УДК 343.3/.7

Ю. Н. Танана,
магистр юридических наук
Учреждение образования «Барановичский государственный университет», Барановичи

ГРАНИЦЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Республики Беларусь, которая существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет только возрастать.

С развитием информационного общества появилась потребность в защите его главного движущего фактора — информации, а теперь и особого ее вида — компьютерной информации. Пресечь наиболее опасные проявления человеческого поведения в информационной сфере — задача уголовного законодательства. В США и странах ЕС составы компьютерных преступлений присутствовали в законе уже с конца 80-х годов прошлого века.

Термин «компьютерная преступность» появился в американской, а затем другой зарубежной печати в начале 60-х годов прошлого века, когда были выявлены первые случаи преступлений, совершенных с использованием вычислительных машин [1, с. 69—70].

В России уголовная ответственность за аналогичные деяния была введена в 1997 году со вступлением в силу действующего УК РФ [2, с. 337], в белорусском же законодательстве подобные нормы появились в 1999 году.

Основная часть. Действующий УК Республики Беларусь содержит отдельный раздел XII (глава 31) «Преступления против информационной безопасности».

Информационную безопасность следует рассматривать в узком и широком смыслах слова. Информационная безопасность в широком смысле слова — это состояние защищенности интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Говоря об информационной безопасности в узком смысле слова, акцент следует делать уже на защищенности самой информации.

Таким образом, информационная безопасность в узком смысле, по сути, является родовым объектом преступлений, предусмотренных гл. 31 УК Республики Беларусь. Вместе с тем следует отметить нечеткость определения родового объекта этих преступлений законодателем, не сделавшим акцент на компьютерном характере охраняемой информационной безопасности. Тогда как ученые, исходя из особенностей преступлений, предусмотренных гл. 31, называют, как правило, их компьютерными преступлениями, соответственно определяя и их родовой объект.

Понятием «компьютерная информация», применяемым в УК Республики Беларусь, охватывается информация, хранящаяся в компьютерной сети, системе, на компьютерных носителях либо передаваемая сигналами, распространяемыми по проводам, оптическим волокнам, или радиосигналами.

Раздел XII УК Республики Беларусь включает следующие преступления против информационной безопасности: с. 349 «Несанкционированный доступ к компьютерной информации»; с. 350 «Модификация компьютерной информации»; с. 351 «Компьютерный саботаж»; с. 352 «Неправомерное завладение компьютерной информацией»; с. 353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»; с. 354 «Разработка, использование либо распространение вредоносных программ»; с. 355 «Нарушение правил эксплуатации компьютерной системы или сети» [3].

Родовым объектом всех этих преступлений является информационная безопасность. Что касается их непосредственных объектов, то в литературе заметен существенный разнобой. Так, одни авторы считают, что непосредственным объектом всех этих преступлений является информационная безопасность, а в качестве их дополнительного непосредственного объекта признают права и законные интересы владельцев и пользователей компьютерной информации [4, с. 648—663]. Другие авторы дифференцируют объект в зависимости от вида преступления, считая его только основным. Например, объектом несанкционированного доступа к компьютерной информации Н. А. Ахраменка в одной работе считает порядок доступа к компьютерной информации, дающей субъекту право на ознакомление с ней [5, с. 761], в другой работе в качестве такового он называет общественные отношения, в которых реализуется установленный порядок ознакомления и работы с компьютерной информацией [6, с. 814].

Порядок доступа к компьютерной информации признает непосредственным объектом данного преступления и О. И. Бахур [7, с. 502].

Исследователь Н. А. Швед, которая провела более глубокое исследование вопроса об уголовной ответственности за несанкционированный доступ к компьютерной информации, непосредственным объектом этого преступления признает общественные отношения по обеспечению охраны компьютерной информации и нормальной работы компьютера, компьютерной системы или их сети от несанкционированного вмешательства. Дополнительный объект, по ее мнению, альтернативен. Его наличие зависит от характера вреда,

причиненного правам и законным интересам потерпевшего. В силу этого и учитывая наличие в ст. 349 УК Республики Беларусь оценочного понятия «существенный вред», автор считает, что дополнительным объектом этого преступления могут выступать как отношения собственности, так и жизнь, здоровье, конституционные права и свободы граждан и т. д., т. е. те общественные отношения, в которых находят применение процессы обработки, хранения и передачи компьютерной информации [8, с. 44—45].

При определении непосредственного объекта рассматриваемого преступления следует, прежде всего, сохранять системность подхода. Учитывая то, что его видовым объектом закон признает информационную безопасность, ее следует признавать и непосредственным объектом с теми поправками, которые вытекают из неточности законодательного определения родового и видового объектов. Иными словами, непосредственным объектом данного преступления является компьютерная безопасность как более широкое понятие. Названные в ч. 1 ст. 349 УК Республики Беларусь последствия в виде изменения, уничтожения, блокирования информации или вывода из строя компьютерного оборудования и будут свидетельствовать о том, что компьютерной безопасности причинен вред. Что касается последствия в виде причинения иного существенного вреда, то здесь должна речь идти о дополнительном объекте (альтернативном).

Следует отметить, что все преступления, закрепленные в разделе XII УК Республики Беларусь (глава 31) «Преступления против информационной безопасности», посягают на компьютерную безопасность. Конкретизация их непосредственных объектов необходима для установления направленности вреда и, соответственно, квалификации содеянного.

Наряду с этим преступления, посягающие на информационную безопасность, понимаемую как состояние защищенности жизненно важных интересов физических и юридических лиц в информационной сфере, указаны и в других главах УК Республики Беларусь: главе 25 «Преступления против порядка осуществления экономической деятельности» (ст. 254 «Коммерческий шпионаж», ст. 255 «Разглашение коммерческой тайны»); главе 26 «Преступления против экологической безопасности и природной среды» (ст. 268 «Сокрытие либо умышленное искажение сведений о загрязнении окружающей среды»); главе 27 «Преступления против общественной безопасности» (ст. 308 «Несообщение информации об опасности для жизни людей») и др.

Заключение. Границы уголовно-правовой охраны информационной безопасности четко очерчены нормами УК Республики Беларусь, содержащего отдельную главу о защите информационной безопасности, но не исчерпываются данной главой.

Анализ кодекса показывает, что в нем правомерно выделены отношения, возникающие в области использования компьютерной информации, подлежащие специальной охране. Между тем название родового объекта слишком широкое, не раскрывающее его особенности применительно к преступлениям, выделенным в специальную главу.

В данной ситуации родовым объектом этих преступлений следует считать безопасность использования компьютерной информации, под которой необходимо понимать отношения, обеспечивающие безопасное производство, хранение, передачу, использование и защиту компьютерной информации от различных посягательств. Такое понимание объекта более конкретно и точнее соответствует содержанию составов преступлений, предусмотренных в главе 31 УК Республики Беларусь.

Изложенное позволяет предложить изменение названия соответствующего раздела и главы уголовного кодекса, которые следует назвать «Преступления против безопасности использования компьютерной информации».

Список источников

1. *Копылов, В. А.* Информационное право. Концепция структуры системы информационного права / В. А. Копылов // Труды по интеллектуальной собственности : материалы науч.-технич. конф. от 27 января 2000 г. — М. : Юристъ, 2000. — Т. II. — 195 с.

2. *Незнамова, З. А.* Уголовное право. Особенная часть / З. А. Незнамова, И. Я. Козаченко. — М. : Издат. группа НОРМА-ИНФРА, 1998. — 750 с.

3. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 19.07.2016 г. // Национальный правовой Интернет-портал Республики Беларусь, 22.07.2016, 2/2403.

4. *Лукашов, А. И.* Уголовное право Республики Беларусь. Особенная часть : учеб. пособие / под общ. ред. А. И. Лукашова. — Минск : Гревцов, 2009. — 892 с.

5. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / под общ. ред. А. В. Баркова, В. М. Хомича. — Минск : ГИУСТ БГУ, 2007. — 1007 с.

6. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / под общ. ред. А. В. Баркова, В. М. Хомича. — 2-е изд., с изм. и доп. — Минск : ГИУСТ БГУ, 2010. — 1064 с.

7. Уголовное право. Особенная часть / под ред. В. А. Кашевского. — Минск : Академия МВД, 2012. — 736 с.

8. *Швед, Н. А.* Уголовная ответственность за несанкционированный доступ к компьютерной информации : дис ... канд. юрид. наук : 28.07.2013 / Н. А. Швед. — Минск, 2009. — 119 л.