УДК 34

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СТРАНАХ ЕС

Н.А. Швед

Научно-практический центр проблем укрепления законности и правопорядка
Генеральной прокуратуры Республики Беларусь, Белоруссия

nadezhdas@tut.by

Поступила в редакцию 01.09.2016

Для эффективной борьбы с компьютерными преступлениями важно учитывать опыт зарубежных стран по противодействию компьютерной преступности, и в первую очередь уголовно-правовыми средствами. В статье проведен сравнительно-правовой анализ уголовного законодательства ряда стран Европейского союза с целью выявления общих и отличительных особенностей установления уголовной ответственности за несанкционированный доступ к компьютерной информации. Определены основные подходы европейских законодателей к криминализации рассматриваемого общественно опасного деяния. Отмечается несогласованность европейского уголовного законодательства и необходимость унификации подходов к криминализации несанкционированного доступа к компьютерной информации.

Ключевые слова: компьютерные преступления, несанкционированный доступ к компьютерной информации, уголовное законодательство, информационная безопасность, компьютерная информация.

Проблема борьбы с несанкционированным доступом к компьютерной информации в настоящее время остро стоит перед зарубежными государствами. Международным сообществом признано, что одним из путей совершенствования сотрудничества в борьбе с компьютерными преступлениями является согласование определенных материальных норм уголовного права различных государств мира. Рост компьютерных преступлений, имеющих международный характер, и все более возрастающая угроза от этих преступлений, в первую очередь для информационной и экономической безопасности, вызывают необходимость унификации законодательства в этой области.

Несанкционированный доступ к компьютерной информации, по сути, является базовым составом, фундаментом компьютерных преступлений. Его опасность усиливается в связи с ростом различных способов использования компьютерных систем и сетей, что происходит в условиях активного развития технологий электронных платежей и увеличения электронного документооборота. Несанкционированный доступ опасен еще и тем, что он нередко становится этапом в совершении других преступлений, поскольку в условиях автоматизированной обработки и хранения информации их совершение без такого доступа фактически невозможно.

Для эффективной борьбы с компьютерными преступлениями, в частности с несанкционированным доступом к компьютерной информации, необходимо учитывать опыт других государств, поскольку данный вид преступлений является относительно новым в отечественном уголовном законодательстве. В этой связи представляет интерес сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах Европейского союза.

Следует отметить, что в Европейском союзе давно и достаточно активно ведется работа по противодействию компьютерным преступлениям. С 1983 г. при Совете Европы была создана экспертная группа по проблеме борьбы с компьютерной преступностью, результатом работы которой явились подготовленные и утвержденные всесторонние рекомендации для стран-участниц [1].

В первой Рекомендации № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях, связанных с компьютером, принятой 13 сентября 1989 г., содержатся руководящие указания для национальных законодательных органов. Так, в частности, в перечень правонарушений, рекомендованных к обязательному включению во внутригосударственное уголовное законодательство, в числе прочих был отнесен и несанкционированный доступ.

Необходимо также отметить, что государства Европейского союза ратифицировали и опираются на Конвенцию о преступности в

сфере компьютерной информации (заключена в г. Будапеште 23 ноября 2001 г.). Следует отметить, что в разделе 1, посвященном преступлениям против конфиденциальности, целостности и доступности компьютерных данных и систем, на первом месте обозначен противозаконный доступ, под которым понимается преднамеренное получение доступа к компьютерной системе в целом или любой ее части неправомерно. При этом любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой [2].

Вместе с тем следует отметить, что законодательство об уголовной ответственности за несанкционированный доступ к компьютерной информации в европейских странах существенно различается. Системный анализ уголовного законодательства ряда стран Евросоюза по изучению опыта криминализации несанкционированного доступа позволяет сделать следующие выводы.

Несанкционированный доступ в том или ином виде, в зависимости от формы выражения, законодательно закреплен во многих изученных нами УК. В первую очередь следует отметить, что европейские законодатели по-разному именуют рассматриваемое преступление – несанкционированный доступ, противозаконный доступ, самовольный доступ, что, впрочем, не меняет их сути.

Позиции европейских законодателей в отношении криминализации несанкционированного доступа, полагаем, можно представить в виде трех групп. К первой группе отнесем позицию законодателей Австрийской Республики, Королевства Бельгии, Королевства Дании, Французской Республики, Латвийской Республики, которые закрепили в УК самостоятельный состав несанкционированного доступа. Ко второй группе отнесем позицию создателей УК Королевства Испании и Королевства Швеции, в которых несанкционированный доступ выступает в качестве способа совершения других преступлений. В третью группу, полагаем, следует отнести УК Республики Польши, Королевства Нидерландов, Федеративной Республики Германии, где законодатели закрепили несанкционированный доступ не только в качестве самостоятельного состава, но и предусмотрели его в качестве способа совершения других преступлений.

Представляет интерес анализ объективных и субъективных признаков состава несанкционированного доступа.

Исходя из расположения несанкционированного доступа в УК зарубежных государств, можно сделать вывод, что законодатели поразному подходят к определению родового объекта этого преступления. В большинстве из изученных нами УК таковыми выступают общественная безопасность и общественный порядок (Нидерланды, Латвия), неприкосновенность системы автоматизированной обработки информации (Бельгия, Франция), частная сфера и профессиональная тайна – Австрия, ФРГ и др. Таким образом, в зарубежном уголовном законодательстве объектом несанкционированного доступа выступают различные группы общественных отношений, отсутствует единый законодательный подход к его определению.

Говоря об особенностях, характеризующих объективную сторону несанкционированного доступа, можно отметить следующее. Во-первых, формулировка состава преступления в УК зарубежных государств позволяет говорить о двух вариантах – о доступе к компьютерной информации (Польша, Дания), данным (Австрия) или сведениям (ФРГ) и о доступе в систему обработки информации (компьютерное устройство, информационную систему) в УК Бельгии, Австрии, Нидерландов, Франции, Латвии. В последнем случае, что следует из текста соответствующих статей, лицо все равно преследует цель ознакомления с данными (информацией), которые в этой системе находятся.

Во-вторых, по-разному сформулированы в изученных европейских УК и обстоятельства совершения несанкционированного доступа. Так, в УК Австрии, Нидерландов, Польши обязательным признаком объективной стороны является способ – с нарушением системы (мер) защиты; в УК Дании указано, что этот доступ является незаконным, противоправным, в УК Бельгии – без разрешения. В УК ФРГ указано на особо охраняемый характер сведений, которые выступают в качестве предмета доступа. Примечательно, что в большинстве УК соответствующие статьи не содержат наименования указанного в них преступления, но в УК Австрии данное преступление называется противозаконным доступом, в УК ФРГ – разведыванием сведений.

В-третьих, в зависимости от указания в УК возможных последствий несанкционированного доступа, можно говорить о том, что в большинстве случаев основной состав данного преступления сформулирован как формальный (Бельгия, Дания, Нидерланды и др.).

Анализ субъективных признаков составов несанкционированного доступа, закрепленных в УК стран Евросоюза, показывает следующее.

По отношению к субъективной стороне можно говорить, что во всех изученных нами УК стран Европейского союза имело место указание на умышленную форму вины. Таким образом, можно говорить о практически полной унификации уголовного законодательства в этом плане. Неосторожная форма вины встречается гораздо реже, в квалифицированных составах несанкционированного доступа, причем альтернативно с умышленной формой вины (УК Бельгии).

Что же касается субъекта изучаемого преступления, то таковым в большинстве случаев является физическое, вменяемое лицо. А вот в отношении возраста привлечения к уголовной ответственности за несанкционированный доступ к компьютерной информации зарубежные законодатели не достигли единства, что связано с различными подходами в установлении возраста уголовной ответственности в целом. Так, с 15 лет предусмотрена ответственность в Швеции и Дании; с 16 лет – в Нидерландах; с 17 лет – в Польше. При этом в некоторых государствах предусмотрена возможность привлечения к ответственности и в более раннем возрасте, при условии совершения преступления умышленно. Например, в УК Нидерландов этот возраст установлен с 12 до 16 лет. Кроме того, в УК Бельгии, Франции, Дании установлена и ответственность юридических лиц. Причем, например, в УК Франции в рамках главы, посвященной посягательствам на систему автоматизированной обработки данных, не только указывается на возможность привлечения к уголовной ответственности юридических лиц, но и подробно прописан перечень наказаний, которые могут применяться к юридическим лицам за совершение указанных преступлений.

Анализируя квалифицирующие признаки несанкционированного доступа, закрепленные в УК европейских государств, можно сказать следующее. Некоторые УК, например Австрии, содержат только основной состав несанкционированного доступа, не имеющий квалифицированных видов. В то же время в других УК содержится ряд квалифицирующих признаков, среди которых чаще встречаются следующие: несанкционированный доступ с намерением совершить обманную операцию (с целью получить незаконный доход), с использованием служебного положения (превышением полномочий), причинивший определенный ущерб, повлекший изменение или уничтожение данных, с целью изъятия (копирования) данных. Среди иных квалифицирующих признаков можно указать такие, как несанкционированный доступ, совершенный повторно, организованной группой, по приказу, повлекший ухудшение функционирования компьютерной системы. Таким образом, можно сделать вывод, что и квалифицированные виды несанкционированного доступа в европейских странах весьма разнообразны.

Для полной юридической характеристики несанкционированного доступа имеет важное значение и анализ санкций в УК некоторых стран Европы, предусматривающих наказание за преступление с основным составом. В подавляющем большинстве изученных нами норм санкции являются альтернативными и относительно определенными. Следует отметить, что значительная часть УК предусматривает в санкциях за данное преступление два вида наказания, максимальное количество наказаний – три. В подавляющем большинстве в качестве одного из наказаний предусмотрен штраф, причем в УК Бельгии и Австрии указаны конкретные размеры штрафа. В качестве альтернативы штрафу чаще других предусмотрено лишение свободы (тюремное заключение). Причем в отношении названного вида наказания следует отметить следующее. В некоторых УК законодатели предусмотрели срок лишения свободы до 6 месяцев (Австрия, Нидерланды, Дания) или до 1 года (Бельгия, Франция). В других УК законодатели установили срок лишения свободы до 3 лет (ФРГ, Польша), т.е. в этих государствах общественная опасность данного преступления повышена. Среди других наказаний встречаются также арест (Латвия) и ограничение свободы (Польша).

Отдельно хотелось бы остановиться на анализе уголовной ответственности за несанкционированный доступ к компьютерной информации в Соединенном Королевстве Великобритании и Северной Ирландии, как представителя общей системы права. Следует отметить, что в Великобритании преступность деяний непосредственно в сфере компьютерной информации установлена Законом о злоупотреблении компьютерами в 1990 г. В соответствии с названным законом к уголовно наказуемым отнесены: умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам; умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях; неправомерный доступ к компьютерной информации на машинном носителе в компьютере, компьютерной системе или сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, компьютерной систе-

мы или сети [3, с. 94]. В данном случае несанкционированный доступ к компьютерной информации подвергся разделению на отдельные преступления в зависимости от целей и намерений преступника. Подобные деяния признаются малозначительными и наказываются тюремным заключением до 6 месяцев или штрафом [4, с. 50].

Подводя итог вышеизложенному, отметим, что анализ европейского уголовного законодательства показал, что многие страны в том или ином виде криминализировали несанкционированный доступ к компьютерной информации. И, хотя признаки состава этого преступления в УК разных государств описаны по-разному, смысл заключается в запрете несанкционированного доступа к компьютерной информации или компьютерному оборудованию. Указанный запрет, независимо от степени описания объективных и субъективных признаков, призван охранять безопасность использования компьютерной информации. В то же время анализ показал, что данные различия могут носить существенный характер. Не во всех европейских государствах рассматриваемое преступление в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны отношений, связанных с использованием компьютерных технологий и информации.

Поскольку несанкционированный доступ относят к международным транснациональным преступлениям, то, несомненно, для успешного противодействия этому преступлению необходимо применять единообразные законодательные подходы к установлению уголовной ответственности за него. В настоящее время можно отметить лишь некоторые схожие черты, характерные, как правило, для стран-соседей. Среди возможных путей решения этой проблемы видится выработка совместных договоренностей на международном уровне. В таком случае возможно будет говорить о перспективах сближения отечественного и европейского законодательства, выработке единых критериев криминализации несанкционированного доступа с целью дальнейшей успешной борьбы с данным и другими видами компьютерных преступлений.

Таким образом, несмотря на то что несанкционированный доступ нашел законодательное закрепление в уголовном законодательстве многих зарубежных государств, отсутствует унифицированный подход к описанию признаков состава данного преступления, что не способствует эффективному противодействию рассматриваемому преступлению. Тем не менее изучение накопленного в других странах законодательного опыта может быть использовано для выработки предложений по совершенствованию УК в части обеспечения безопасности компьютерной информации.

Список литературы

1. Chawki M. A critical look at the regulation of cybercrime // Computer Crime Research Center [Electronic resource]. Mode of access: http://www.crime-research.org/library/Critical.doc. Date of access: 05.05.2016.

2. Convention on Cybercrime, Budapest, 23.11.2001 // Council of Europe [Electronic resource]. Mode of access: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185. Date of access: 20.05.2016.

3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.

4. Уголовное право зарубежных государств. Особенная часть: Уч. пос. / Под ред. А.Д. Козочкина. М.: Камерон, 2004. 528 с.

COMPARATIVE ANALYSIS OF THE CRIMINAL LIABILITY FOR UNAUTHORIZED ACCESS TO COMPUTER INFORMATION IN THE EU COUNTRIES

N.A. Shved

To effectively combat computer-related crime, it is important to take into account foreign experience of combating computer crime, especially by criminal law means. This article provides a comparative legal analysis of the criminal legislation of a number of European Union countries in order to identify common and distinctive features of criminal liability for unauthorized access to computer information. The main approaches of European legislators to the criminalization of this type of socially dangerous act are identified. We note the inconsistency of European criminal law and the need to harmonize approaches to the criminalization of unauthorized access to computer information.

Keywords: computer crime, unauthorized access to computer information, criminal legislation, information security, computer information.

References

1. Chawki M. A critical look at the regulation of cybercrime // Computer Crime Research Center [Electronic resource]. Mode of access: http://www.crime-research.org/library/Critical.doc. Date of access: 05.05.2016.

2. Convention on Cybercrime, Budapest, 23.11.2001 // Council of Europe [Electronic resource]. Mode of access: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185. Date of access: 20.05.2016.

3. Volevodz A.G. Protivodejstvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. M.: Yurlitinform, 2002. 496 s.

4. Ugolovnoe pravo zarubezhnyh gosudarstv. Osobennaya chast': Uch. pos. / Pod red. A.D. Kozochkina. M.: Kameron, 2004. 528 s.