DOI 10.37882/2223-2974.2024.08.03

МЕЖДУНАРОДНО-ПРАВОВАЯ КЛАССИФИКАЦИЯ НОВЫХ КИБЕРПРЕСТУПЛЕНИЙ

INTERNATIONAL LEGAL CLASSIFICATION OF NEW CYBERCRIMES

R. Abboud

Summary. The issue of international information security, which includes international legal counteraction to cybercrime, is one of the most controversial and controversial issues since the emergence of this phenomenon. The list of cybercrimes is fixed in almost all international agreements regarding crimes in the field of information technology. However, now, given the rapid development of technology in the era of digitalization, the classification of cybercrimes contained in existing international agreements is losing relevance. The analysis of international agreements on cybercrime, as well as the development and adoption of a new universal convention that will regulate new types of cybercrime, seems necessary to address this issue.

The author draws attention to the fact that such crimes in the field of information technology as cryptojacking, cyberbullying or deepfake are not fixed in international agreements. In order to fill the gap in the above-mentioned problem, the author conducts a comparative legal analysis of international agreements regulating the fight against cybercrime and defines a new classification of cybercrime, which is not enshrined in international treaties.

The conducted research allowed the author to identify an additional classification. according to the following criterion of the object: «illegal use of information and communication technologies for the purpose of violating personal rights in terms of honor and dignity, as well as property in the information space.» The following types of cybercrimes follow from this thesis: a) cyberbullying, b) deepfake, c) cryptojacking, d) duffel carding.

Keywords: cybercrime, cyberbullying, cryptojacking, deepfake, carding, information and communication technologies, international information security.

Аббуд Руслан Ратебович
Старший преподаватель,
Российский государственный университет правосудия
ruslan625@yandex.ru

Аннотация. Вопрос международной информационной безопасности, которая включает в себя международно-правовое противодействие киберпреступлениям, является одним из самых неоднозначных и дискуссионных проблем со времени появления этого феномена. Перечень киберпреступлений зафиксирован практически во всех международных соглашениях в части преступлений в сфере информационных технологий. Однако, в настоящий момент, учитывая стремительное развитие технологий в эпоху цифровизации, классификация киберпреступлений, содержащаяся в действующих международных соглашениях, теряет актуальность. Анализ действующих международных соглашений в части киберпреступлений, а также выработка и принятие новой универсальной конвенции, которая будет регламентировать новые виды киберпреступлений, видится необходимым для решения данной проблематики.

Автор обращает внимание на тот факт, что такие преступления в сфере информационных технологий, как криптоджекинг, кибербуллинг или дипфейк в международных соглашениях не закреплены. Для того чтобы восполнить пробел в вышеназванной проблеме, автор проводит сравнительно-правовой анализ международных соглашений, регулирующих противодействие киберпреступлениям, и определяет новую классификацию киберпреступлений, которая не закреплена в международных договорах.

Проведенное исследование позволило автору выделить дополнительную классификацию по следующему критерию объекта: «противоправное использование информационно-коммуникационных технологий (далее — ИКТ) в целях нарушения прав личности в части чести и достоинства, а также собственности в информационном пространстве». Из данного тезиса вытекают следующие виды киберпреступлений: а) кибербуллинг, б) дипфейк, в) криптоджекин, г) кардинг.

Ключевые слова: киберпреступление, кибербуллинг, криптоджекинг, дипфейк, кардинг, информационно-коммуникационные технологии, международная информационная безопасность.

Наибольший интерес для целей настоящей статьи представляет сравнительно-правовой анализ Конвенции Совета Европы о преступности в сфере компьютерной информации 2001 года (далее — Конвенция СЕ) с проектом Конвенции ООН, внесенным Российской Федерацией о противодействии использованию информационно-коммуникационных технологий (далее — ИКТ) в преступных целях от 27 июля 2021 года (далее — проект Конвенции ООН). Европейский опыт правового регулирования данного вопроса является наиболее наработанным и практически апробированным. Что касается проекта Конвенции ООН, то он находится на стадии принятия.

Конвенция СЕ является первым международным договором, направленным на борьбу с киберпреступлениями путем гармонизации национальных законов, совершенствования метод расследования и расширения сотрудничества между странами.

Киберпреступления, содержащиеся в Конвенции СЕ, в общей сложности образуют 10 видов. В свою очередь, проект Конвенции ООН охватывает 22 вида киберпреступлений. Проект Конвенции ООН дублирует 10 видов киберпреступлений, содержащиеся в Конвенции СЕ, а также вводит новые 12 видов преступлений в сфере ИКТ, которые в Конвенции СЕ не освещены. Среди не-

освещенных в Конвенции СЕ киберпреступлений можно выделить следующие: склонение к самоубийству или доведение до его совершения, оправдание геноцида, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий и тд. Более того, проект Конвенции ООН является существенно прогрессивнее ныне действующих международных соглашений, в котором заложены эффективные механизмы сотрудничества, в частности, в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов.

На сегодняшний день международные соглашения в части противодействия киберпреступлениям не содержат регулирования таких преступлений в сфере информационных технологий, как кибербуллинг, кибержекинг, дипфейк, а также кардинг. Для целей настоящей статьи проведён анализ каждого из вышеперечисленных противоправных деяний в сфере компьютерной информации.

Изначально само определение кибербуллинга было дано Биллом Белсеем, который обозначил его как применение ИКТ в целях недружественного поведения и нанесения вреда пользователям [6, P. 187–189].

В Российской Федерации понятийно-категориальный аппарат в отношении кибербуллинга не установлен, так как отсутствует легальная дефиниция. С.И. Ковалева считает, что кибербуллинг является одной из форм киберпреступления и определяет его, как перманентное направление сообщений, которые содержат информацию, содержащую унижающий достоинства контент. Отличительной особенностью кибербуллинга по мнению

С.И. Ковалевой является так называемая онлайн-агрессия, когда пользователь может пострадать как в эмоциональном, так и в физическом плане [2, С. 122–127].

В качестве примера можно привести Ирландию, где в 2021 году приняли так называемый «Закон Коко», предусматривающий лишение свободы на срок до 7 лет для тех, кто выставляет на всеобщее обозрение в сети «Интернет» интимные изображения человека без его согласия. Николь Фокс повесилась в возрасте 21 года после того, как в течение 3 лет подвергалась физическому и виртуальному насилию. После смерти, затравленной в соцсетях гражданки Ирландии, в ЕС готовится закон против кибербуллинга.

В деле *Geoffrey Andare v Attorney general & 2 others* (2016) Высокий суд Кении признал неконституционным положение, предусматривающее уголовную ответственность за оскорбительные высказывания, а также клевету. Дело возникло из-за сообщения Джеффри Андаре в социальной группе Facebook (запрещенный на территории РФ), в котором он обвинил Титуса Куриа, представителя стипендиального фонда, в использовании своего служебного положения в целях интимного досуга с девушками, претендующими на стипендии. Курия подал жалобу на Андаре в соответствии с разделом 29 кенийского Закона об информации и связи, предусматривающий уголовную ответственность за информацию порочащую честь. Пока дело рассматривалось в уголовном суде, Андаре подал заявление с целью оспорить конституционность раздела 29. Высокий суд постановил, что раздел 29 является неконституционным, поскольку он необоснованно ограничивает свободу выражения мнений, а также потому, что он сформулирован нечетко.

Важно понимать, что кибербуллинг может осуществляться как одним лицом, так и группой, и направлен на определённого человека при помощи ИКТ в целях унижения его чести и достоинства, запугивания или причинения иного морального вреда. Однако последствия данного противоправного деяния посредством ЭВМ носит публичный характер. Потерпевшими от кибербуллинга могут быть как лица, не достигшие совершеннолетнего возраста, так и совершеннолетние лица [4, P. 6–9]. Кибербуллинг в отсутствие юридического регулирования является проблемой моральных и культурных ценностей, выражением отрицательного мнения в безнравственной форме. Так как на данный момент отсутствуют юридические механизмы защиты против кибербуллинга, то наилучшим способом защититься является самозащита. Например, установка настроек конфиденциальности в приложениях, а также коллективная защита, когда пользователи становятся на защиту потерпевшего.

Более того, к одному из современных видов киберпреступлений можно отнести дипфейки. Дипфейк — это генерация изображения или голоса, которая основана на искусственном интеллекте (далее — ИИ). Киберпреступники посредством ИИ переделывают фотографии или видеозаписи своей жертвы в порнографические ролики. Во многом ИИ облегчил задачу преступникам. Злоумышленники обнаруживают такие механизмы в области ИИ, которые доступны и просты в эксплуатации и не требуют специального обучения. Дипфейк осуществляется путем перемещения фотографии лица в видео эротического характера. Далее видео размещается на разных платформах. Преступники совершают данное противоправное деяние при использовании ИКТ из-за корыстных побуждений в целях мести, выкупа, дискредитации или, например, в целях развлечения. В основном жертвами преступников становятся лица, не достигшие совершеннолетнего возраста. Кроме того, с помощью ИИ можно сгенерировать голос любого человека. Например, возможно сымитировать голос человека посредством использования модифицированного алгоритма трансформации текстового содержания в речь

и обработкой нейросетью аудиозаписей речи любого человека.

Другим видом киберпреступления, который не отображён ни в одном из международных соглашений является криптоджекинг. Криптоджекинг — это противоправное использование технических средств преступниками в целях получения криптовалюты. Особенность криптоджекинга заключается в трудности обнаружения, так как он скрыт от жертвы. Данный вид киберпреступления представляет собой угрозу, которая интегрируется в компьютерные системы или мобильные гаджеты, и в дальнейшем использует данные девайса в целях получения криптовалюты. Криптовалюта — это электронные деньги. Биткойн является самой известной криптовалютой. Криптовалюты используют для работы блокчейн (распределенная база данных). В целях создания нового блокчейна необходима добыча вычислительной мощности, и криптовалюта является платой за вычислительные ресурсы, а тех, кто занимается обменом, называют майнерами. Большие компании по майнингу криптовалюты нанимают майнеров в целях управления майнинг-фермами, которые осуществляют вычислительные расчеты. Соответственно преступники, которые совершают криптоджекинг, хотят получить прибыль от майнинга криптовалюты, не неся убытков. Больше всего преступников интересует криптовалюта Monero, которую затруднительно отследить, так как добывается на персональных компьютерах. Таким образом, криптоджекинг помогает преступникам получать криптовалюты, не неся при этом видимых расходов: не оплачивать огромные счета за электроэнергию и специальное оборудование для майнинга.

Другим противоправным деянием, направленным в отношении личной собственности, является кардинг. Несмотря на то, что данный вид киберпреступления не является новым, в международных соглашениях, регламентирующих киберпреступления, данное противоправное деяние с использованием ИКТ конкретно не освещено. Кардинг — это форма кражи личных данных, при которой человек использует информацию о чужой кредитной карте для оплаты покупок или снятия средств со счета. Более того, существует вещевой кардинг, который является разновидностью кардинга. По сравнению с реальным кардингом, вещевой кардинг является менее масштабным. Он направлен на приобретение товаров в онлайн-магазинах, посредством оплаты с чужой кредитной карты. Одним из способа совершения такого рода киберпреступления — совершить взлом онлайн-магазина, где клиенты совершают покупку в сети «Интернет».

По данному виду киберпреступления существует внутригосударственная судебная практика. Национальные суды с такого рода преступлениями уже столкнулись. Так, в деле США против Карима Баратова, обвиняемый взломал аккаунты пользователей Yahoo и украл их личные данные, включая адреса электронной почты и номера телефонов. Хакер был арестован в Канаде 14 марта 2017 года. Затем киберпреступника экстрадировали в США. Федеральный суд Северного округа Калифорнии в Сан-Франциско приговорил уроженца Казахстана 23-летнего Карима Баратова к 5 годам лишения свободы и штрафу в четверть миллиона долларов за взлом почтовых аккаунтов более чем 11 тысяч потерпевших.

В деле США против Романа Селезнева, 21 апреля 2017 года Окружной Суд Соединенных Штатов по Западному Округу Вашингтона в Сиэтле приговорил к 30 годам тюремного заключения ответчика. Сторона обвинения заявляла, что г-н Селезнев путем мошеннических действий с использованием ИКТ украл личную информацию американских граждан с банковских карт. Вследствие чего обвиняемый получил незаконную прибыль в размере 2-ух миллионов долларов США. Г-н Селезнев был задержан в международном аэропорту Мальдив. Стоит отметить, что между Мальдивами и США отсутствует договор об экстрадиции иностранных граждан.

Таким образом, данные преступления по своему характеру могут не ограничиваться территорией одного государства. По мнению А.Г. Волеводз киберпреступление не ограничено территориальными границами одного государства, что говорит о его трансграничном характере [1, С.11–20]. Последствия киберпреступлений выходят за пределы правопорядка отдельного государства в силу степени общественной опасности [7, P. 25–38]. В этом смысле киберпреступление как противоправное уголовно наказуемое деяние, ответственность за которое предусмотрено в законодательстве государства, может быть квалифицировано в качестве преступления международного характера. М.Ч. Бассиуни отмечает, что преступления международного характера содержат «иностранный элемент», т.е. угрожают порядкам двух или более государств [5, P. 28–29]. Для признания киберпреступления преступлением международного характера осложнение «иностранным элементом» должно быть выражено в форме негативных последствий правопорядкам двух или более государств.

С учетом вышеизложенного автор приходит к выводу о том, что киберпреступление является преступлением, обладающее трансграничным характером. Трансграничность выражается в отягощении иностранным элементом и, как следствие, угрожает национальным правопорядкам двух или более государств. Более того, о трансграничном характере говорит то, что киберпреступление не ограничено территориальными границами одного государства [3, С.164–172].

Трансграничный характер киберпреступления позволит максимально эффективно защитить публичные интересы и задействовать международно-правовые механизмы в поимке преступника, а также предотвратить последствия этого противоправного деяния. Несмотря на то, что в каждом национальном законодательстве существует регулирование киберпреступлений, механизмы противодействия будет затруднительно задействовать, если это будет только внутригосударственное регулирование. Международные механизмы борьбы против киберпреступлений осуществимы на основе международных соглашений и в рамках деятельности международных органов, организаций.

Таким образом, трансграничность киберпреступления характеризуется отсутствием каких-либо ограничений по субъектному составу и способам совершения, поскольку информационное пространство не имеет определенных границ, и его последствия выходят за пределы правопорядка отдельного государства в силу степени общественной опасности.

Международные договоры в части противодействия киберпреступлениям не акцентируют внимание на территории конкретного государства. Ни в части субъекта, находящегося на территории данного государства, ни то, что противоправное деяние совершено на территории определенной страны, ни то, что последствия противоправного деяния возникают на территории данного государства. Квалифицирующие признаки данного рода преступления, вышеприведенные международные соглашения не содержат.

Исходя из анализа международных документов в области регулирования преступлений в сфере информационных технологий, и, учитывая, что вышеперечисленные преступления в сфере информационных технологий в международных соглашениях не закреплены, предлагается выделить дополнительную классификацию по следующему критерию объекта: «противоправное использование информационно-коммуникационных технологий в целях нарушения прав личности в части чести и достоинства, а также собственности в информационном пространстве». Из данного тезиса вытекают следующие виды киберпреступлений: а) кибербуллинг, б) дипфейк, в) криптоджекин, г) кардинг.

ЛИТЕРАТУРА

1. Волеводз А.Г. К вопросу о сущности и содержании международного сотрудничества в борьбе с преступностью / А.Г. Волеводз // Международное уголовное право и международная юстиция. — 2007. — No 1. — С. 11–20.
2. Ковалева С.Е. О некоторых актуальных социально-психологических проблемах виртуальной коммуникации в информационную эпоху // XXI век: итоги прошлого и проблемы настоящего плюс. 2017. No 5–6. С. 122–127.
3. Чернядьева Н.А. Цифровые технологии и права человека: эпоха взаимозависимости или кризис международной системы защиты прав человека? // Правопорядок: история, теория, практика. № 2 (37) / 2023. С. 164–172.
4. Aaron, A. (2019). A legal Analysis of Cybercrime and Cyber Torts: Lessons for Nigeria. [LL. B Thesis, University of Lagos], p.6–9.
5. Bassiouni M.C. 1983. The Penal Characteristics of Conventional International Criminal Law. P. 28–29.
6. Belsey B. Cyberbullying: An emerging threat to the «always on» generation. Recuperado el 14. 2006. P. 187–189.
7. Schjolberg, Stein. The history of cybercrime (third edition). 2020. P. 25–38.

Журнал «Современная наука: актуальные проблемы теории и практики»