УДК 343.34

Уголовная ответственность за создание организованных групп, направленных на совершение компьютерных преступлений, по законодательству зарубежных стран

И.Н. Мосечкин

Вятский государственный университет, ул. Московская, 36, Киров, 610000, Россия

E-mail: Weretowelie@gmail.com

Аннотация. Статья посвящена изучению проблем уголовно-правового противодействия организованным преступным формированиям, созданным с целью совершения противоправной деятельности в сфере компьютерной информации. Автором предпринята попытка оценить уголовно-правовые нормы об ответственности за компьютерные преступления в законодательстве зарубежных стран в контексте их противодействия организованной преступности. Автор показывает, что сам факт создания организованных формирований может быть признан отдельным деликтом, как это сделано в законодательстве ряда стран англосаксонской правовой семьи.

Ключевые слова: компьютерная информация, компьютерное преступление, организованная группа, преступное сообщество, киберпреступление, общественная безопасность

Criminal liability for the creation of organized groups aimed at committing computer crimes under the laws of foreign countries

I.N. Mosechkin

Vyatka State University, Moskovskaya str., 36, Kirov, 610000, Russia

E-mail: Weretowelie@gmail.com

Abstract. The article is devoted to the study of the problems of criminal legal counteraction to organized criminal groups created for the purpose of committing illegal activities in the field of computer information. The author made an attempt to assess the criminal law norms on responsibility for computer crimes in the legislation of foreign countries in the context of their counteraction to organized crime. The author shows that the very fact of the creation of organized formations can be recognized as a separate tort, as is done in the legislation of a number of countries of the Anglo-Saxon legal family.

Keywords: computer information, computer crime, organized group, criminal community, cybercrime, public safety

ISBN 978-5-6045165-2-2

Компьютерные преступления, совершаемые организованными формированиями, приобрели устойчивую тенденцию к росту, а их общественная опасность за последние несколько лет существенно возросла. В связи с чем в научной среде возникают предположения об установлении уголовной ответственности за сам факт создания организованных групп, направленных на совершение преступлений в сфере компьютерной информации.

Для исследования проблем противодействия организованной киберпреступности полезным представляется изучение зарубежного законодательства и мнений ученых, анализирующих его. Законодательство США и Великобритании позволяет применять меры уголовной ответственности не только в случае совершения конкретного компьютерного преступления, но также за создание преступных формирований в противоправных целях. В частности, в США на федеральном уровне преимущественно применяется Закон о компьютерном мошенничестве и злоупотреблениях 1986 года (H.R.4718 - Computer Fraud and Abuse Act of 1986). В Великобритании достаточно похожие положения содержатся в Законе о неправомерном использовании компьютеров 1990 года (Computer Misuse Act 1990). Как отмечается учеными, вероятность потенциальной уголовной ответственности в США выше, поскольку самостоятельными преступлениями признаются подстрекательство и сговор в совершении компьютерных преступлений. Вместе с тем, судебная практика Великобритании показывает, что к уголовной ответственности также могут быть привлечены лица за сговор и дачу советов в совершении киберпреступлений [1, С. 135-136].

Уголовное законодательство Австралии признает сговор в совершении преступления отдельным наказуемым актом. Вместе с тем ст. 478.4 Уголовного закона Австралии (Criminal Code Act 1995) от 1995 года устанавливает ответственность за различные формы пособничества и иного содействия в совершении компьютерных преступлений.

В Ямайке действует Закон о компьютерных преступлениях 2015 года, содержащий перечень деликтов и наказания за их совершение. Исследователи отмечают, что раздел 12 данного нормативного акта признает наказуемым любую разновидность соучастия в совершении компьютерного преступления [2, С. 85].

В зарубежной литературе указывается, что объединение в разные формы соучастия для совершения компьютерного преступление признается отдельным

ISBN 978-5-6045165-2-2

преступлением в странах Южной Африки, где действует Закон об электронных коммуникациях и сделках (ECT act) [3].

Таким образом, в ряде стран, принадлежащих к англосаксонской правовой семье, сложились такие меры противодействия, при которых объединение в преступные группы признается отдельным деликтом, независимо от степени реализации целей группы.

Для соблюдения объективности исследования следует обратить внимание на анализ законодательства стран, принадлежащих к романо-германской правовой семье.

Исследователи законодательства Венгрии отмечают, что ни старый, ни новый уголовный закон не содержат норм, предусматривающих ответственность за создание хакерских сообществ. Вместе с тем, подчеркивается, что такие изменения необходимы, поскольку существует правовой пробел [4, С. 173-174].

В законодательстве Финляндии совершение компьютерных преступлений в соучастии признается квалифицирующим признаком. Сам факт объединения для совершения таких правонарушений может указывать только на неоконченный характер преступлений [5, С. 94-97].

В законодательстве Эстонии присутствует ответственность за подготовку компьютерного преступления, что считается отдельным деликтом, предусмотренным ст. 216.1 Пенитенциарного кодекса [6, С. 246].

Вместе с тем анализ законодательства ряда стран показал отсутствие составов преступлений, включающих только лишь факт создания организации в целях совершения компьютерных преступлений. Чаще всего совершение деяний в соучастии закрепляется в качестве отягчающего признака. В числе таких стран Федеративная Республика Германия, Нидерланды, Французская Республика, Китайская Народная Республика и другие.

Таким образом, следует отметить, что в законодательстве ряда стран содержатся положения, позволяющие привлекать к уголовной ответственности за любое объединение с целью совершить компьютерное преступление как за оконченное деяние. Большинство таких стран относится к правовой семье «общего права». В странах континентальной правовой семьи законодательство включает разные формы соучастия в качестве квалифицирующих признаков.

Список литературы

ISBN 978-5-6045165-2-2

1. Karagiannopoulos, V. Contemporary Norms and Law and Hacktivism / V. Karagiannopoulos // Living With Hacktivism. Palgrave Macmillan, Cham. – 2018. – С. 91-142.
2. Barclay, C. Cybercrime and Legislation: A Critical Reflection on the Cybercrimes Act, 2015 of Jamaica / C. Barclay // Commonwealth Law Bulletin. – 2017. – 43(1). – С. 77-107.
3. Schultz, C. Cybercrime: An Analysis of Current Legislation in South Africa: LLM diss. abstract / Schultz Charlotte Beverly. – Hatfield, 2016. – 48 с.
4. Béla, S. Hacktivism and Its Status in Hungary / S. Bela // Magyar Rendésze. – 2016. – 16(2). – С. 161-174.
5. Calcara, G. Cybercrime, law and technology in Finland and beyond / G. Calcara, P. Sund, M. Tolvanen. – Tampere, Police University College of Finland Publ., 2019. – 160 с.
6. Пелевина, А.В. Ответственность за преступления в сфере компьютерной информации в странах Балтии / А.В. Пелевина // Татищевские чтения: актуальные проблемы науки и практики. Материалы XIV Международной научно-практической конференции. В 4-х томах. Тольятти: Волжский университет имени В.Н. Татищева (институт). – 2017. – С. 245-248.

ISBN 978-5-6045165-2-2