УДК 314.1

КИБЕРПРЕСТУПЛЕНИЯ КАК ОДИН ИЗ ВИДОВ УГОЛОВНОГО ПРАВОНАРУШЕНИЯ МЕЖДУНАРОДНОГО ХАРАКТЕРА

Аружан Рустамовна Калиева
aruzhankaliyeva@gmail.com
Магистрант второго курса специальности 6D030200 – Международное право
ЕНУ имени Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Ф. Карабаев

Интернет, компьютеры, мобильные телефоны и другие гаджеты технологий за последние несколько десятилетий произвели революцию во всех аспектах человеческой жизни, включая то, как мы общаемся, берём деньги, делаем покупки, читаем новости и развлекаемся. Эти технологические достижения создали множество возможностей для совершения различных форм уголовных правонарушений международного характера. Интернет-преступления часто называют киберпреступностью и происходят потому, что «преступник использует специальные знания о киберпространстве». Таким образом, киберпреступность можно рассматривать как широкий обобщающий термин, охватывающий преступления с использованием компьютеров, в которых эти технологии используются в качестве вспомогательных средств. В то же время термин киберпреступность также включает в себя преступления, связанные с использованием компьютеров, которые являются прямым результатом компьютерных технологий и не существовали бы без них, такие как незаконное проникновение в компьютерную систему. Киберпреступления можно классифицировать по различным категориям, включая киберпреступление (например, незаконный доступ к системе), кибер-обман/кражу (например, кражу личных данных, онлайн-мошенничество, цифровое пиратство), кибер-порно/непристойность (например, материалы о сексуальной эксплуатации детей) и кибер-насилие (например, кибersталкинг; кибертерроризм) [1]

Практически невозможно оценить количество киберпреступлений, которые происходят в большинстве стран мира из-за отсутствия стандартизированных юридических определений этих преступлений и небольшого количества достоверных официальных статистических данных [1].Однако факты свидетельствуют о том, что уровень киберпреступности растёт по мере того, как уровень многих форм преступлений продолжает снижаться [2]

За последние несколько десятилетий объем исследований по киберпреступности вырос в геометрической прогрессии. Большая часть предварительной работы в этой области была сосредоточена на изучении того, как природа киберпреступности и киберпространства отличается от традиционной преступности и земного пространства [3].

Серьёзной проблемой для исследователей киберпреступности, как исторически, так и в настоящее время, является отсутствие официальной статистики по большинству форм киберпреступности. Наиболее часто используемый источник данных о преступлениях, не содержит никакой информации о киберпреступности или о том, была ли какая-либо технология вовлечена в совершение преступления (допустим, в Соединённых Штатах единая система сводной отчётности Федерального бюро расследований (СГД)). Национальная система отчётности об инцидентах (NIBRS), к которой США полностью переходят в 2021 году, также не предусматривает конкретной категории киберпреступности, но позволяет агентствам указывать, был ли компьютер вовлечён в совершение преступления. Поскольку необходимость является матерью изобретения, учёные, изучающие киберпреступность, должны были собирать первичные данные инновационными способами, такими как анализ

обсуждений на форумах, досках объявлений и блогах, развёртывание медовых горшков и разработка полевых экспериментов [4] Кроме того, многие учёные обследовали различные группы населения, уделяя особое внимание выборкам из колледжей.

Учёные особенно заинтересовались проверкой того, применимы ли традиционные криминологические теории, такие как теория рутинной деятельности, теория социального обучения и общая теория преступности, к различным формам киберпреступности. В результате учёные собрали первичные данные и измерили ключевые понятия традиционных криминологических теорий. Акцент сместился с анализа сходств и различий киберпреступности в целом на изучение того, одинаково ли применимы к киберпреступности одни и те же теоретические причины и корреляты традиционной преступности. Эти исследования часто основывались на выборках студентов и молодёжи, учёные изучали более простые формы киберпреступности, такие как онлайн-преследование, цифровое пиратство и угадывание паролей учётных записей, а не более сложные формы киберпреступности, требующие технических навыков. Ограничения данных были не единственным препятствием для исследователей киберпреступности. Они поделились историями о проблемах, с которыми столкнулись при публикации исследований киберпреступности в традиционных журналах уголовного правосудия. Авторы часто слышали от редакторов, что их рукописи интересны, но что «киберпреступность не является преступлением, и эта тема не понравится широкой аудитории». Учёные начали обсуждать международные акты и законы разных государств, чтобы проиллюстрировать, что поведение в Интернете, на самом деле было незаконным и наказывалось правонарушением и применялись определённые санкции. Тем не менее, исследователи киберпреступности все ещё слышали, что их рукописи недостаточно «преступны» и что рукопись будет более уместна в журналах по кибербезопасности, информатике и ИТ.

Тем не менее, общее правовое поля в отношении данного уголовного правонарушения меняется. Ежегодно на национальных и международных конференциях проводится значительное и растущее число докладов, связанных с киберпреступностью. Рабочая группа Европейского общества криминологии (ESC) по киберпреступности, созданная в последние несколько лет, организует дискуссионные форумы и дискуссии по этим темам на заседаниях ESC. Кроме того, отдел киберпреступности был утверждён Американским обществом криминологии (ASC). Также, по всей стране растёт число студентов и аспирантов, занимающихся киберпреступностью. Даже в некоторых программах иностранных образовательных системах предлагают специальные сертификаты и степени бакалавра и магистра в области киберпреступности, такие как Южный университет Джорджии и Университет Южной Флориды и т.д.

Эти события вдохновили на создание первой ежегодной конференции по правам человека в киберпреступности, состоявшейся в Еврейском университете в Иерусалиме, Израиль, в октябре 2018 года. Криминологи и социологи искали возможность собраться вместе, чтобы поделиться своими целенаправленными исследованиями в области киберпреступности с другими специалистами в этой области и определить потенциальных сотрудников в области компьютерных наук и инженерии. Вторая ежегодная конференция по правам человека в киберпреступности состоялась в октябре 2019 года в Нидерландах, а в будущем возможны конференции в Канаде, США и других странах-участницах.

Статьи в этом специальном выпуске были взяты из исследований, представленных на первой конференции, и иллюстрируют несколько моментов о современном состоянии исследований киберпреступности.

Во-первых, они подчёркивают международный характер исследований киберпреступности. Авторы-выходцы из США, Канады, Израиля, Нидерландов и Германии. Во-вторых, они демонстрируют, что теория лежит в основе всех криминологических исследований, даже когда основное внимание уделяется сложным формам киберпреступности. Учёные в этом выпуске используют традиционные криминологические теории, такие как теория рутинной деятельности, теория сдерживания и социального

контроля, чтобы лучше понять причины и корреляции онлайн-мошенничества, порчи веб-сайтов, кибератак на критическую инфраструктуру, проникновения в систему и кибератак на автомобили и т.д. Эти исследования демонстрируют необходимость понимания человеческого элемента киберпреступности, а также ее технических компонентов.

В-третьих, большинство статей в этом выпуске посвящены более сложным формам киберпреступности, демонстрируя, что в настоящее время эта область способна лучше решать эти проблемы с помощью инновационных методов сбора данных. Только в двух статьях были собраны первичные данные путем проведения обследований. Все остальные статьи собирали данные различными способами, такими как изучение полицейских, судебных или пробационных записей и файлов, отправка электронной почты онлайн-мошенникам, очистка онлайн-платформ и загрузка данных о порче веб-сайтов.

Исследования ученых-киберпреступников должны стать ключевым источником информации для политиков, общественности, специалистов по безопасности и других ученых в области права о том, как уменьшить различные формы киберпреступности. К сожалению, сейчас недостаточно научно обоснованных исследований, проверяющих эффективность политики киберпреступности. Дюпон в своей книге "Повышение эффективности предотвращения киберпреступности посредством мониторинга политики" утверждает, что страны по всему миру потратили огромные суммы на инвестиции в кибербезопасность, но не потратили ресурсы на разработку инструментов оценки эффективности государственного вмешательства в сокращение киберпреступности. Дюпон иллюстрирует, что мониторинг политики приведет к созданию более надежной базы знаний об эффективности политики в области киберпреступности, поскольку это приведет к систематическому сбору данных, строгим оценкам и широкому распространению результатов оценки. В своем анализе 18 платформ политического наблюдения он описывает их основные особенности и обсуждает, как они могут быть применены к усилиям по предотвращению киберпреступности. Он утверждает, что создание инструмента наблюдения за предотвращением киберпреступности должно рассматриваться в качестве приоритета с учетом вреда, наносимого киберпреступностью. Дюпон пишет: «Теперь кибер-криминологи должны определить актуальность этой структуры, ее осуществимость и совместные ресурсы, которые понадобятся для ее воплощения в реальность».[5]

Область исследований киберпреступности растет, ученые исследуют новые инновационные методы, и данные исследования оказывают все большее влияние. Этот специальный выпуск, является еще одним показателем того, что область исследований киберпреступности появилась и что человечество движется вперед. Все авторы в этом специальном выпуске предлагают новые направления для этой области, но все они указывают вперед.

Анализ показывает, что в решении проблемы предупреждения преступлений в киберпространстве наибольшую пользу могут дать аналитические, объединительные и юридические подходы. Аналитический метод изучает предотвращение преступлений главным образом за счёт мероприятий технического и аналитического характера. Объединительный метод связан с осуществлением разнообразных организационных мероприятий. Юридический метод опирается на совершенствование юридических механизмов: улучшение юридической базы борьбы с данным видом преступлений, оптимальное решение проблем криминализации общественно опасных деяний, закрепление процессуальных механизмов и т.п. Практика показала бесполезность попыток обеспечения безопасности компьютерных сетей исключительно за счёт защитных организационно-технических мероприятий. Для борьбы с угрозой киберпреступности, которая, безусловно, будет расти с дальнейшим расширением сферы использования информационных технологий, предоставляя всё больше возможности для противоправной деятельности, как отдельным лицам, так и преступным группам, необходимо постоянное международное сотрудничество. Контролировать киберпреступность и бороться с ней на уровне отдельного государства практически невозможно. Важную роль в борьбе с киберпреступностью поэтому играют международные соглашения в

соответствующей области. В уголовном законодательстве Республике Казахстан ответственность за уголовные правонарушения в сфере информатизации и связи регламентируется главой 7 УК РК, в которую включены девять статьи: 205. (Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций) 206. (Неправомерные уничтожение или модификация информации), 207. (Нарушение работы информационной системы или сетей телекоммуникаций 208. Неправомерное завладение информацией), 209. (Принуждение к передаче информации) 210. (Создание, использование или распространение вредоносных компьютерных программ и программных продуктов), 211. (Неправомерное распространение электронных информационных ресурсов ограниченного доступа), 212. (Предоставление услуг для размещения Ьнтернет-ресурсов, преследующих противоправные цели), 213. (Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства) Модельный кодекс государств участников Содружества независимых государств. [6] Что касается обеспечения прав и безопасности, то механизм реализации и функционирования поведения субъектов в глобальном информационном пространстве возможен только на основе комплексного подхода в рамках решения организационных, правовых и технологических вопросов под эгидой ООН.

Подводя итог вышесказанному, отметим, что борьба за безопасность киберпространства недостаточна на уровне отдельных государств. Сам характер рассматриваемых преступлений, основанный на открытом и публичном характере телекоммуникационных сетей и связанный со спецификой вопросов подсудности, а также спецификой подхода правоохранительных органов к расследованию таких преступлений, способствует росту и развитию киберпреступности. Для эффективной борьбы с глобальным явлением киберпреступности необходимо сотрудничество на международном уровне, на двусторонней и многосторонней основе, путём подписания договоров, соглашений и участия государств в международных организациях и конференциях. Необходимы усилия со всех сторон государств мира по созданию правовой базы борьбы с киберпреступностью.

Список использованных источников

1. Holt, Bossler, and Seigfried-Spellar 2018; Wall 2001
2. Tcherni et al. 2016 январь, Университет Нью Хейвен, штат Коннектикут .
3. Grabosky 2001; Wall 1998. Professor Peter Grabosky, PhD (Political Science), MA (Political Science) (Northwestern University), BA (Colby College), Professor Emeritus, College of Asia & the Pacific
4. Holt and Bossler 2016.Cybercrime in Progress, Theory and prevention of technology-enabled offenses, стр. 10
5. Enhancing the effectiveness of cybercrime prevention through policy monitoring - Benoît Dupon, (стр. 74) Pages 500-515 13 Dec 2019
6. Әділет информационно-правовая система нормативных правовых актов Республики Казахстан 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан