УДК 343.2/.7

С. С. Захарова
доцент кафедры уголовного права
Академии ФСИН России,
кандидат юридических наук, доцент
С. А. Корнеев
преподаватель кафедры уголовного права
Академии ФСИН России,
кандидат юридических наук

СТАНОВЛЕНИЕ И РАЗВИТИЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА КИБЕРПРЕСТУПЛЕНИЯ В РОССИИ

В теории уголовного права нет единообразного понимания сущности преступлений в сфере компьютерной информации. За время действия норм-новелл Уголовного кодекса Российской Федерации (далее — УК) как в теории, так и в практике их применения выявились существенные противоречия, причинами которых являются: недостатки уголовно-правовой конструкции норм о преступлениях в сфере компьютерной информации; неверное представление правоохранительных органов о значении и роли исследуемых норм в охране общественных отношений; ошибки в теоретическом и практическом толковании некоторых уголовно-правовых терминов и положений ст. 272–274 УК. Изменения уголовного законодательства в части регламентации преступлений в сфере компьютерной информации, на наш взгляд, нуждаются в комплексном, всестороннем изучении, что и обуславливает актуальность выбранной темы исследования.

В большинстве случаев термин «преступления в сфере компьютерной информации» ученые употребляют в широком смысле и относят к ним все общественно опасные деяния, где компьютерная техника (компьютерная информация) выступает средством (способом) совершения преступления, т. е. не ограничиваются анализом деяний, предусмотренных в главе 28 УК.

Если подходить формально юридически, под «преступлениями в сфере компьютерной информации» необходимо понимать только те, которые включены в одноименную главу 28 УК. Однако очевидно, что деяния, зафиксированные, например, в ст. 159^6 УК, являются: а) преступлениями; б) в сфере компьютерной информации, что следует из гипотезы этой статьи.

Проблема усугубляется тем, что дать однозначное определение этим преступлениям объективно затруднительно, так как есть сложности с выделением какого-либо одного объекта преступного посягательства.

Ученые по-разному объясняют отсутствие в науке и практике однозначного определения «преступлений в сфере компьютерной информации»: одни — значительным практическим разнообразием подобных преступлений [1, с. 23], другие — отсутствием единообразной доктринальной позиции и отнесения конкретных общественно опасных деяний к таким преступлениям [2, с. 54].

Очевидно, что различие в терминологии указывает на отсутствие единого подхода к данной проблеме как в научном сообществе, так и среди субъектов, уполномоченных принимать нормативно-правовые акты. Попытки систематизировать и унифицировать понятийный аппарат в рассматриваемой сфере на законодательном уровне предпринимались достаточно давно, однако прошедшие десятилетия не позволили сформировать единых подходов к определению термина «преступления в сфере компьютерной информации». Указанная проблема стала предпосылкой для развития доктринальных исследований в данном направлении, однако в уголовно-правовой науке так и не удалось выработать общепринятого и не имеющего заметных недостатков определения понятия «информационные преступления». При этом обращает на себя внимание тот факт, что все рассмотренные определения в качестве своей опорной точки используют понятие «информация», которое является крайне широким, поскольку относится к любым сведениям, сообщениям и данным независимо от их носителя.

Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий с вредоносными целями. Представляется, что именно использование информационных технологий и информационно-телекоммуникационных сетей может быть положено в основу при выделении информационных преступлений как особой группы уголовно наказуемых деяний [3]. В соответствии же с действующим законодательством, информационные технологии — это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационно-телекоммуникационная сеть — это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [4].

Исходя из этого, можно определить информационные преступления как запрещенные уголовным законодательством под угрозой наказания виновно совершенные общественно опасные деяния, механизм совершения которых предполагает использование информационных технологий и (или) информационно-телекоммуникационных сетей. Сразу же становится возможным выделить особенность таких преступлений, отличающую их от уголовно наказуемых

деяний иных видов. Данные преступления по своей природе являются высокотехнологичными, требующими наличия у преступника определенных знаний и опыта, специального оборудования и (или) компьютерных программ.

Считаем, что одной из основных причин отсутствия единообразия в понимании, определении и правоприменении термина «преступления в сфере компьютерной информации» является отсутствие единообразного понимания его элементов. Так, понятие «преступление в сфере компьютерной информации» состоит из следующих элементов: «преступление»; «в сфере» и «компьютерная информация».

Определение понятий первых двух элементов не вызывает сложностей в восприятии и толковании. Сложнее обстоит вопрос с определением понятия «компьютерная информация». Полагаем, что понятие компьютерных преступлений является более широким понятием по сравнению с преступлениями в сфере компьютерной информации и включает их в себя. Такой подход, имеющийся в теории уголовного права, к разграничению компьютерных преступлений и преступлений в сфере компьютерной информации не вызывает сомнений. Уточняя его, отметим, что основным, дополнительным либо факультативным объектом посягательства при совершении компьютерных преступлений будет выступать компьютерная безопасность, т. е. состояние защищенности компьютерных и сетевых устройств от угроз различного характера.

Под преступлениями против безопасности компьютерной информации следует понимать запрещенные уголовным законом Российской Федерации виновно совершенные общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности обращения (производства, хранения, использования либо распространения) компьютерной информации или вреда КИИ РФ.

Список основных источников

1. Чуищев, И. М. Может ли хакер защитить от компьютерных преступлений / И. М. Чуищев // Юрист. — 1999. — № 2. — С. 22–26. Вернуться к статье

2. Ястребов, Д. А. Институт уголовной ответственности в сфере компьютерной информации: опыт международно-правового сравнительного анализа / Д. А. Ястребов // Государство и право. — 2005. — № 1. — С. 53–63. Вернуться к статье

3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом Рос. Федерации 24.07.2013 г. № Пр-1753) [Электронный ресурс] // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2022. Вернуться к статье

4. Об информации, информационных технологиях и защите информации [Электронный ресурс] : Федер. закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2022. Вернуться к статье