УДК 343.2/7

ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ: ПОНЯТИЯ, ВИДЫ

В.В. Боричевская
Полесский государственный университет, Valentina_Bor@mail.ru

В юридической литературе в последнее время появилось понятие «информационные преступления», содержание которого не вполне определено. Осознавая важность информации, общество приходит к пониманию опасности информационной преступности.

Исходя из теоретических знаний, и с учетом того, что они представляют угрозу именно информационной сфере, понятие «информационные преступления» изначально можно определить как общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области информационных правоотношений, то есть отношений, связанных с созданием, сбором, обработкой, накоплением, хранением, поиском и распространением информации. Однако следует заметить, что такое понимание информационных преступлений является слишком широким. Так, в ряде составов преступлений информационным является способ совершения общественно опасного деяния, который может выступать, например, в виде угроз различного характера или обмана, используемых для достижения тех или иных целей виновного. В этих случаях налицо процессы распространения информации, следовательно, преступления, совершаемые подобными способами, нужно относить к информационным преступлениям. Получается, что и изнасилование, и мошенничество, и разбой, а также некоторые другие преступления необходимо отнести к информационным, что является неверным.

В связи с этим необходимо подробно изучить и проанализировать действующее законодательство, различные взгляды и теории научных исследователей, чтобы увидеть реальную действительность и разобраться в понятии, видах информационных преступлений.

По мнению Крылова В.В., информационные преступления это общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания [2.с.11].

Уголовно-правовые нормы, устанавливающие ответственность за данные виды преступлений, отличаются друг от друга тем, что в первом случае они направлены на защиту информации того или иного содержания, во втором – на защиту человека и общества от «вредной» информации, а в третьем – на защиту права любого члена общества на доступ к открытой информации.

Исходя из данного подхода к информационным преступлениям следует относить преступления, которые связаны:

а) с посягательством на саму информацию;

б) с распространением «вредной» (вредоносной) информации;

в) с посягательством на право граждан и иных субъектов на доступ к открытой информации.

Таким образом, в зависимости от тех целей первого вида информационных преступлений, которые преследовал законодатель, устанавливая ответственность за деяния, совершаемые с информацией, можно выделить две их группы.

1. Преступления (предусмотренные, например, ст. 192, 227, 237, 268, 349, 349-355 Уголовного кодекса Республики Беларусь (далее УК) и др., предметом которых является информация, зафиксированная на строго определенных носителях. В данном случае законодатель стремится обеспечить порядок формирования, должного хранения, использования и распространения информационных ресурсов.

2. Преступления (предусмотренные, например, ст. 177-179, 201, 254, 255, 356, 358 УК и др.), предметом которых является информация, вне зависимости от того, на каком носителе она закреплена. В указанных нормах даже не упоминается вид носителя информации.

В данном случае цель уголовного закона – защитить сведения, имеющие ограниченный доступ, к которым относятся:

а) сведения, составляющие государственную тайну (государственные секреты);

б) сведения конфиденциального характера.

В зависимости от содержания сведений конфиденциального характера можно предложить следующую классификацию информационных преступлений:

1) Преступления, посягающие на сведения о частной жизни лица (ч. 1 ст. 179 УК – нарушение неприкосновенности частной жизни, ст. 177 УК – разглашение тайны усыновления (удочерения) общим субъектом).

2) Преступления, посягающие на сведения, составляющие коммерческую и банковскую тайну (ст. 255 УК – Умышленное разглашение коммерческой или банковской тайны).

3) Преступления, посягающие на служебную тайну (ст. 375 УК Умышленное разглашение служебной тайны специальным субъектом, ст. 408 УК – разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса. Кроме того, служебная тайна может нарушаться путем совершения иных общественно опасных деяний (ст. 226-1, 254, 255, 356 и 358 УК и др.).

Квалификация по той или иной статье УК зависит от субъекта, совершающего преступление, и содержания сведений, составляющих служебную тайну.

4) Преступления, связанные с посягательствами на профессиональную тайну (например, врачебную, ст. 178УК). Преступления, посягающие на сведения, которые составляют тайну предварительного расследования (ст. 407УК) и судопроизводства.

Предметом здесь можно признать сами сведения, как уже говорилось, учитывая то, что, в конечном счете, указанная информация содержится на определенных материальных носителях (в широком смысле). Вид носителей в данном случае (бумага, фотопленка, магнитный диск, и т. п.) и форма представления информации (письменная, устная, визуальная, в виде рисунков, чертежей и т. п.) не имеют значения.

Особый вид информационных преступлений составляют общественно опасные посягательства, предметом которых является так называемая «вредная» (вредоносная) информация:

– изготовление и распространение порнографических материалов или предметов порнографического характера (ст. 343 УК);

– изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего (ст. 343-1 УК) и др.

Исследуя проблему понятия и видов информационных преступлений, можно предложить третью классификацию информационных преступлений в связи с посягательствами на право доступа каждого к открытой (общедоступной) информации.

Путем анализа уголовно-правовых норм, можно выделить две группы деяний, посягающих на общедоступную информацию.

1)Непредставление подобной информации.

Это вид деяния выражается в таких действиях (бездействии), как отказ в предоставлении информации (статья 204 УК), уклонение от ее предоставления (ст. 308 УК) или ее сокрытие (ст. 228 УК), отказ и уклонение от предоставлении информации (ст.402 УК).

2) Предоставление информации ненадлежащего вида (ложной или искаженной, неполной) (например, 227,238, 239, 243,249, 250, 340, 400,401,427 УК и др.). Указанная информация может предоставляться как конкретному субъекту, так и неопределенному кругу лиц.

В УК Республики Беларусь есть деяния, которые содержат признаки 2-х этих групп, например, представление заведомо ложных документов и сведений либо умышленное несообщение информации (ст.237); Уклонение от представления информации (документов, объяснений), либо представление заведомо ложной информации (ст.244) и др.

В свете рассматриваемой проблемы интерес представляет такое понятие, как «компьютерные преступления», которые составляют особую группу информационных преступлений.

На мой взгляд, данные информационные преступления можно определить как общественно опасные деяния, представляющие угрозу информационной безопасности, связанные с порядком использования компьютерной информации.

Все еще не существует четкого определения понятия данного вида преступлений, и дискутируются различные точки зрения по их классификации. Сложность в формулировке этих понятий существует, по-видимому, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны.

И. Чуищев, например, объясняет отсутствие в уголовном праве « единого понятия компьютерного преступления» их чрезвычайным практическим разнообразием [6.с.24]. Также существует такая точка зрения, что компьютерные преступления представляют собой все преступления, при котором компьютер является орудием, средством или целью их совершения, а другие объединяют под этим термином все противозаконные действия, которые причиняют ущерб имуществу и связаны с электронной обработкой информации.

По мнению Ю.М. Батурина, компьютерных преступлений как особой группы преступлений в юридическом смысле не существует, однако при этом отмечает тот факт, что многие традиционные виды преступлений модифицировались из-за вовлечения в них вычислительной техники и поэтому правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу [1.с.156].

Другого, более определенного взгляда придерживается А.Н. Караханьян. Под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины [3.с.18]. В.В. Крылов использует подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя не оправдывает и поэтому нецелесообразно принимать термин "компьютерные преступления" за основу для наименования в е всей совокупности преступлений в области информационных отношений. Компьютер, по его мнению, является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением конфиденциальной документированной информации. Данный автор предлагает рассматривать в качестве базового понятия "информационные преступления", исходя из того, что сложившаяся система правоотношений в области информационной деятельности, позволяет абстрагироваться от конкретных технических средств. Конечно, можно согласиться с данным мнением, что преступление в области компьютерной информации, выделенные в отдельную главу УК Республики Беларусь, являются частью информационных преступлений, объединенной общим инструментом обработки информации – компьютером.

Но, на мой взгляд, можно выделить в отдельный вид "компьютерные преступления" или преступления в сфере высоких технологий – общественно опасные деяния в области информационных правоотношений, представляющие угрозу информационной безопасности, связанные с порядком использования компьютерной информации. Такие деяния подпадают под санкции статей УК Республики Беларусь, содержащихся в 31 главе "Преступления против информационной безопасности". Судя по своему названию, данная глава должна бы содержать все информационные преступления по своей сути, однако, по моему мнению, данная глава не охватывают всех общественно опасных деяний в сфере информационных правоотношений - это видно из нашего анализа уголовного закона выше.

На основании выше изложенного, можно сделать следующие выводы:

1) информационные преступления характеризуются общим объектом, предметом. Общим объектом информационных преступлений всегда выступают правоотношения в информационной сфере. Родовыми объектами информационных преступлений являются личность, сфера экономики, общественная безопасность и общественный порядок, государственная власть. Непосредственным объектом преступных посягательств в области информационных правоотношений выступают конституционные права, свободы и достоинство личности, экономические интересы общества и личности, общественная и безопасность государства, связанные с неправомерным доступом к информации, нарушением режима ее конфиденциальности, распространением ложной и вредной информации или отказом в предоставлении информации. Предметом преступных посягательств является охраняемая законом

информация, вне зависимости от того, на каком носителе она закреплена, в том числе и на машинных носителях;

2)анализ уголовно-правовых последствий неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных программ показал наличие достаточных оснований для введения дополнительных квалифицирующих признаков в составы некоторых статей Уголовного кодекса Республики Беларусь;

3)под информационным преступлением следует понимать запрещенные Уголовным Кодексом общественно опасные деяния, объектом преступных посягательств которых являются информационные правоотношения в информационной сфере.

Список использованных источников:

1. Батурин, Ю.М Проблемы компьютерного права / Ю.М. Батурин. – М. : Юридическая литература,1991. – 272 с.

2. Копылов, В.А. Информационное право. Учебное пособие / В.А. Копылов. – М. : Юристь,1997. – 281 с.

3. Крылов, В.В. Основы криминологической теории расследования преступлений в сфере информации / В.В. Крылов, М. : МГУ, 1998. – 50 с.

4. Полевой, Н.С. Правовая информация и кибернетика./ Н. С. Полевой. – М. : Юридическая литература, 1993. – 18 с.

5. Селиванов, Н. Проблемы борьбы с компьютерной преступностью / Н. Селиванов. – М. : Законъ, 1993. – 199 с.

6. Чуищев, И.М. Может ли хакер защитить от компьютерных преступлений / И.М. Чуищев. – М. : Юрист, 1999. – 24 с.

7. Уголовный кодекс Республики Беларусь: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г. (ред. от 15.07.2010) (с изм. и доп., вступившими в силу с 13.08.2010) // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2010.