DOI: 10.36719/2706-6185/04/10-15

Ильгар Имдат оглу Гасанов
Бакинский Государственный Университет
магистрант
ilqar-hesenov-9797@mail.ru

ПОНЯТИЕ И ХАРАКТЕРНЫЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПЛЕНИЙ В МЕЖДУНАРОДНОМ ПРАВЕ

Резюме

В статье рассматриваются понятие и характерные признаки киберпреступлений в современном международном праве, их виды и возможные способы их совершения. Понятия киберпреступность и киберпреступник в настоящее время используются достаточно широко в связи с произошедшим в 21 веке информационно-телекоммуникационным прорывом и стали неотъемлемой частью всех сфер жизни человека. Киберпреступность носит трансграничный характер. Поэтому преступники (особенно хакеры) могут совершать преступления из страны, где такая деятельность не является незаконной или отсутствует законодательство об этой деятельности.

Ключевые слова: *киберпреступление,международное право, транснациональные преступления, Интернет, ксенофобия, контент, конвенция*

Ilgar Imdat Hasanov
Baku State University
master student
ilqar-hesenov-9797@mail.ru

The concept and characteristics of cybercrimes in international law

Abstract

The article examines the concept and characteristic features of cybercrime in modern international law, their types and possible ways of their commission. The concepts of cybercrime and cybercriminal are currently used quite widely in connection with what happened in the 21 st centry information and telecommunication breakthrough and became an integral part of all spheres of human life. Cybercrime is cross-border in nature. Therefore, criminals (especially hachers) can commit crimes from a country where such activity is not illegal or there is no legislation on this activity.

Keywords: *cybercrime, international law, transnational crimes, Internet, xenophobia, content, convention*

Введение

Преступность в киберпространстве является одной из самых сложных проблем, с которыми международное сообщество сталкивается в последние годы в связи с развитием информационных и коммуникационных технологий.Возможности современных информационных технологий активно пытаются использовать организованные преступные сообщества и преступники-одиночки, что приводит к появлению новых видов преступных деяний - киберпреступлений. Представители криминалитета осуществляют незаконное вмешательство в работу компьютеров, систем и компьютерных сетей, осуществляют хищение, присвоение, вымогательство компьютерной информации, организуют удаленные атаки на информационные ресурсы, разрабатывают и распространяют компьютерные вирусы и т.д. По своему механизму, способам совершения и сокрытия эти виды преступлений имеют определенную специфику, они характеризуются высоким уровнем латентности и низкой раскрываемостью (Журавленко, Шведова, 2015: 66-67).

Особое место в этом плане занимает Интернет, правовой статус которого до сих пор четко не определен, а отлаженных механизмов государственного регулирования этого нового для юриспруденции феномена пока не существует. Подобное положение дел играет на руку преступному миру, оно способствует быстрой криминализации Интернета. Например, наркоторговцы и их клиенты все чаще заключают сделки в «закрытых» чат-каналах, защищенных от внимания посторонних программно-аппаратными средствами. Наркодилеры используют для отмывания доходов интернет-банки. Увеличивается число сайтов, принадлежащих организованным преступным группировкам, через которые они интенсивно обмениваются информацией (Белов, 2009: 116-117). С учетом современных процессов информатизации общества сфера компьютерных технологий используется как плацдарм для совершения многих преступлений, входящих в структуру киберпреступности. С одной стороны, речь идет о тех киберпреступлениях, которые непосредственно посягают на информационную безопасность личности, общества и государства (к этой категории относятся, например, несанкционированный доступ к компьютерной информации, модификация компьютерной информаци и др.) (Majidli, 2013: 112; Бородин, 2011: 217; Douglas, 2016: 17-20). С другой стороны, можно говорить о преступлениях, связанных с кибертехнологиями. Использование при их совершении информационно-телекоммуникационных систем характеризует киберпреступную направленность деяния (в частности, в данную группу входят кража, мошенничество, присвоение или растрата, совершенные с использованием компьютерных технологий, манипулирование рынком и проч.) (Семыкина, 2014: 49-54).

Несмотря на все эти существующие проблемы, в современном праве, о том числе в правовой доктрине, международном и внутригосударственном законодательстве до настоящего времени не выработаны единая терминология и единый подход к явлению и понятию киберпреступлении, употребляемому наряду с понятием компьютерная преступность.

В научных кругах, о том числе в отечественных и зарубежных изданиях и средствах массовой информации, преступления, совершаемые в компьютерных и телекоммуникационных системах, номинируются по-разному: компьютерные преступления, преступления в сфере высоких технологий, информационные преступления, киберпреступления, преступления в сфере безопасности обращения компьютерной информации, преступления в сфере компьютерной информации, кибербандитизм и др.

Термин «киберпреступность или киберпреступление» часто употребляется наряду с термином «компьютерная преступность», причем нередко эти понятия используются как синонимы. Действительно, эти термины очень близки друг другу, но все-таки, на наш взгляд, не синонимичны. Однако понятие «киберпреступление» (в англоязычном варианте - cybercrime) семантически шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого глобального явления, как преступность в информационном пространстве. Если термин «киберпреступление» соотносится как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей, то понятие «компьютерная преступность» в основном относится к преступлениям, совершаемым против электронных устройств и хранящихся в них данных (Номоконов, Тропина, 2013: 148-159). Так, Оксфордский толковый словарь определяет приставку «cyber-» как компонент сложного слова. Ее значение - «относящийся к информационным технологиям, сети Интернет, виртуальной реальности» (6). Практически такое же определение дает Кембриджский словарь. Таким образом, «cybercrime»-это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. В то же время термин «computer crime» в основном относится к преступлениям, совершаемым против компьютеров или компьютерных данных (7).

В опубликованных теоретических источниках продолжаются дискуссии о подходах к определению понятия «киберпреступление». Например, по словам Сьюзан Берннер и Марка Гудмана термин киберпреступление предпочтительнее, потому что он включает традиционные преступления, такие как компьютерные кражи, мошенничество и обман, а также преступления, в которых компьютерные системы и информация являются объектом преступления (Brenner, Goodman, 2002: 3-153). Некоторые авторы считают, что киберпреступление в широком смысле -

это любое противоправное деяние, совершаемое посредством или в связи с компьютерными устройствами, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством использования компьютерных технологий (например, Пестриков, В.А., Мамлеев, Р.Р., Маджидли, С.Т. и др.). В общем и в целом киберпреступления связываются указанными авторами с правонарушениями, совершаемыми в различных информационных сетях.По мнению И.Г.Чекунова, киберпреступлениями являются общественно опасные деяния, совершаемые с использованием средств и способов компьютерной и мобильной (сотовой) техники, их программных компонентов в отношении информации, размещенной, используемой, обрабатываемой, изменяемой в виртуальном пространстве сети Интернет (Чекунов, 2012: 9-12).

Профессор Марко Греке отмечает, что термин киберпреступление более успешен, чем термин компьютерное преступление, которое используется для описания ряда преступлений, включая традиционные компьютерные преступления, а также сетевые преступления (Greke, 2012: 11). В.Д.Курушин и В.А.Минаев считают, что киберпреступления - это действия в Интернете, при которых компьютер является либо орудием, либо предметом криминальных посягательств в виртуальном пространстве. С позиции И.М.Рассолова, киберпреступления - это общественно опасные деяния, совершаемые с применением средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете (Рассолов, 2009: 135). По мнению Т.Л.Тропина, «киберпреступление - это виновно совершённое общественно опасное, уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные, общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству» (Тропина, 2005: 9). Известный ученый в области транснационального уголовного права, профессор Н.Бойстер подчеркивает, что киберпреступления это вид транснациональной преступлений, который подпадает под действие статьи 3 Палермской конвенции 2000 года о транснациональной организованной преступности и обычно совершается транснациональными организованными преступными группами и организациями в определенных целях (Boister, 2012: 3-6).

В настоящее время все чаще отмечаются факты освоения информационных технологий и компьютерных сетей транснациональными террористическими и экстремистскими организациями, что обусловило появление наиболее опасной разновидности киберпреступленй – кибертерроризма. По заявлениям западных спецслужб и правоохранительных органов, такие террористические организации, как «Аль-Каида», «Хезболла», «Абу Нидаль», «ПКК» и др., активно используют возможности Интернета. С применением его возможностей ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение в свои ряды новых членов, осуществление незаконных финансовых операций и т.д. (Eagle, 2018: 39-77). Например, многие хакерские группы, такие как югославская «Черная рука», палестинская «Unix Security Guard», не сделав ни единого выстрела, своими кибератаками наносили столь серьезный ущерб институтам государственной власти ряда стран, что заняли «достойное» место в списках террористических организаций. В феврале 2015 г. «Лаборатория Касперского» раскрыла одну из крупнейших киберафер в истории. При проверке в Киеве «взбесившегося» банкомата, который «выплевывал» купюры под ноги прохожим, специалисты выяснили, что в компьютерную сеть банка проникла программа червь, с помощью которой злоумышленники отслеживали каждый шаг сотрудников. Это позволило им имитировать их действия и незаметно переводить со счетов деньги малыми суммами, чтобы не вызвать подозрение. За несколько месяцев они перевели более 300 млн (а по некоторым данным - около миллиарда) долларов из десятков банков в России, США, Японии и стран ЕС (6).

При рассмотрении национального законодательства мы видим, что в отношении этих преступлений используются по существу различные термины: например, компьютерные

преступления (Закон Малайзии о компьютерных преступлениях 1997 г, и Суданский Закон о компьютерных преступлениях 2002 г.), киберпреступления (Глава XX Уголовного кодекса Азербайджанской Республики; Раздел IX Уголовного кодекса Болгарии), преступления в области электронных коммуникаций (Закон Албании об электронных сообщениях 2008 г, Закон Республики Тонго 2000 г.), преступления в области информационных технологий (Закон об информационные технологии Индии 2000 г, Закон о преступлениях в области информационных технологии Саудовской Аравии 2007 г), преступления в области высоких технологий (Закон Сербии о борьбе с преступлениями в области высоких технологий 2010 года). Следует признать, что несмотря на нынешние глобальные угрозы, создаваемые киберпреступлении, не удалось достичь консенсуса по определению киберпреступлений и ее видов не только в международном праве, но и в национальном законодательстве зарубежных государств. Кроме этого, в настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надежных методов сбора таких данных. И дело не только в отсутствии единообразия национального уголовного законодательства стран в сфере борьбы с киберпреступностью и разной практике его применения, различиях в формировании уголовной статистики и особенностях правоохранительной системы. До сих пор неясно, до какой степени достоверна статистика об экономических потерях от киберпреступности. Есть мнение, например, что доход от киберпреступлений значительно превышает доход от других преступлений, включая торговлю наркотиками.

На пути разграничения терминологических единиц «киберпреступление» и «компьютерная преступность» и предпочтения именно первой из них стоит и международное право. Впервые признаки, классификация и оценка значения киберпреступлений были закреплены решением «Конвенции о киберперступности», принятой Советом Европы 23 ноября 2001 года, которая оперирует именно термином «cybercrime», а не «computer crime». Конвенция СЕ различает два вида противоправных действий, связанных с киберпреступностью: преступления и правонарушения. Часть первая второй главы Конвенции СЕ построена таким образом, что все составы преступлений поделены подразделами по родовому объекту, а подразделы, в свою очередь, делят преступления по видовым признакам объекта посягательства. Конвенцией СЕ и Протоколом № 1 (принятым в 2002 г.) к Конвенции о кибер-преступности предусмотрено пять групп преступлений: 1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. 2. Правонарушения, связанные с использованием компьютерных средств. 3. Правонарушения, связанные с содержанием данных. 4. Правонарушения, связанные с нарушением авторских и смежных прав. 5. Акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

Последние два вида киберпреступлений являются спорными при квалификации преступлений. Некоторые ученые полагают, что эти два вида преступлений - противо-правные деяния, которые охватываются составами в национальных уголовных кодексах. Не являются новыми категориями преступлений, так как совершены с помощью современных средств, которые можно отнести к факультативному признаку преступления. Другие ученые считают, что такие киберпреступления - качественно новая категория преступлений, требующая принятия новых норм, освоения новых методов расследовани (Федулов, 2007: 103-107).

Попытка объяснения сущности понятия киберпреступности предпринята Конгрессом ООН по предупреждению преступности и обращению с правонарушителями. Согласно его резолюции «киберпреступление – это любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети» Иными словами, к киберпреступлениям может быть отнесено любое противоправное деяние, совершённое в электронной среде. Значительно шире рассматривают компьютерные преступления авторы «модельного закона» о киберпреступности Международного союза электросвязи (2009 г.), соотнося их с противоправными деяниями, совершенными в киберпространстве, и предметом атак которых являются: «компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных и пользователи. В настоящее время официальное законодательное

закрепление термина «киберпространство» на международном уровне не принято, впрочем, как и определение киберпреступности.

Выводы

Таким образом, понятие киберпреступлений шире компьютерных, так как охватывает большую сферу действий, совершаемых преступниками. Киберпреступления - это те виды преступлений, которые совершаются посредством не только использования компьютеров, но и других технических устройств, виртуального пространства, сети Интернет. Киберпреступления это умышленные преступные деяния, совершаемые в виртуальном пространстве с использованием телекоммуникационных способов и средств (Бородин, 2011).

Киберпреступность - явление по своей природе трансграничное. Особо важно подчеркнуть необходимость разработки единого подхода к явлению киберпреступности, так как отсутствие общепринятых и нормативно закрепленных дефиниций Интернет, киберпреступление, киберпреступность, компьютерные преступления, позволяет преступникам избегать юридической ответственности, пользуясь несогласованностью правовых баз различных государств. Преступники могут совершать преступления из страны, где подобная деятельность не является противозаконной (17).

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности:повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.); трансграничный характер сетевых преступлений; особая подготовленность преступников и интеллектуальный характер преступной деятельности; нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств; возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно, возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления; многоэпизодный характер преступных действий при множественности потерпевших; неосведомленность потерпевших о том, что они подверглись преступному воздействию; дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего; невозможность предотвращения и пресечения преступлений данного вида традиционными средствами (Douglas, 2016).

Таким образом, киберпреступление может быть определена как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных.

Литературы

1. Журавленко, Н., Шведова, Л. (2015). Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере. Общество и право. № 3 (53), с.66-70.
2. Белов, О. (2009). Информационное обеспечение раскрытия и расследования преступлений.
3. Majidli, S. (2013). Internet law and ethics. Textbook. Baku. Science and education publishing house.
4. Семыкина, О. (2014). Тенденции борьбы с преступлениями в сфере информационных технологий (сравнительно-правовой аспект). Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов», с.49-54
5. Номоконов, В., Тропина, Т. (2013). Киберпреступность: проблемы борьбы и прогнозы. Библиотека криминалиста. № 5 (10), с.148-159.
6. Cambridge dictionaries, http://www.dictionary.com/browse/cybercrime
7. Oxford dictionaries, www https://en.oxforddictionaries.com/definition/cybercrime

8. Brenner, S., Goodman, M. (2002). The emerging consensus on criminal conduct in cyberspase. International Journal of Law and Information Technology. Volume. No 02, p. 3-153
9. Чекунов, И. (2012). Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений. Право и кибербезопасность. Юрист.
10. Greke, M. (2012). Understanding cybercrime: phenomena, challenges and legal response. Geneva.
11. Рассолов, И. (2009). Право и Интернет. Теоретические проблемы. Изд. 2-е, доп. Норма.
12. Тропина, Т. (2005). Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Авторефарат канд. юрид. наук. Владивосток.
13. Boister, N. (2012). An İntroduction to Transnational Criminal Law. Oxford. Oxford University Press.
14. Eagle, A. (2018). The Changing Structure of International Terrorism and Terrorist Organizations' Use of Social Media. The Example of DAESH and YPG in Syria. Security Strategies Year: 14 Issue: 27, pp.39-77.
15. Федулов, В. (2007). Компьютерный терроризм как инновация современного высокотехнологичного общества. Вестник Московского областного государственного университета. Серия: Юриспруденция. № 1-2, с.103-107.
16. Бородин, К. (2011). Проблемы правового регулирования отношений в сети Интернет. Современные проблемы юридической науки. Часть I. Материалы VII Международной научно-практической конференции молодых исследователей. Челябинск.
17. Взбесившийся банкомат вскрыл одну из крупнейших киберафер в истории http://www.pravda-tv.ru/2015/02/16/123671
18. Douglas, J. (2016). İnformation security policies, procedures and standards. A practitioner’s reference. London-New York, CPC Press.

Рецензент: к.ю.н. Рахим Мамедов

Сообщение от: 10.06.2021 Отправлено: 01.08.2021