УДК 343

Китайкина Оксана Олеговна, *магистрант 2 курса юридического факультета ФГБОУ ВО «МГУ им. Н. П. Огарева», г. Саранск*

О СООТНОШЕНИИ ПОНЯТИЙ «КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ» И «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Аннотация: В статье проводится анализ конструкций «компьютерные преступления» и «преступления в сфере компьютерной информации», исследуются широкая и узкая трактовки компьютерных преступлений. Автор исследует как уголовно-правовой, так и криминологический подходы к решению проблеме, мнения экспертов-программистов. Дана классификация компьютерных преступлений. Раскрыты особенности преступлений в сфере компьютерной информации по российскому законодательству.

Ключевые слова: компьютерные преступления, преступления в сфере компьютерной информации, информационные преступления, компьютерная преступность, информационная безопасность, компьютерная информация.

Abstract: In the article the analysis of structures «computer crimes» and «crimes in the sphere of computer information», explores the broad and narrow conceptions of computer crimes. The author examines both criminal law and criminological approaches to solving the problem, the opinions of expert programmers. Classification of computer crimes is given. The features of crimes in the sphere of computer information under the Russian legislation are revealed.

Keywords: computer crimes, crimes in the sphere of computer information, computer crime, computer crime, information security, computer information.

О важном значении информации и обмена ею в современном мире не говорит только ленивый. Само общество все чаще называется информационным. Важнейшее место в таком обществе принадлежит компьютерным системам, которые обеспечивают эффективную работу с информацией как на этапе ее создания и обработки, так и ходе последующих ее хранения, накопления и передачи. И если изначально компьютер задумывался как машина, при помощи которой проводятся математические вычисления, то в настоящее время трудно назвать сферу, где бы он не использовался.

В тоже время даже при такой высокой значимости компьютерной техники следует признать, что она не является абсолютно надежной. Компьютеры, как и

любая техника, могут давать сбои в работе. Причиной сбоев могут быть и противоправные действия людей, в том числе преступного характера. Последствия таких преступлений крайне опасны по своим масштабам, начиная с миллиардных убытков различных (как частных, так и государственных) организаций в финансовой сфере вплоть до угроз человеческим жизням и управленческим системам, все активнее использующим сегодня бесконтактные способы передачи информации. В масштабе государства при этом важно обеспечить безопасность военных объектов, предприятий, выполняющих функции жизнеобеспечения населения, объектов энергетики, транспорта и пр. Компьютерные атаки на их информационную инфраструктуру могут быть катастрофическими. Так в литературе приводится пример, когда в результате вирусной атаки прекратила работу защитная система Ингалинской АЭС в Литве (1992), что чуть было не закончилось катастрофой, равной по последствиям аварии на Чернобыльской АЭС [6, с. 14].

Обеспечение информационной безопасности по этой причине сегодня становится одной из ключевых задач государственно-управленческой деятельности.

Достаточно часто при характеристике преступлений в сфере компьютерной информации используется понятие «компьютерные преступления». Как соотносятся названные конструкции?

В уголовно-правовой практике зарубежных государств (Франция, США, Великобритания) к компьютерным преступлениям нередко относятся такие, при совершении которых компьютер является как предметом, средством или орудием посягательства, так и его объектом. Например, по законодательству США и кража компьютера, и распространение порнографических материалов с изображением несовершеннолетних через компьютерные сети будут считаться компьютерными преступлениями [9, с. 59-62].

В нашей стране и в большинстве государств на постсоветском пространстве (Польша, Болгария и др.) предметом или орудием преступления признается в таких случаях только компьютерная информация, а не компьютер

как объект материального мира, а потому в упомянутых ситуациях квалификация преступлений по отечественному уголовному законодательству будет совершенно иная (кража компьютера будет относиться к разряду преступлений против собственности, а распространение порноматериалов с изображением несовершеннолетних – к преступлениям против общественной нравственности).

По сути можно вести речь о двух основных тенденциях: широкая и узкая трактовки компьютерного преступления [4, с. 20].

Из совокупности компьютерных преступлений складывается понятие компьютерной преступности. Впервые его начали использовать в США приблизительно в 70-е годы прошлого столетия [2, с. 158].

Давая характеристику компьютерными преступлениям А. И. Долгова обратила внимание на тот важный факт, что соответствующая дефиниция не имеет уголовно-правового значения, а используется, прежде всего, в широком смысле и имеет криминологическое значение [6, с. 736].

По мнению данного автора, компьютерные преступления в криминологическом смысле могут быть дифференцированы следующим образом: 1) компьютерные преступления против конституционных прав и свобод человека и гражданина (например, компьютерное пиратство, различные нарушения тайны электронных сообщений и пр.); 2) компьютерные преступления в сфере экономики (хищения, совершаемые с помощью компьютерной техники; мошенничества в системе электронных платежей с использованием электронных кредитных карт и пр.); 3) компьютерные преступления против общественной безопасности (собственно преступления в сфере компьютерной информации); 4) компьютерные преступления против государственной безопасности (неправомерный доступ к государственной тайне, осуществленный с помощью компьютера, компьютерный шпионаж, диверсия в сфере компьютерной информации и пр.).

В международном праве также предпринимались попытки классификации данных преступлений [4, с. 28].

Смежной правовой конструкцией, используемой в науке, является конструкция информационного преступления. В этом ключе заслуживает внимания классификация преступлений против информационной безопасности, зафиксированная в гл. 30 Модельного УК стран СНГ. Здесь предусмотрены шесть составов преступлений, три из которых совпадают с преступлениями гл. 28 УК РФ: несанкционированный доступ к компьютерной информации (ст. 286 – аналог ст. 272 УК РФ); разработка, использование и распространение вредоносных программ (ст. 291 – аналог ст. 273 УК РФ); нарушение правил эксплуатации компьютерной системы или сети (ст. 292 – аналог ст. 274 УК РФ). Не предусмотрены действующим УК РФ, но зафиксированы в Модельном УК СНГ: компьютерный саботаж (ст. 288); неправомерное завладение компьютерной информацией (ст. 289); изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 290)».

Можно рассматривать понятие информационного преступления как общее по отношению к понятию компьютерного преступления, но следует оговориться, что официально ни термин «информационное преступление», ни термин «компьютерное преступление» в уголовной науке не применяются.

Как дефинируется преступление в сфере компьютерной информации в российской уголовно-правовой доктрине? И существует ли его нормативное определение? Попытаемся дать ответ на этот вопрос.

В уголовно-правовой литературе приводятся различные трактовки преступлений в сфере компьютерной информации. Так, В. И. Алескеров понимает их как такие посягательства на безопасность компьютерной информации, которые причинили или создали угрозу причинения существенного вреда личности, обществу и государству в связи с использованием соответствующей информации» [1, с. 5; 5. С. 10]. Речь идет о деяниях, указанных в нормах ст. 272-274 гл. 28 раздела 9 УК РФ.

Часто во время описания преступлений данной группы применяется указание на дополнительный объект. Таким объектом является информационная безопасность [8, с. 9].

В. В. Сверчков характеризует их через общий объект [7, с. 503].

Как итог, преступления в сфере компьютерной информации относятся к компьютерным преступлениям. К ним по действующему УК РФ относятся неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных компьютерных программ (ст. 273), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274), неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1).

Компьютерная информация в них – именно предмет преступления. Напомним, что в другой группе компьютерных преступлений такая информация выступает в качестве орудия или средства их совершения. По действующему УК РФ ответственность за их совершение наступает по другим статьям УК РФ, но в необходимых случаях они могут квалифицироваться по совокупности с преступлениями, предусмотренными гл. 28 УК РФ.

Такое разграничение компьютерных преступлений предлагалось еще до принятия УК РФ 1996 г. [3, с. 11].

Специалисты-«компьютерщики», например, представители Центра глобальных исследований и анализа угроз «Лаборатории Касперского» (gReAT), структуру компьютерной преступности рассматривают немного иначе. Здесь, кстати, следует оговориться, что в их трактовке компьютерными преступлениями являются компьютерные угрозы в виде целевых кибератак (внедрение программ в компьютерные системы с целью сбора информации частного характера), кибершпионажа (незаконное получение доступа к охраняемой законом информации), хактивизма (использование компьютерной техники для продвижения своих политических и иных идей), кражи

конфиденциальных данных (хищение соответствующих данных), кибервымогательства (например, при попадании в компьютер вредоносной программы, например, типа «crypto locker», шифрующей документы пользователя компьютерной сети, после чего предлагаются услуги по восстановлению доступа к таким документам за определенное вознаграждение), кибернаемничества (совершение кибератак по найму), использования вредоносного программного обеспечения для мобильных устройств (использование вредоносных компьютерных программ для получения доступа к сервисам пользователя компьютерной сети, защищенным паролем), целевого фишинга (массовые рассылки внутри социальных сетей от имени банков, известных сервисов и пр. с целью сбора информации о логинах и паролях пользователя для последующего их неправомерного использования), нарушения тайны частной жизни, использования эксплойтов для уязвимостей программного обеспечения, создания (использование фрагментов компьютерных программ и (или) их отдельных кодов для атаки на компьютер) и использования ботнетов (использование набора программного обеспечения, включающего вирусы, брандмаузеры, программы (боты) для удаленного управления компьютером) [10].

Как видим, такая классификация компьютерных преступлений и способов их совершения в некоторой степени отличается от юридической. Это вполне справедливо, поскольку она опирается на программно-технические характеристики. Все обозначенные «компьютерные угрозы» так или иначе могут быть квалифицированы по нормам действующего УК РФ (например, по ст. ст. 138 (ч. 1), 146, 159.3, 159.6, 163, 165, 272, 273, 274, 274.1 и пр. УК РФ) как преступные деяния. Наибольший удельный вес в ряду компьютерных преступлений в целом по России приходится сегодня на преступления в сфере компьютерной информации (гл. 28 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).

Учитывая изложенное, полагаем, что в уголовном праве преступлением в сфере компьютерной информации следует признавать виновно совершенное

общественно опасное деяние, запрещенное уголовным законом под угрозой наказания, причиняющее вред либо создающее угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту.

Библиографический список

1 Алескеров В. И. О преступлениях, совершаемых в сфере телекоммуникаций и компьютерной информации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2018. – № 1. – С. 5-10.

2 Антонян Ю. М. Криминология: учебник для академического бакалавриата. – 3-е изд. – М.: Юрайт, 2018. – 388 с.

3 Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзинский. – М.: Юрид. лит., 1991. – 160 с.

4 Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дисс. … канд. юрид. наук. – М., 2007. – 33 с.

5 Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дисс. … канд. юрид. наук. – Казань, 2008. – 27 с.

6 Рубцова А. С. Актуальные проблемы уголовного права. Особенная часть: учебное пособие для магистрантов. – М.: Проспект, 2018. – 112 с.

7 Сверчков В. В. Уголовное право. Общая и Особенная части: учебное пособие. – М.: Юрайт, 2008. – 574 с.

8 Суслопаров А. В. Информационные преступления: автореф. дисс. … канд. юрид. наук. – Красноярск, 2008. – 23 с.

9 Эмиров М. Б. Борьба с компьютерными преступлениями: международно-правовые аспекты / М. Б. Эмиров, А. Г. Саидов, Д. А. Рагимханова // Юридический вестник ДГУ. – 2011. – № 4. – С. 59-62.

10 Kaspersky Security Bulletin 2014. [Электронный ресурс] // Режим доступа : http://securelist.ru/files/2014/ 12/Kaspersky-Security-Bulletin-2014-Ru.pdf