**УДК 343.34**

**А.И. ХАЛИУЛЛИН,**

***старший следователь, аспирант***

*ГОУ ВПО «Академия Генеральной прокуратуры Российской Федерации», г. Москва*

# МЕСТО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ КАК ПРИЗНАК СОСТАВА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

*В статье рассматриваются проблемы определения места совершения компьютерных преступлений во взаимосвязи с юрисдикцией государств, а также нормативно-правовая база государств в отношении преступлений данного типа. Указываются их характерные особенности, приводится анализ существующих подходов к вопросу места совершения преступлений в сфере компьютерной информации.*

В Уголовном кодексе Российской Федерации закреплено понятие времени совершения преступления (ч. 2 ст. 9 УК РФ), но не решен вопрос относительно места совершения преступления. Это обстоятельство затрудняет единообразное решение вопроса о наличии оснований уголовной ответственности. Вместе с тем определение места совершения преступления необходимо для установления пределов действия уголовного закона, что немаловажно для материального уголовного права [1, с. 18].

Установлению места совершения преступления в сети Интернет препятствует «коллизия между фундаментальными принципами физики и международного права, а именно: электроны могут перемещаться по сетям, свободно пересекая государственные границы, а юрисдикция представителей национальных властей нет <…>. Согласно принципу суверенитета каждое правительство обладает исключительной властью в отношении событий, произошедших в рамках его границ» [2, с. 220–221].

Исследователи неоднократно указывали на необходимость установления «общепризнанного перечня преступлений международного характера, посягающих на международные отношения и правопорядок, чему должна способствовать в ближайшей перспективе кодификация норм и принципов международного уголовного права» [3, с. 29–34]. По мнению Е. Войниканис и М. Якушева, в подобный перечень должны быть включены компьютерные преступления с учетом их возрастающей международной опасности и причинения при их совершении ущерба минимум двум, а, как правило, большему числу государств [4, с. 69].

В вопросах регулирования киберпространства и, в частности, определения места совершения преступления в сети Интернет существует ряд интересных мнений. Д. Менте предлагает рассматривать правовой режим информационно-телекоммуникационной сети Интернет в рамках теории интернациональных пространств [5, с. 18], на которые не распространяется национальный суверенитет. К ним, помимо киберпространства, отнесены также Антарктика, космос и открытое море. По данному вопросу разумной представляется точка зрения Д.А. Савельева, согласно которой вопрос «более сложен, чем проведение простой аналогии с такими объектами, как космос или открытое море, хотя бы потому, что не существует какого-то материального знака, на котором можно было бы отметить принадлежность к государству» [6, с. 52].

Высказан ряд схожих предложений, в рамках которых Интернет рассматривается по аналогии с так называемыми открытыми пространствами (космическое пространство, открытое море) [7, с. 313–314], территориями со смешанным правовым режимом (территориальные воды прибрежных государств, исключительные экономические зоны, континентальный шельф, реки) [8, с. 80].

По мнению Ю.М. Батурина, необходимо распространение национальной юрисдикции в

сети Интернет, а именно суверенитета над ее национальным сегментом [9, с. 92]. Примером являются домены различных стран. В отношении Российской Федерации юрисдикция распространяется, следуя данной логике, на сайты в доменах «.ru», «.рф» и «.su» (последний как правопреемник СССР). Информация в указанных пределах образует так называемый «Рунет», то есть российский сегмент киберпространства. Полагаем, что при реализации данного подхода возникнут закономерные сложности в отношении международных доменов «.edu», «.int», «.com», так как их принадлежность к определенному государству отсутствует. Кроме того, физически информация сайта домена «.ru» либо «.рф» может храниться на сервере, который при этом находится в другом государстве, что создает определенные сложности для национальной юрисдикции Рунета.

Следует отметить, что принцип национальной юрисдикции нашел свое отражение в ст. ст. 2, 11 модельного закона СНГ «Об основах регулирования Интернета» [10], причем сфера его действия искусственно сужена в предельно возможную форму. Согласно ст. 11 указанного модельного закона «юридически значимые действия, осуществленные с использованием Интернета, признаются совершенными на территории государства, если действие, породившее юридические последствия, было совершено лицом во время его нахождения на территории этого государства». Следовательно, по законодательству РФ, у лица, совершившего преступление в сети Интернет, ответственность фактически наступает лишь в случае его физического нахождения на территории РФ.

В рамках настоящего исследования предпринята попытка анализа территориального, реального, универсального принципов, а также принципа гражданства при определении места совершения преступления в отечественной практике, которая показала неоднозначный характер возможности применения принципов к деяниям, совершаемым с использованием сети Интернет, обладающей свойством существования в ней трансграничных правоотношений. Содержание принципов представляет интерес при рассмотрении проблемы уголовной юрисдикции в зависимости от конструкции состава преступления. Как отмечает В.Н. Щепетильников, «в преступлениях с материальным составом следует вести речь о юрисдикции того государства, которому причинен ущерб, где находится оконечное устройство, на которое, например, пришло сообщение оскорбительного содержания, вредоносная программа, поступила команда на перемещение денежных средств и т.п.» [11, с. 112]. В формальных же и усеченных составах, наоборот, «наиболее целесообразно в качестве места причинения вреда рассматривать именно местонахождение оконечного устройства (компьютера), с которого производится размещение в сети информации, порочащей честь или рассылка вредоносных программ» [12, с. 50], а следовательно, и вести речь о юрисдикции соответствующего государства.

Для определения места совершения преступления К. Корнилс предлагает в целях четкой локализации ответственности и ограничения национальной юрисдикции руководствоваться местом действия виновного. Но автор делает вывод, что если правонарушитель вводит незаконный материал на территорию своей страны, то действия виновного подпадают всегда под юрисдикцию этой страны с учетом его местонахождения. Если данные вводятся из-за рубежа в сервер, расположенный в этой стране, то деяние должно рассматриваться как внутригосударственное преступление. Если данные вводятся из-за рубежа в сервер третьей страны, то налицо экстерриториальное деяние, то есть уголовная ответственность может наступать по законодательству любой страны–участницы отношений по передаче такой информации посредством Интернета, но только при наличии соответствующих международных соглашений [13, с. 80–92].

Существующие международные соглашения, направленные на противодействие преступлений трансграничного характера, носят в целом рекомендательный характер и не охватывают все криминальные проявления в сети интернет. Международная консолидация усилий в борьбе с международной преступностью нашла свое отражение в Конвенции ООН против транснациональной организованной преступности [14], Международной конвенции о борьбе с финансированием терроризма [15], Конвенции ООН против коррупции [16]. Европейским союзом были приняты: Конвенция Совета Европы об отмывании, выявлении, изъятии, конфискации доходов от преступной деятельности и финансировании

терроризма и Конвенция Совета Европы о предупреждении терроризма [17, с. 199] и т.д.

В международно-правовой практике существуют примеры использования отдельными государствами процедуры насильственного захвата обвиняемых на территории иностранного государства. Расширение «экстерриториальной» юрисдикции получило формализованное отражение в правовой доктрине Кера-Фрисби и выражение принципом «male captus bene detentus», согласно которому суд может установить юрисдикцию над лицом независимо от обстоятельств его ареста. Реализация принципа происходит не в силу права, а по праву силы [18, с. 192].

Значимой с точки зрения развития международного законодательства в сфере противодействия трансграничным компьютерным преступлениям является Европейская Конвенция о киберпреступности (далее – Конвенция) и Дополнительный протокол к ней относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем [19]. В преамбуле Конвенции определена цель ее принятия – поддержание «общей уголовной политики, нацеленной на защиту общества от киберпреступлений, через принятие соответствующих законодательных актов и укрепление международного сотрудничества». Достаточная согласованность правовых норм позволяет государствам-участникам Конвенции осуществлять эффективное сотрудничество, например, при проведении совместных целевых операций по пресечению преступных действий в сетевом пространстве. В соответствии с распоряжением Президента РФ «О подписании Конвенции о киберпреступности» от 15.11.2005 Россия оставляла за собой право определиться с участием в Конвенции при условии возможного пересмотра положений пункта «b» ст. 32, которые «могут причинить ущерб суверенитету и безопасности государств-участников конвенции и правам их граждан» [20].

Конвенция устанавливает, что каждое государство принимает законодательные и иные меры для уголовного преследования лиц, совершивших преступления на его территории. Юрисдикция государства распространяется и на его граждан, если совершенное ими деяние является уголовно наказуемым в месте совершения преступления, либо если деяние совершено за пределами территориальной юрисдикции какого-либо государства. При возникновении ситуации, когда о своем праве на юрисдикцию заявляют более одного государства, им предлагается проводить консультации в целях выбора «наиболее подходящей юрисдикции для осуществления судебного преследования» [21, с. 192]. На наш взгляд, это имеет важное значение, поскольку при преследовании участников международной преступной группы возможна ситуация проведения судебного разбирательства по поводу одних и тех же противоправных действий в отношении различных субъектов в нескольких государствах одновременно. При таком согласовании может учитываться и заинтересованность в уголовном преследовании преступников, которая может существенно различаться для вовлеченных сторон в зависимости от внутренней политической или экономической ситуации.

В Конвенции оговаривается возможность получения доступа представителей правоохранительных органов к компьютерным данным, хранящимся на территории другого государства, без передачи запроса о предоставлении взаимной помощи. В то же время необходимо учитывать обстоятельства индивидуального случая, что делает нецелесообразным навязывание жестких общих правил. Определены два варианта, при которых односторонний трансграничный доступ считается допустимым: в-первых, признается правомерным доступ к любым общедоступным данным, расположенным в открытых источниках, независимо от их географического местонахождения; во-первых, трансграничный доступ к компьютерным данным на территории другой страны и их получение считаются правомерными, если субъект, производивший доступ, получил добровольное согласие лица, уполномоченного раскрывать эти данные на законном основании.

На наш взгляд, признание компьютерных преступлений, совершаемых в сети Интернет, носящих международный характер, способствовало бы уменьшению количества спорных аспектов при установлении юрисдикции по данным фактам. Достижение поставленной цели возможно путем присоединения Российской Федерации к Европейской Конвенции о борьбе с киберпреступностью. Существующие правовые механизмы

способны обеспечить оптимальное определение юрисдикции при стремлении государств к согласованным действиям.

Таким образом, решить проблему определения места совершения преступления в сфере компьютерной информации можно основываясь принципе гражданства, при этом обязательно учитывая физическое местонахождение преступников и жертв.

**Список литературы**


1. Поддубный А.А. Определение места совершения преступления при квалификации преступления // Российский следователь. – 2001. – № 3. – С. 18.
2. Панов Н.И. Способ совершения преступления и уголовная ответственность. – Харьков, 1982. – С. 20.
3. Информационная война и международное право. Право и информатизация общества. – М., 2002. – С. 220–221.
4. Каюмова А.Р. Соотношение международной и национальной уголовной юрисдикции // Российское правосудие. 2007. – № 9(17). – С. 29–34.
5. Войниканис Е., Якушев М. Информация, собственность интернет: традиции и новеллы в современном праве. – М.: Волтерс-Клувер, 2004. – С. 69.
6. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces // Mich. Telecomm. Tech. L. Rev.69 1998. – P. 18.
7. Савельев Д.А. Юрисдикция государств в сети Интернет // Сборник тезисов II Всероссийской конференции «Право и Интернет: теория и практика». – М.: Спарк, 2008. – С. 52.
8. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2009. – С. 313–330.
9. Дашян Ш.С. Право информационных магистралей: вопросы правового регулирования в сфере Интернет.– М.: Ворлтерс-Клувер, 2007. – С. 80.
10. Телекоммуникации и право: вопросы стратегии / под ред. Ю.М. Батурина. – Сер. «Журналистика и право». Вып. 26. – М.: Центр Право и СМИ, 2000. – С. 92.
11. Модельный закон СНГ «Об основах регулирования Интернета»:приложение к постановлению МПА СНГ от 16.05.2011 № 36–9. – URL: http://www.iacis.ru/data/prdoc/09a-2011.doc (дата обращения 10.08.2011).
12. Щепетильников В.Н. Уголовно-правовая охрана электронной информации: дис. ... канд. юрид. наук. – Елец, 2006. – С. 112.
13. Бабкин С.А. Право, применимое к отношениям, возникающим при использовании сети «Интернет»: основные проблемы. – М.: Центр ЮрИнфоР, 2003. – С. 50.
14. Корнилс К. Локализация места ответственности за преступления, связанные с Интернетом // Право и информатизация общества. – М., 2002. – С. 80–92.
15. Собрание законодательства РФ. – 2004. – № 40. – Ст. 3882.
16. Собрание законодательства РФ. – 2003. – № 12. – Ст. 1059.
17. Собрание законодательства РФ. – 2006. – № 26. – Ст. 2780.
18. Правовые основы деятельности органов внутренних дел: сб. нормативных правовых актов. В 3 т. Т. 1. – М., 2007. – С. 199.
19. Попов В.М. Международное право: учебник для вузов. – М.: Бриз-М., 2008. – С. 192
20. Европейская Конвенция о взаимной правовой помощи по уголовным делам (ETS № 185, 2001 г., ETS №186, 2003 г.) // Собрание законодательства РФ. – 2003. – № 23. – Ст. 2349.
21. О признании утратившим силу распоряжения Президента РФ от 15.11.2005 № 557-рп «О подписании Конвенции о киберпреступности»: распоряжение Президента РФ от 22.03.2008 № 44-рп // Собрание законодательства РФ. – 2008. – № 13. – Ст. 1295.
22. Report of United Nations Commission on International Trade Law – United Nations Publications. – 2008. – P. 192.


*В редакцию материал поступил 15.11.11*

*Ключевые слова*: место совершения преступления; преступление в сфере компьютерной информации; трансграничные преступления.