УДК 341.48

Кукеев А.К.
Южно-Казахстанский университет имени М. Ауэзова,
г. Шымкент, Казахстан

ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО СОТРУДНИЧЕСТВА В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. В данной статье рассматриваются проблемы теории и практики международного права – международно-правового сотрудничества в сфере борьбы с киберпреступностью. Автором рассмотрены международно-правовое регулирование кибервойн, пути совершенствования материальных и процессуальных норм института международно-правового сотрудничества в сфере борьбы с киберпреступностью, а также осуществлен анализ правовых и институциональных основ противодействия киберпреступности в Республике Казахстан.

Ключевые слова: киберпреступление, киберпреступность, кибератака, кибервойна, ИКТ, интернет вещей, трансграничный доступ к информации, мультистейкхолдеризм.

Проведение исследования института международно-правового сотрудничества в противодействия киберпреступности в динамике его развития позволяет выделить основные направления совершенствования очерченной сферы.

Киберпреступления следует отличать от кибератак и кибервойны.

Кибератака - это нарушение прав и законных интересов участников киберпространства с помощью ИКТ, осуществляемых физическими и юридическими лицами с участием (содействие, финансирование и т.д.) государств. При условии, если кибератака заключается в осуществлении действий, предусмотренных уголовным и международным правом, такие действия могут быть квалифицированы как киберпреступления, национальные и международные соответственно.

Кибервойна - это значительные, масштабные, целенаправленные и систематические кибератаки с применением кибероружия, осуществляемые вооруженными силами или специальными подразделениями государства против суверенитета, территориальной целостности, независимости другого государства и международного мира и стабильности. Кибератаки, не соответствующие этим признакам, но осуществляются государствами против прав и интересов других государств или международного сообщества, могут признаваться недружественными актами.

В современной доктрине и практике международного права вопросы квалификации кибервойны остается дискуссионным. Существуют подходы по обоснованию применения международного гуманитарного и уголовного права. Наиболее оправданным, на наш взгляд, является квалификация кибервойны как нарушение Устава ООН и применения силы, а в отдельных случаях - преступления агрессии.

Материально-правовые нормы института международного сотрудничества в борьбе с киберпреступностью определяют специальные принципы такого сотрудничества, кримина-

лизации отдельных видов противоправных деяний, а также институциональные механизмы и наращивания потенциала (capacity building).

Система международного противодействия киберпреступности основана на принципах технической нейтральности, мультистейкхолдеризму (государственно-частного партнерства), а также эквивалентности прав человека онлайн и офлайн. В будущем кибернетическая преступность будет связана с использованием инновационных технологий. Как было установлено на примере Интернета вещей, новейшие технологии по общему правилу входят в сферу действия действующих международных соглашений о киберпреступности, но специального регулирования по ним не предусмотрено.

Институт международно-правового сотрудничества в сфере борьбы с киберпреступностью - это совокупность материальных и процессуальных норм и принципов, регулирующих сотрудничество между государствами, направленное на противодействие киберпреступности. Названный институт находится на стадии формирования и осуществляется на наднациональном уровне в рамках механизмов международной правовой помощи и сотрудничества по уголовным делам. для исследуемого института присуща фрагментарность и неоднородность, а потому он нуждается гармонизации. С этой целью необходима разработка и принятие универсального международного договора в рамках ООН. Поэтому считаем целесообразным инициировать подготовку универсальной Конвенции о борьбе против киберпреступности. Целесообразность принятия универсальной конвенции о киберпреступности обосновывается следующими факторами: 1) положения Конвенции ООН против транснациональной организованной преступности не регулируют весь комплекс правоотношений в сфере противодействия киберпреступности; 2) регулирование международного сотрудничества в сфере борьбы с кибернетической преступностью на основе действующих региональных актов приводит к дальнейшей фрагментации и расслоения института; 3) расширение сферы действия действующих международных соглашений, прежде всего Конвенции Совета Европы о киберпреступности, приводит к одновременному их применения, а поскольку положения таких международных договоров отличаются, необходимо дополнительное согласование и гармонизация; 4) Конвенция Совета Европы о киберпреступность не может стать универсальным договором в определенной сфере через политические и правовые разногласия. Кроме этого, в универсальном договоре о киберпреступности должно быть учтено криминализации кибернетических деяний, наносящих вред объектам критической инфраструктуры. Учитывая особенно высокую общественную опасность таких преступлений, мера ответственности за их совершение по сравнению с другими киберпреступностью должна быть повышенной.

Развитие международного противодействия киберпреступности, связанным с нелегальным контентом, развивается за счет привлечения частных посредников, осуществляют контроль и могут влиять на содержание распространяемой информации (Например, социальных сетей и поисковых ресурсов).

Институциональные механизмы международно-правового сотрудничества государств в сфере борьбы с киберпреступностью созданы бессистемно при отсутствии достаточных конвенционных механизмов. Как следствие, их деятельность является несогласованной и фрагментарной, а полномочия часто дублируются. Для повышения эффективности исследуемого

института необходимо создание централизованного органа на основании универсальной конвенции и в рамках ООН с учетом существующих институтов.

Неотъемлемой частью института международно-правового сотрудничества государств в борьбе с киберпреступностью является уголовно-процессуальные нормы. Посредством сотрудничества с уголовно процессуальных вопросов в сфере борьбы с киберпреступностью устанавливаются общие подходы к определению юрисдикции в киберпространстве, признание и использование чувствительных электронных доказательств, выполнения процессуальных действий, в том числе трансграничного доступа к информации, а также определяются каналы связи между государствами.

Проблема распределения суверенных юрисдикций государств в киберпространстве решается за счет применения критериев местонахождение информационной инфраструктуры, локализации преступного действия и последствий, которые она вызвала, а также гражданства преступника и потерпевшей стороны.

Сфера уголовно-процессуального сотрудничества государств и дальше расширяться. Во-первых, традиционные методы и способы уголовного процесса не соответствуют требованиям работы с электронными доказательствами; во-вторых, расследование других видов преступлений также требует использования электронных доказательств; в-третьих, концепцию трансграничного доступа к информации все больше начинает восприниматься.

Среди негативных тенденций следует отметить формирование двух противоположных систем: государств, осуществляющих сотрудничество по процессуальным вопросам расследований киберпреступлений, а также государств, которые находятся вне таких механизмов; сложность в достижении консенсуса по вопросу транснационального доступа к информации, а также параллельное создание каналов, предусмотренных для оперативного реагирования на киберпреступления и передачи данных по ним.

Решение этих проблем возможно за счет создания Конвенции ООН о борьбу против киберпреступности, с включением общего положения о трансграничных доступ к информации и возможностью внесения оговорок к нему. Кроме этого, универсальная сеть 24/7 должна существовать в рамках централизованного органа ООН.

Развитие отечественного законодательства в сфере борьбы с киберпреступностью происходил постепенно с учетом международно-правовых документов, а также в тесной взаимосвязи с формированием национальной системы кибербезопасности РК.

Криминализация киберпреступлений осуществляется в Казахстане на основании Уголовного кодекса РК, требует внесения изменений и дополнений. Так, в первую очередь, нужно дополнить уголовное законодательство понятием киберпреступности, а кроме этого считаем целесообразным принятие поправки к ст. 203.1 УК РК по в становления дополнительной отягчающего обстоятельства «совершение преступления с помощью ИКТ». В уголовно-процессуальном законодательстве следует учесть особенности оценки судом электронных доказательств, как таковых, что чаще всего фигурируют в уголовных производствах по расследованию киберпреступлений, а также разработать отдельные криминалистические методики расследования киберпреступлений, с учетом последних тенденций типичных способов совершения данного вида преступлений.

Список литературы и источников

1. Кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК «Уголовный кодекс Республики Казахстан» //ИПС «Әділет» // https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения 01.09.2021).

Askar K. Kukeev
Mukhtar Auezov South Kazakhstan University

Issues of international legal cooperation in the sphere of combating cybercrimes in the Republic of Kazakhstan.

Abstract. This article discusses the problems of theory and practice of international law – international legal cooperation in the field of combating cybercrimes. The author considers the international legal regulation of cyber warfare, ways to improve the material and procedural norms of the Institute of international legal cooperation in the field of combating cybercrimes, and also analyzes the legal and institutional foundations of countering cybercrimes in the Republic of Kazakhstan.

Keywords: cybercrime, cyberattack, cyberwar, ICT, emergent technologies, internet of things, cross-border access to information, multistakeholderism.

УДК 342.25

Бизяев К.Д.
Самарский национальный исследовательский университет имени академика С.П. Королева

ПРАВОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ КОМФОРТНОЙ ГОРОДСКОЙ СРЕДЫ

Аннотация. В статье обозначены основные направления развития и реализации составляющей национального проекта «Жилье и городская среда» - федерального проекта «Формирование комфортной городской среды». Также автор предлагает задуматься над обозначенными трудностями, с которыми на практике сталкиваются институты гражданского общества и государства.

Ключевые слова: комфортная городская среда, благоустройство, инфраструктура, городские пространства, национальные проекты.

Современный горожанин воспринимает всю территорию города как единое пространство и ожидает от него безопасности, комфорта, функциональности и эстетики. Рационально выстроенная городская среда позволяет снизить социальную напряженность, на освещенных людных улицах ниже уровень преступности, при наличии безопасных и современных спортивных площадок увеличивается доля населения, регулярно занимающегося спортом, снижа-