьютерная система находится в пределах ее территории, даже если злоумышленник там не находится.

В-третьих, по причине отсутствия или декларативности и неэффективности международных соглашений страны предпочитают и вынуждены заключать двусторонние соглашения по оказанию взаимной правовой помощи, которые имеют более взаимовыгодный, действенный и оперативный характер реализации договоренности. В настоящее время существует около 40 двусторонних соглашений Республики Узбекистан с зарубежными государствами по вопросам взаимной помощи по уголовным делам. Однако лишь с четырьмя государствами (Азербайджан, Молдова, Туркменистан, Кувейт) предусматривается сотрудничество в области информационной безопасности, с семью странами (Австрия, Кипр, Беларусь, Иран, Саудовская Аравия, ОАЭ, Вьетнам) имеются соглашения в области противодействия компьютерным преступлениям и киберпреступлениям. Во многом приоритет двусторонних соглашений связан с тем, что надгосударственный характер глобальных сетей часто приводит к возникновению юрисдикционных проблем по фактам совершаемых киберпреступлений. Возникновение множественных правовых коллизий обуславливается трансграничным характером совершаемых деяний.

Заключение двусторонних соглашений между странами вызвано тем, что по причине отсутствия глобального уголовно-правового акта между странами не достигнут консенсус по вопросу эквивалентности криминализации. Данный вопрос все еще сохраняет свою актуальность, являясь одним из самых обсуждаемых на международных площадках, вызывающим бурные, неоднозначные дискуссии среди экспертно-аналитических кругов на различных уровнях. Принцип двойной уголовной ответственности содержится в международных и региональных правовых документах по борьбе с киберпреступлениями. Он является необходимым требованием для выдачи и предоставления взаимной правовой помощи, например, в Конвенции Совета Европы о компьютерных преступлениях и Конвенции Лиги арабских государств [6].

Одним из условий создания эффективной системы международной информационной безопасности является разработка и принятие современного, универсального международного правового акта, обеспечивающего адекватную защиту от новых угроз, при этом учитывающего национальный суверенитет государств в отличии от устаревшей европейской конвенции по киберпреступности. Заключение универсального международного договора о борьбе с информационными преступлениями, который учитывал бы накопившийся опыт международных соглашений в данной области и особенности национального законодательства стран-участниц, довольно сложная и трудоемкая задача. Таким универсальным регулятором могла бы стать отдельная Конвенция ООН по борьбе с киберпреступлениями и обеспечению глобальной информационной безопасности, которая на международном уровне помогла бы комплексно и системно, противодействовать киберпреступности и кибертерроризму, а также бороться с ними.

В целях анализа состояния и обмена информацией о киберпреступности между странами-участниками ШОС, ЕС и других региональных организаций, оценки принятых на национальном уровне превентивных мер и оперативных мероприятий, в том числе проведения специальной подготовки сотрудников правоохранительных органов, судебных и прокурорских кадров необходимо создать в рамках ИНТЕРПОЛ глобальный координационный центр по противодействию киберпреступности [7]. Создание данного Центра позволит системно осуществить сбор, обработку данных, оказание информационной, технической и криминалистической поддержки соответствующим подразделениям правоохранительных органов стран-членов Интерпола, координацию совместных расследований, а также специализированное обучение и подготовку специалистов. Центр может содейство-

вать проведению необходимых исследований и созданию программного обеспечения, заниматься оценкой и анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений. В сферу деятельности Центра также будет входить помощь судьям, прокурорам и сотрудникам правоохранительных органов.

Принимая во внимание масштабность проблемы динамичного роста киберпреступности в мире, возникновения реальных рисков и угроз для всего человечества, международные институты и страны обязаны прийти к общей консолидации сил правоохранительных и судебных органов, забыв про свои амбиции, во имя спасения существующего миропорядка.

Список цитированных источников:

1. *Cassese, C*. International Law / C. Cassese. – Oxford University Press, 2005. – 180 p.

2. *Fletcher, G*. Rethinking Criminal Law / G. Fletcher. – Oxford : Oxford University Press, 1978.

3. *Brownlie, I*. Principles of Public International Law. – 6th ed / I. Brownlie. – Oxford : Oxford University Press, 2003. – 426 p.

4. *Турсунов, А. С*. Уголовно-правовые и криминологические меры борьбы с преступлениями в сфере информационных технологий и безопасности / А. С. Турсунов, А. К. Расулев // Вопр. криминологии, криминалистики и судебной экспертизы : сб. науч. тр. ; ГУ «Науч.-практ. центр Гос. комитета судеб. экспертиз Респ. Беларусь», 2019. – Вып. 2 (46). – 207 с.

5. *Волеводз, А. Г*. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М. : Юрлитинформ, 2002. – 176 с.

6. *Расулев, А. К*. Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности : автореф. дис. … д-ра юрид. наук (Dsc) / А. К. Расулев ; Акад. МВД Респ. Узбекистан. – Ташкент, 2018. – 75 с.

7. Будапештская конвенция по киберпреступлениям, 23 авг. 2001 г. [Электронный ресурс]. – Режим доступа : www.mvd.gov.by. – Дата доступа : 28.11.2020.

8. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора [Электронный ресурс] ; Группа экспертов для проведения всестороннего исследования киберпреступности, Вена, 25–28 февр. 2017 г. – Режим доступа : UNODC/CCPCJ/EG.4/2017/2. – Дата доступа : 28.11.2020.

9. Конвенция ООН против транснациональной организованной преступности, 15 нояб. 2000 г. [Электронный ресурс]. – Режим доступа : www.un.org/ru/. – Дата доступа : 28.11.2020.

10. Стратегия развития Шанхайской организации сотрудничества до 2025 года [Электронный ресурс]. – Режим доступа : http://infoshos.ru/ru/?id=125. – Дата доступа : 28.11.2020.

ПРИЗЫВЫ К ДЕЙСТВИЯМ, НАПРАВЛЕННЫМ НА ПРИЧИНЕНИЕ ВРЕДА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ: УГОЛОВНО-ПРАВОВОЙ АСПЕКТ

Реутская Анастасия Николаевна,
студент 3-го курса Академии управления при Президенте Республики Беларусь
reutskaya-2000@mail.ru
Научный руководитель: Клим Анатолий Марьянович,
заведующий кафедрой
правового обеспечения правоохранительной деятельности
Академии управления при Президенте Республики Беларусь,
кандидат юридических наук, доцент
(Республика Беларусь, г. Минск)

Защита конституционного строя – необходимая функция государства, непременное условие обеспечения его безопасности. В системе правовых мер, обеспечивающих осуществление этой функции, важное место занимают уголовно-правовые нормы. Статья 361 УК Республики Беларусь предусматривает ответственность за призывы к захвату государственной власти, или насильственному изменению конституционного строя Республики Беларусь, или измене государству, или совершению террористического акта или диверсии, или совершению иных действий в ущерб внешней безопасности Республики Беларусь, ее суверенитету, территориальной неприкосновенности, национальной безопасности и обороноспособности либо распространение материалов, содержащих такие призывы. Ответственность за указанное преступление выступает важной характеристикой политического режима в стране, официального отношения государственной власти к демократическим правам и свободам граждан. Существование в уголовном законодательстве норм, подобных ст. 361 УК Республики Беларусь, предопределено конституционными положниями: