УДК 343.3/.7

© Гульнара Шарафиева
адъюнкт
Казанского юридического института МВД России

© Gulnara Sharafieva
Postgraduate of the Kazan Law Institute of MIA of Russia

КЛАССИФИКАЦИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Автором анализируются различные подходы к пониманию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Сделан вывод о необходимости международного сотрудничества путем формулирования единых критериев и подходов к определению преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Общепринятого определения преступлений, совершаемых с использованием информационных технологий, нет. Ученые и практики оперируют понятиями «киберпреступления», «преступления в сфере цифровой информации», «компьютерные преступления», в государственных структурах чаще используют понятия «преступления, совершенные в сфере информационно-телекоммуникационных технологий или высоких технологий».

При этом существуют и разные определения рассматриваемых преступлений как социально-правового явления: «цифровая преступность», «информационно-цифровая преступность», «интернет-преступность», «киберпреступность» и др.

Анализ норм международного права позволяет сделать вывод об отсутствии последовательности в определении данного вида деяний и в мировом сообществе, несмотря на то что рассматриваемые преступления имеют трансграничный характер и могут совершаться из любой точки мира.

Впервые на проблему совершения преступлений с использованием компьютеров обратили внимание в конце XX века. С тех пор Организация Объединенных Наций активно занимается рассмотрением различных

аспектов преступлений, связанных с использованием компьютеров. В большинстве международных актов используется термин «компьютерное преступление», под которым понимается любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры, компьютерные сети, а также цифровые технологии [1, с. 21]. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) выделила следующие подразделы: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием данных; правонарушения, связанные с нарушением авторского права и смежных прав [2]. Представляется, что типология не является полностью последовательной, поскольку она не основана на единых критериях.

Необходимо отметить, что при официальном переводе текста документа Правовым управлением Государственной думы Федерального собрания Российской Федерации используемое в названии понятие cybercrime было переведено как «преступность в сфере компьютерной информации». При этом можно также увидеть и другие переводы названия: Конвенция о киберпреступлениях или киберпреступности, Конвенция о компьютерных преступлениях. Однако речь будет идти об одной и той же Конвенции.

Во время 10-го Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями в рамках соответствующего семинара были разработаны два определения: киберпреступность в узком смысле, которая охватывает любое незаконное поведение, объектом которого является обеспечение безопасности компьютерных систем и обрабатываемых ими данных; киберпреступность в более широком смысле, охватывающая любое незаконное поведение, совершаемое с помощью компьютерной системы или сети или в связи с ними, включая такие преступления, как незаконное владение информацией, распространение информации с помощью компьютерной системы или сети.

В рамках Содружества Независимых Государств действует Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации». Соглашение заключено в 2001 г. между 10 государствами Содружества Независимых Государств, в числе участников Российская Федерация и Республика Беларусь [3].

В данном документе содержится определение преступления в сфере компьютерной информации, под которым понимается уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация. Под компьютерной информацией понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию электронных вычислительных машин, или передающаяся по каналам связи. Таким образом, при сравнении определений видно, что оно ближе по содержанию к узкому подходу определения киберпреступлений.

В современном понимании понятия «компьютерные преступления» и «киберпреступления» не признаются тождественными. Когда речь идет о компьютерных преступлениях, чаще всего имеют в виду преступления, включенные в главу 21 Уголовного кодекса (далее — УК) Российской Федерации «Преступления в сфере компьютерной информации» [4]. Тогда как определение понятия «киберпреступления» в науке не имеет однозначного подхода. Под ними предлагают понимать преступления в сфере компьютерной информации и преступления, совершенные с использованием информационно-телекоммуникационных технологий [5], либо любое преступление, совершенное с помощью информационных технологий либо в информационном пространстве [6].

Переходя к классификации, приходим к выводу, что более широкой формулировкой обладает понятие «преступления, совершаемые с использованием информационно-телекоммуникационных технологий», куда можно включить и компьютерные преступления. Поэтому при рассмотрении классификации будем опираться на данное понятие.

С. И. Буз классифицировала рассматриваемые преступления на два основных типа: компьютерные преступления и преступления, совершаемые в киберпространстве. Разграничение осуществлялось по месту совершения преступления и предмету посягательства. К компьютерным преступлениям она отнесла преступления, направленные на получение неправомерного доступа к информации (в целях завладения, изменения или уничтожения), находящейся в памяти конкретного персонального компьютера, либо на неправомерное подключение к компьютерной сети в тех же целях. К преступлениям, совершаемым в киберпространстве, она отнесла традиционные преступления, совершенные с помощью специфических орудий (например, мошенничество в сфере интернет-продаж и покупок). При этом предметом первой группы преступлений названа компьютерная информация, а предметом второй группы — практически любые предметы: денежные средства, информация, оружие, наркотические средства и т. д. [6].

Е. А. Русскевич выделил следующие виды преступлений, совершаемых с использованием информационно-коммуникационных технологий:

1) компьютерные преступления — преступления, включенные в главу 28 УК Российской Федерации, посягающие на установленный порядок хранения, обработки или передачи компьютерной информации либо эксплуатации информационно-коммуникационных сетей и оконечного оборудования;

2) компьютеризированные преступления — общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой (ч. 3 ст. 141, п. «г» ч. 3 ст. 158, ст. 159.3, 159.6, 187 УК Российской Федерации), которые, в свою очередь, подразделяются на две подгруппы:

– простые — общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий является значимо распространенным (в отдельных случаях — единственно возможным) способом осуществления общественно опасного деяния (ст. 137, 138, 138.1, 146, 171.2, 185.3, 282, 354.1 УК Российской Федерации);

– квалифицированные — общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий является не только распространенным, но и отягчающим способом осуществления общественно опасного деяния (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, п. «в» ч. 2 ст. 151.2, ст. 205.2, п. «б» ч. 2 ст. 228.1 УК Российской Федерации и др.) [7, л. 72].

Объединяет вышеприведенные примеры классификаций то, что они разделяют те преступления, которые могут совершаться только в компьютерной среде, и те традиционные составы преступлений, которые с развитием информационных технологий трансформируются и приобретают признаки компьютеризированности.

Интересную классификацию приводит А. А. Рудых, которая опирается на функции информационных технологий в механизме преступления. Согласно данному подходу, в группу преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, включены две подгруппы: преступления, совершенные с использованием информационных технологий; преступления против информационной безопасности.

В первую подгруппу входят: 1) преступления, в способе совершения которых используются информационные технологии и цифровая информация, которые не подвергаются несанкционированному воздействию (преступления, в которых информационные технологии используются как коммуникативно-координационное средство общения между субъектом преступления и иными лицами; 2) преступления, в которых используется операционная функция информационных технологий, в том числе как орудие и средство совершения преступления; 3) преступления, в которых используется функция информационных технологий, — различные виды преступных деяний, в механизме которых информационные технологии служат элементом сокрытия.

Во вторую группу предлагается включать деяния, в способе совершения которых присутствуют процессы несанкционированных информационных преобразований цифровой информации или если этим способом создается угроза информационной безопасности (преступления против информационной безопасности): 1) преступления против безопасности цифровой информации; 2) преступления в сфере незаконного оборота цифровой информации; 3) преступления в сфере незаконного оборота программных и технических средств, используемых против информационной безопасности [8, с. 11].

С учетом того, что преступления, совершенные с использованием информационно-телекоммуникационных технологий, в последние годы возглавляют «мировой криминальный рейтинг», необходимо стремиться решать проблему путем унификации права на международном уровне. Исходной позицией по данному вопросу должен являться тезис о том, что для преступлений данного вида государственных границ в принципе не существует. Необходимо выработать единый подход к определению понятийного аппарата рассматриваемой совокупности общественно опасных деяний и предъявляемых к ним критериев. Это также позволит увидеть реальную картину киберпреступности, ее структуры, динамики, уровня и тенденций развития в мировом масштабе. Указанные рекомендации позволят облегчить преследование лиц, совершающих преступления с использованием информационно-телекоммуникационных технологий на межгосударственном уровне.

Список основных источников

1. Ищук, Я. Г. Цифровая криминология : учеб. пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. — М. : Акад. упр. МВД России, 2021. — 244 с.

2. Конвенция о преступности в сфере компьютерной информации ETS № 185 [Электронный ресурс] : [заключена в г. Будапеште 23.11.2001 г.] : с изм. от 28.01.2003 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.

3. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации [Электронный ресурс] : [заключено в г. Минске 01.06.2001 г.] // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.

4. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. Федер. закона от 29.12.2022 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.

5. Кириленко, В. П. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы [Электронный ресурс] / В. П. Кириленко, Г. В. Алексеев // Всерос. криминол. журн. — 2020. — № 6. — С. 898–913. — Режим доступа: https://cyberleninka.ru/article/n/garmonizatsiya-rossiyskogo-ugolovnogo-zakonodatelstva-o-protivodeystvii-kiberprestupnosti-s-pravovymi-standartami-soveta-evropy. — Дата доступа: 12.02.2023.

6. Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика [Электронный ресурс] / С. И. Буз // Юристъ-Правоведъ. — 2019. — № 4 (91). — С. 78–82. — Режим доступа: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika/. — Дата доступа: 12.02.2023.

7. Русскевич, Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук : 12.00.08 / Е. А. Русскевич. — М., 2020. — 521 л.

8. Рудых, А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : автореф. дис. … канд. юрид. наук : 12.00.12 / А. А. Рудых ; Ростов. юрид. ин-т М-ва внутр. дел Рос. Федерации. — Ростов н/Д, 2020. — 24 с.

CLASSIFICATION OF CYBERCRIME

Cybercrime are at the top of the «world criminal ranking», it is necessary to strive to solve the problem by unifying law at the international level. The starting position on this issue should be the thesis that there are no state borders for crimes of this type in principle. It is necessary to develop a unified approach to the definition of the conceptual apparatus of the considered set of socially dangerous acts and the criteria presented. It will also allow you to see the real picture of cybercrime, its structure, dynamics, level and development trends. The study and subsequent implementation of the elements of crimes in the field of information and telecommunication technologies proposed in international acts into national legislation will facilitate the prosecution of persons committing cybercrimes at the interstate level.