

Парламентское собрание Союза Беларуси и России
Постоянный Комитет Союзного государства
Оперативно-аналитический центр
при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Полоцкий государственный университет



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)
К63

К63

Комплексная защита информации : материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)

КИБЕРПРЕСТУПНОСТЬ: ПРОБЛЕМЫ ПРИВЛЕЧЕНИЯ К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

В.Р. МЕЛЬНИК, Т.В. РАДЫНО

Юридический колледж БГУ

Использование компьютерной техники сегодня вошло не только в жизнь всех законопослушных граждан – в уголовном кодексе то один из наиболее распространенных способов совершения преступления. Исследование проблем компьютерной преступности носит междисциплинарный характер и является предметом изучения многих наук и учебных дисциплин, среди которых юридические науки, в том числе и уголовное право, занимают одно из основных мест. Базовым в сфере уголовно-правовых и криминалистических наук является понятие «киберпреступность».

Киберпреступность часто понимают, как преступность в виртуальном пространстве или же преступление, совершаемое с помощью компьютера. Виртуальное пространство, или киберпространство определяется как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, в математическом, символьном или другом виде и в процессе движения по локальным и глобальным компьютерным сетям, либо сведениям, хранящимся в памяти любых реальных или виртуальных устройств, а также другим носителям, специально предназначенным для их хранения, обработки и передачи.

С каждым годом киберпреступность развивается и набирает обороты: в то время как в период с 1998 по 2002 год было совершено всего несколько сотен преступлений в сфере IT-технологий, в 2016 году их совершили уже 2471 только на территории Республики Беларусь. В 2016 году в сравнении с 2015 годом число выявленных преступлений в сфере высоких технологий увеличилось на 1,3% (с 2 440 до 2 471), в том числе по областям: Брестская – 260 (276), Витебская – 286 (243), Гомельская – 353 (354), Гродненская – 206 (249), Минск – 818 (776), Минская – 311 (304), Могилевская – 237 (238). Общий уровень раскрываемости составил 56,5 % (в 2015 г. – 55,5 %). К уголовной ответственности привлечено 866 человек, в том числе 286, имеющих судимость, 648 неработающих и 34 несовершеннолетних. Возмещение установленного материального ущерба составило 48,5 %.

Увеличение количества киберпреступлений произошло за счет прироста преступлений против информационной безопасности на 63,6 % (с 404 до 651). Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (с 102 до 258). Последнее объясняется в первую очередь высоким уровнем латентности преступлений данной категории.

Доля хищений путем использования компьютерной техники от всех выявленных преступлений в сфере высоких технологий ежегодно снижается (с 2036 до 1820), в 2016 году их удельный вес составил – 73,7 % от общего числа. Количество хищений в особо крупном и крупном размерах также уменьшилось (с 45 до 41) [1].

На сегодняшнем этапе правоохранительная система пока находится в поиске не только методов борьбы с этой проблемой, но и в процессе выработки единой политики по этому вопросу. Отсутствие фундаментальных научных исследований, посвящённых изучению проблемы компьютерной преступности как явления, охватывающих собой весь спектр преступлений, заменяется вопросом совершенствования уголовной ответственности за совершение преступлений в сфере информационной безопасности. Такой

путь скорее тупиковый: игнорируется возможность создания прогноза на будущее, развития стратегии борьбы с этим явлением, получая на выходе слабую готовность правоохранительных органов к борьбе с преступностью в области информационной безопасности. Такое положение дел отражается на результатах деятельности правоохранительных органов Республики Беларусь по выявлению (раскрытию), расследованию и предупреждению криминальных деяний, относящихся к преступлениям в сфере информационной безопасности.

Проблема уголовной ответственности в практическом ее значении выходит за рамки "совершения виновно запрещенного уголовным законом деяния" [2, статья 11]. Она включает и необходимость указания на объект посягательства, поскольку это позволяет более точно определить форму запрета на деяние, и на субъект преступления, который одновременно является виновником запрещенного уголовным законом деяния и объектом воздействия уголовной ответственности и поэтому должен отвечать определенным условиям, установленным законом. Понятие "преступление" как основание уголовной ответственности включает в себя и фактическое основание (общественно опасное поведение или причинение вреда объектам уголовно-правовой охраны), и юридическое основание (состав как совокупность законодательных признаков).

Что касается субъекта, совершающего преступления с помощью компьютера, то сегодня это – лицо, достигшее 14 лет, вменяемое, если не будет установлено, что вследствие отставания в психическом развитии, не связанного с психическим расстройством (заболеванием), оно во время совершения общественно опасного деяния было не способно сознавать фактический характер или общественную опасность своего деяния [2, статья 27].

Что же касается объекта уголовно-правовой охраны – то здесь и кроются первые подводные камни, которые угрожают «посадить на мель» правоприменителя. Дело в том, что сегодня нормативно-правовые акты, обеспечивающие защиту информации, принимаются зачастую бессистемно, не вносятся своевременно изменения в уголовный кодекс, непосредственно устанавливающий круг преступных деяний. Чтобы внести в Уголовный кодекс Республики Беларусь (УК) новый состав преступления, необходимо для начала определить объект преступного посягательства, поскольку именно он ложится в основу классификации преступных деяний и размещения их в кодексе по разделам и главам. Далее выделяется предмет, на который покушается преступник – неразрывно связанный с объективной стороной (деянием). Однако при том, что принятие изменений в нормативные акты, напрямую связанных с Интернет-пространством, приводит к появлению по существу новых правонарушений, совершаемых в глобальной сети Интернет с использованием компьютерной техники – тем не менее, объектом таких посягательств напрямую не является непосредственно информационная безопасность, более того – зачастую такие преступления не относятся к киберпреступности в обозначенном выше ее понимании вообще.

Так, например, материалы, опубликованные в глобальной сети Интернет, сегодня признаются опубликованными в средствах массовой информации, благодаря внесению изменений в пункт 19 Закона Республики Беларусь от 17.07.2008 № 427-З "О средствах массовой информации". В результате – к составу такого преступления, как клевета (ст. 188 УК) относятся также действия, связанные с размещением в глобальной компьютерной сети Интернет информации определенного свойства и содержания. Тот же подход имеет место при привлечении к уголовной ответственности за оскорбление – хотя как раз в статье 189 УК прямо и не упоминается глобальная сеть Интернет. Объектом преступного посягательства в данном случае является честь и достоинство человека.

Базовым подходом в борьбе с так называемой «киберпреступностью» является направленность работы оперативно-следственных органов на предупреждение и раскрытие хищений с использованием компьютерной техники (статья 212 УК), а также - причинение имущественного ущерба без признаков хищения (статья 216 УК). Однако следует отметить, то объектом уголовно-правовой охраны в данном случае является не что иное, как овеществленная собственность, имеющая рыночную стоимость – а не информация, к которой получает несанкционированный доступ либо которую модифицирует преступник. Предметом таких преступлений является исключительно имущество с точки зрения гражданско-правовых отношений.

Традиционно в науке уголовного права отмечается, что к имуществу не относится и соответственно предметом посягательств на собственность не является интеллектуальная собственность, поскольку последняя не содержит в себе экономического содержания собственности. За посягательство на интеллектуальную собственность ответственность предусмотрена в главах о преступлениях против конституционных прав и свобод человека и гражданина (нарушение авторских и смежных прав, изобретательских и патентных прав), против порядка осуществления экономической деятельности (незаконное использование товарного знака), против информационной безопасности (неправомерное завладение компьютерной информацией) и т.д. [3]. Однако, охраняемые авторским правом изображения, видео, текстовые и иные материалы, которые попадают в сеть Интернет, становятся доступны неопределенному кругу лиц, но не утрачивают статуса объектов интеллектуальной собственности. Их несанкционированное использование влечет риск привлечения к гражданско-правовой, административной или уголовной ответственности. В целях обеспечения защиты интересов личности, общества и государства в информационной сфере, создания условий для дальнейшего развития национального сегмента глобальной компьютерной сети Интернет, повышения качества и доступности, предоставляемой гражданам и юридическим лицам информации был принят Указ Президента Республики Беларусь от 01.02.2010 № 60 (ред. от 23.01.2014) "О мерах по совершенствованию использования национального сегмента сети Интернет".

Уже имеет место судебный прецедент вынесения обвинительного приговора за распространение порнографических материалов с использованием глобальной компьютерной сети Интернет (ст. 343 УК): после оценки фото порнографического характера пользователь Интернет поделился ссылкой на него в социальных сетях – за что и был осужден по приговору суда. Объектом такого преступления является общественная нравственность, способом его совершения – использование компьютерной техники, доступ к материалам, просмотр которых преследуется по закону и их распространение.

Как видно из вышеприведенных примеров, информационная безопасность как объект преступных посягательств присутствует во многих составах преступлений, хотя непосредственно представлена в качестве непосредственного объекта уголовно-правовой защиты только в составах главы 31 УК.

Список литературы

1. Статистические данные Министерства внутренних дел Республики Беларусь за 2016 год // Электронный документ [Электронный ресурс]. - Режим доступа: <http://mvd.gov.by/main.aspx?guid=3311>, свободный.
2. Кодекс Республики Беларусь от 09.07.1999 № 275-3 (ред. от 19.07.2016) "Уголовный кодекс Республики Беларусь" // СПС «КонсультантПлюс» (дата обращения: 21.04.2017).
3. "Интеллектуальная собственность как предмет хищения" (В.В. Хилюта) (по состоянию на 19.08.2013) // СПС «КонсультантПлюс» (дата обращения: 21.04.2017).