Научная статья
УДК 34
https://doi.org/10.24412/2073-0454-2023-7-144-148
EDN: https://elibrary.ru/zsgjgo
NIION: 2003-0059-7/23-911
MOSURED: 77/27-003-2023-07-110

Актуальные вопросы борьбы с киберпреступностью

Ерлан Думанович Намысов
Карагандинская академия МВД Республики Казахстан имени Б. Бейсенова, Караганда, Россия, ynamysov@inbox.ru

Аннотация. Рассматривается международный и зарубежный опыт противодействия интернет-мошенничеству. Описываются правовые механизмы противодействия данному виду противоправных посягательств. Изучаются проблемные стороны с целью выработки путей совершенствования исследуемого механизма.

Ключевые слова: интернет-мошенничества, противодействие, международный и зарубежный опыт, правоохранительная деятельность, меры безопасности

Для цитирования: Намысов Е. Д. Актуальные вопросы борьбы с киберпреступностью // Вестник Московского университета МВД России. 2023. № 7. С. 144–148. https://doi.org/10.24412/2073-0454-2023-7-144-148. EDN: ZSGJGO.

Original article

Topical issues of combating cybercrime

Erlan D. Namysov
Karaganda Academy of the Ministry of Internal Affairs of Republic of Kazakhstan named after B. Beisenov, Karaganda, Russia, ynamysov@inbox.ru

Abstract. The international and foreign experience of countering Internet fraud is considered. The legal mechanisms for countering this type of illegal encroachments are described. The problematic sides are being studied in order to develop ways to improve the mechanism under study.

Keywords: internet fraud, counteraction, international and foreign experience, law enforcement, security measures

For citation: Namysov E. D. Topical issues of combating cybercrime. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(7):144–148. (In Russ.). https://doi.org/10.24412/2073-0454-2023-7-144-148. EDN: ZSGJGO.

Проблематика интернет-мошенничества представляет собой относительно молодое, но высокоактуальное направление в рамках криминологической практики. В ходе научного анализа обнаруживается, что даже в странах, находящихся на передовом рубеже технологического прогресса, формирование соответствующих нормативных и правовых подходов к интернет-мошенничеству началось лишь в период с 70-х по 80-е гг. XX в. Это связано с эмпирическим восприятием нового явления и неотложной потребностью в создании адекватных механизмов реагирования на вновь возникающие киберпреступления.

В указанный период отдельные страны уже проявляли определенные попытки внедрения административно-правовых и уголовно-правовых мер ответственности за действия, содержащие признаки интернет-мошенничества. Тем не менее, подобные меры имели дискретный характер и представляли собой реакцию на изменяющиеся криминальные сценарии, связанные с развитием информационных технологий.

Исследование этого периода является ключевым для понимания эволюции правового реагирования на интернет-преступности. Анализ существующих подходов и их прогрессивное развитие способствуют построению эффективных стратегий противодействия, а также формированию нормативных оснований для борьбы с современными проявлениями киберугроз. В данном контексте важно выявить не только изменения в сфере технологий, но и трансформации в правовых концепциях, направленных на предотвращение и реагирование на интернет-мошенничество.

При этом достаточно быстро интернет-преступность, в том числе, различные формы хищений и

причинения имущественного ущерба, стали все больше приобретать трансграничный характер, что требовало, в том числе, и гармонизации национальных законодательств. Это привело к выработке на уровне ряда европейских стран первоначальных рекомендаций относительно перечня и признаков деяний, которые следует относить к группе компьютерных преступлений [1]. Данный период характеризуется интенсивным приложением усилий в вопросах поиска объединяющих факторов (понятий, параметров ответственности и т. д.), которые позволили бы эффективно реализовывать ответственность за киберпреступления. При этом первыми совместными рекомендациями европейских государств были сформулированы фактически два перечня (списка) деяний, которые должны быть криминализованы в национальных юрисдикциях.

В рамках первого списка формулировался «минимальный» набор криминальных деяний, которые запрещались (должны запрещаться) на территории ЕС:

♦ компьютерное мошенничество;

♦ повреждение компьютерной информации и компьютерных программ;

♦ компьютерных подлог;

♦ компьютерный саботаж;

♦ несанкционированный перехват информации в компьютерной сети;

♦ несанкционированный доступ к компьютерной сети;

♦ запрещенное копирование компьютерной информации или программ.

В данном аспекте примечательно, что интернет-мошенничество (в точной формулировке — «компьютерное мошенничество») стало фактически ключевым в списке деяний, сопряженных с киберугрозами [2].

В рамках второго перечня, которому придавалось факультативное значение, на усмотрение национальных юрисдикций относилась криминализация таких деяний, как:

♦ компьютерный шпионаж;

♦ те или иные формы незаконного использования компьютера (в рамках совершения отдельных видов преступлений);

♦ изменение информации, компьютерных программ;

♦ несанкционированное применение защищенных компьютерных программ.

Следует в данном случае отметить, что понятие «компьютерное мошенничество», которому придавалось приоритетное значение в рамках первых рекомендательных документов, не тождественно в полной мере понятию интернет-мошенничества. Последнее мы рассматриваем как разновидность «традиционного» мошенничества, когда конститутивный способ обмана или злоупотребления доверием реализовывается мошенником в информационной системе (сети, ресурсе и т. д.). Под компьютерным мошенничеством изначально понимался более широкий спектр деяний, которые связаны с причинением имущественного ущерба: здесь в гораздо более типичной форме выступают действия злоумышленника, который посредством тех или иных манипуляций в сети причиняет вред собственнику имущества. Фактически в большей степени принимаются во внимание признаки тайного хищения, а не мошенничества. В таком виде криминализация встречается гораздо чаще, нежели обособленное оформление именно интернет-мошенничества. Действующее уголовное законодательство всех стран ближнего зарубежья (будет проанализировано далее) к настоящему времени содержит более или менее подробные перечни преступлений, которые совершаются в киберпространстве, причем, чаще всего они сконструированы в рамках самостоятельных глав уголовных законов.

Разд. IX Резолюции Генеральной Ассамблеи ООН от 31 января 2002 г. № 56/261 «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» получил наименование «Меры по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров» [3]. В качестве национальных мер указанной Резолюцией отмечались, в частности, следующие:

1) криминализация различных форм неправомерного использования информационных технологий. При этом особо отмечалась необходимость пересмотра составов таких преступлений, как мошенничество (т. е. тяготеющих именно к использованию ресурсов информационных ресурсов);

2) необходимость выработки механизмов для реализации уголовной ответственности в случаях, когда совершение преступления имеет отношения к различным национальным юрисдикциям;

3) рекомендация по обучению и оснащению сотрудников правоохранительных органов в вопросах

выявления и расследования преступлений, связанных с использованием компьютеров и др.

В качестве международных мер предусматривались мероприятия Центра по международному предупреждению преступности, на который возлагались функции по:

♦ поддержке исследовательской деятельности в данном направлении;

♦ разработке рекомендаций, руководств, принципов, типовых законов;

♦ оказанию помощи государствам, нуждающимся в технической и иной помощи и др.

Большинство национальных юрисдикций к настоящему времени демонстрируют как практику взаимодействия с транснациональными структурами (Интерпол, Европол), так и создание национальных специальных правоохранительных служб, деятельность которых непосредственно связана с расследованием преступлений, сопряженных с использованием информационных систем и технологий: Национальное подразделение по борьбе с киберпреступностью (Соединенное Королевство); Агентство национальной безопасности (США); Австралийский центр преступности в сфере высоких технологий при Федеральной полиции Австралии; Подразделение по борьбе с киберпреступностью (Греция); Группа по расследованию киберпреступлений (Индия, Мумбаи); Департамент киберполиции (Япония) и др. [4].

Специальные подразделения создавались и в виде трансграничных организаций, на которые возлагались соответствующие правоохранные функции в вопросах обеспечения кибербезопасности. Так, Европейский союз организовал сеть правоохранительных органов «Европейский центр киберпреступлений» (European cybercrimecentre или «ЕС-3»), который включил десять самостоятельных подразделений, на которые было возложено осуществление анализа статданных, разработка специальных способов выявления и поимки киберпреступников, а также их непосредственная поимка и привлечение к ответственности [5].

По пути специализации правоохранительной деятельности в рамках противодействия преступности в сфере «высоких технологий» пошел и Казахстан, где созданы так называемые отделы «К» при департаментах полиции. В сферу их деятельности включены исключительно составы преступлений в сфере информатизации и связи, а также деяния, связанные с использованием сети Интернет при совершении отдельных преступлений (например, при распространении порнографических материалов с изображением несовершеннолетних), а также интернет-мошенничество.

Анализ первых и последующих международных документов, касающихся вопросов противодействия преступности в сфере «высоких технологий», свидетельствует о том, что основной акцент изначально устанавливался на мерах обеспечительного, организационного характера, которые должны привести к консолидации усилий правоохранительных структур различных государств.

При этом, несмотря на наличие рекомендаций относительно необходимости криминализации соответствующих признаков в контексте традиционного состава мошенничества, авторы недавних исследований совершенно справедливо отмечают, что соответствующие уголовно-правовые нормы в большинстве стран «характеризуются весьма общим определением компьютерного мошенничества — как действия, совершаемого с компьютерной информацией с корыстной целью, причинившего вред собственнику или иному владельцу имущества» [6].

В плане общей оценки следует отметить, что большинство вариантов регламентации ответственности за интернет-мошенничество не связывают ее с фактом именно незаконного воздействия на информационный ресурс (в случае его установления возможна квалификация по совокупности преступлений против собственности и информационной безопасности). В рамках наиболее строгих подходов (например, в уголовном законодательстве Новой Зеландии) имеются варианты формулировки уголовно-правовых норм по превентивному принципу.

Так, в соответствии со ст. 250 «Повреждение или вмешательство в компьютерную систему» Закона Новой Зеландии «О преступлениях» 1961 г. (размещена в главе о преступлениях против права собственности) предусматривается наказание от семи до десяти лет уже за сам факт совершения виновным лицом действий в целях завладения имуществом (т. е. даже до момента появления реальной возможности им распорядиться).

Учитывая то обстоятельство, что первоначально с угрозами киберпреступности столкнулись наиболее развитые в технологическом отношении страны, они закономерно стали лидерами в вопросах выра-

ботки первоочередных стратегий борьбы с данными видами преступлений. Так, в июне 1996 г. в городе Лион состоялся саммит «G-8», по итогам которого был выработан Регламент № 16, непосредственно посвященный вопросам криминализации и наказуемости деяний, которые совершаются с помощью использования информационных технологий. Именно в рамках его решений образовалась так называемая «Лионская группа», ставшая одним из лидеров в вопросах противодействия киберпреступности.

До настоящего времени основным международным документом, который выработан в рамках противодействия киберпреступлениям, является Конвенция ЕС «О киберпреступности» от 23 ноября 2001 г. (так называемая Будапештская конвенция) [7]. Учитывая то обстоятельство, что ко времени ее разработки и принятия уровень киберпреступности в мире приобрел уже деструктивные масштабы, а ущерб от соответствующих преступлений стал составлять критические объемы ВВП многих стран, положения данной Конвенции отличаются высокой строгостью, вплоть до возможности правоохранительных органов одной страны вмешиваться в информационные ресурсы другой страны и принимать необходимые решения, независимо от согласия соответствующей юрисдикции.

В соответствии с указанной Конвенцией, выделены пять основных групп киберпреступлений, которые должны иметь четкую форму криминализации в национальных законодательствах.

Во-первых, это преступления, посягающие на конфиденциальность, целостность и доступность компьютерных данных и систем (вмешательство, перехват, незаконный доступ в систему).

Во-вторых, отдельно были выделены преступления, в механизме которых манипуляция с информационными ресурсами выступала в качестве способа совершения преступлений (в том числе, «компьютерное мошенничество», различные формы искажения информации, подлога, фальсификации и т. д.).

В-третьих, особо отмечались преступления, в которых имеет место недопустимый контент, распространяемый в информационных сетях (в частности, порнографические материалы с изображением детей).

В-четвертых, были особо отмечены в качестве самостоятельной группы криминальные посягательства, совершаемые с использованием информационных систем и сопряженные с демонстрацией, призывами к расизму, ксенофобии и другим подобным явлениям.

В-пятых, выделялась также группа преступлений, которые были связаны с нарушением авторского и смежных с ним прав в рамках информационных систем.

К настоящему времени вопросы выработки универсального документа (на уровне ООН), касающегося вопросов противодействия киберпреступлениям, в том числе, и интернет-мошенничествам, еще не получили окончательного решения.

При этом еще в 2010 г. в Бразилии прошел 12-й Конгресс ООН, на котором активно обсуждались вопросы борьбы с компьютерными преступлениями, обеспечением безопасности государств мирового сообщества от киберугроз. На указанном конгрессе уже отмечалось, что назрела необходимость в выработке глобального документа, который был бы направлен на противодействие киберпреступности во всех странах мирового сообщества [8].

Причем, здесь следует учитывать, что различный уровень технологического развития стран приводит к заметному дисбалансу и в уровне защиты от угрозы преступных посягательств, связанных с использованием возможностей информационных систем. Кроме того, понятие «киберпреступление» неизбежно подверглось трансформации, поскольку степень внедрения в жизнь современного человека информационных технологий к настоящему времени резко возросла в сравнении с той, которая имела место на момент первоначальной актуализации вопроса. В настоящее время многие факты интернет-мошенничества, в целом, уже не могут быть отнесены к понятию киберпреступности. В качестве более верного определения уже будет их отнесение к преступлениям, совершаемым с применением информационных технологий (систем, сетей, устройств и т. д.).

В завершение настоящего исследования, посвященного эволюции правового реагирования на интернет-мошенничества необходимо подчеркнуть важность проанализированных событий и их влияние на современную криминологическую практику. Проведенный анализ позволяет сделать ряд важных выводов относительно динамики формирования правовых механизмов в ответ на новые вызовы, связанные с развитием информационных технологий.

Список источников

1. Recommendation № R (95) 13 of the Committee of Ministers of the Council of Europe to member States for the 11 concerning problems of criminal procedural law connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543 rd meeting of the Ministers' Deputies). Strasbourg, 1995.

2. Побегайло А. Э. Борьба с киберпреступностью: учеб. пособие. М. : Университет прокуратуры Российской Федерации, 2018.

3. Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века: принята в г. Нью-Йорке на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН: Резолюция Генеральной Ассамблеи ООН от 31 января 2002 г. № 56/261 // URL://https://e-ecolog.ru/docs/SO_2cfcPHUefe7PjGX64j?utm_referrer=https%3 A%2F%2Fyandex.kz%2F.

4. Сабадаш В. П. Специальные подразделения и организации по борьбе с интернет-мошенничеством в различных государствах мира // Библиотека криминалиста. 2013. № 5 (10). С. 328–338.

5. Киселев А. К. Киберпреступность — взгляд из Европы // Библиотека криминалиста. 2013. № 5 (10). С. 309–313.

6. Фролов Ф. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: автореф. дисс. … канд. юрид. наук. М., 2019.

7. Конвенция Европейского Союза «О киберпреступности»: принята в Будапеште 23 ноября 2001 г. // URL://https://online.zakon.kz/Document/?doc_id=30170556.

8. Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией // URL:// http://www.crimeresearch.ru/articles/Dubko_0001.

References

1. Recommendation № R (95) 13 of the Committee of Ministers of the Council of Europe to member States for the 11 concerning problems of criminal procedural law connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543 rd meeting of the Ministers' Deputies). Strasbourg, 1995.

2. Pobegailo A. E. Combating Cybercrime: textbook. M. : University of the Prosecutor's Office of the Russian Federation, 2018.

3. Plans of Action for the Implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century: adopted in New York City at the 93rd plenary meeting of the 56th session of the UN General Assembly: UN General Assembly Resolution No. 56/261 of January 31, 2002 // URL:// https://e-ecolog.ru/docs/SO_2cfcPHUefe7PjGX64j?utm_referrer=https%3A%2F%2Fyandex.kz%2F.

4. Sabadash V. P. Special units and organizations to combat Internet fraud in different states of the world // Library of criminalist. 2013. № 5 (10). P. 328–338.

5. Kiselev A. K. Cybercrime — a view from Europe // Library of criminalist. 2013. № 5 (10). P. 309–313.

6. Frolov F. D. Criminal-legal and criminological counteraction to fraud in the sphere of computer information: autoref. diss. … kand. jurid. nauk. M., 2019.

7. European Union Convention on Cybercrime: adopted in Budapest on November 23, 2001 // URL:// https://online.zakon.kz/Document /?doc_id=30170556.

8. Dubko M. International cooperation in the sphere of criminal-legal fight against illegal acquisition of computer information // URL://http://www.crimeresearch.ru/articles/Dubko_0001.

Информация об авторе

Е. Д. Намысов — заместитель начальника Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова.

Information about the author

E. D. Namysov — Deputy Head of the Karaganda Academy of the Ministry of Internal Affairs of Republic of Kazakhstan named after B. Beisenov.

Статья поступила в редакцию 13.11.2023; одобрена после рецензирования 01.12.2023; принята к публикации 18.12.2023.

The article was submitted 13.11.2023; approved after reviewing 01.12.2023; accepted for publication 18.12.2023.