технических средств с использованием современных технологий. Не принимая на вооружение ОВД существующие инновационные технологии, в дальнейшем будет сложно противостоять росту преступности.

Одним из обстоятельств, затруднявших учет преступлений в начале развития использования высоких технологий в преступных целях, являлось отставание уголовных законодательств государств от темпов развития научно-технического прогресса. Это позволило преступникам некоторое время безнаказанно использовать возможности высоких технологий в своих целях. В данной связи существует необходимость и предпосылки для правового регулирования информационного пространства. В соответствии с УК Республики Казахстан предпосылки правового регулирования проявляются, во-первых, в возрастающей роли информационной деятельности самой информации; во-вторых, в становлении единого информационного пространства страны признаком государства и государственности на современном этапе развития; в третьих, в возможности включения в сферу правового обращения объектов информационных отношений и объективной необходимостью такого воздействия со стороны государства с целью упорядочения самой системы отношений, в которых прямо или косвенно проявляются эти объекты. Необходимость правового регулирования информационного пространства основывается на данных предпосылках, а также на самой природе права как социального регулятора конституционно-правовых отношений в информационном пространстве.

Деятельность по незаконному использованию высоких технологий отличает повышенные меры конспирации и скрытность предстоящих операций со стороны готовящих их группировок. Это ставит перед ОВД сложную задачу превентивного получения оперативной информации о готовящихся преступлениях. Так, анализ обстановки, сложившейся, например, в сфере интеллектуальной собственности, показывает, что современные информационные технологии все чаще стали использоваться преступниками для распространения продукции, запрещенной в свободном обороте. Потребительский рынок наводнен контрафактной аудио-, видео продукцией и программным обеспечением. В данном контексте ОВД необходимо выявлять и устанавливать лиц, занимающихся изготовлением, тиражированием и распространением контрафактной продукции. Такая работа должна постоянно совершенствоваться и находиться на постоянном контроле заинтересованных органов.

Таким образом, наряду с положительными сторонами развития высоких технологий, охвативших все сферы нашего общества, имеются и негативные стороны, которые выражаются в появлении новых видов преступлений. По своему механизму, способам совершения и сокрытию следов эти преступления имеют определенную специфику, характеризующуюся высочайшим уровнем латентности и низким уровнем раскрываемости. Это связано с тем, что их появление застало врасплох правоохранительную систему. Правоохранительные органы оказались не готовыми к адекватному противостоянию в борьбе с новым видом преступного посягательства

из-за отсутствия должного законодательного обеспечения и научно обоснованных рекомендаций по выявлению и раскрытию преступлений с использованием высоких технологий.

Мировая практика свидетельствует о том, что невозможно создать абсолютно защищенную информационную систему, но для обеспечения высокой степени защиты компьютерной информации необходим комплексный подход к информационной безопасности, при котором законодательные, организационные, программно-технические меры и средства защиты используются одновременно, дополняя друг друга. Для эффективного предупреждения неправомерного доступа к компьютерной информации необходима система мер нормативно-правового, организационного, технического и информационного характера, адресованная не столько правоохранительным органам, сколько широкому кругу пользователей компьютерной информации. Усовершенствование законодательства, регулирующего деятельность и отношения в сфере использования информационных ресурсов, эффективные приемы технического характера во многом будут способствовать снижению уровня преступлений в сфере высоких технологий.

В рамках изложенных тезисов не представляется возможным охватить проблемы киберпреступности в деятельности ОВД Республики Казахстан, поэтому были выборочно затронуты основные аспекты расследования преступлений в информационном пространстве, а также рассмотрены пути решения проблем в данной сфере высоких технологий.

1. Назмышев Р.А. Проблемы расследования неправомерного доступа к компьютерной информации : учеб. пособие. Астана : Данекер, 2002.

2. Жатканбаека А.Е. Правовые аспекты информационной безопасности в Республике Казахстан. Алматы, 2009.

3. Баишев Ж. Конституционное право Республики Казахстан : учеб.-метод. пособие. Алматы : Жеты Жаргы, 2001.

УДК 343.3

В.В. Лавренов

О НЕКОТОРЫХ АСПЕКТАХ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕЛАРУСИ

Информационное общество – современный этап развития цивилизации с доминирующей ролью знаний и информации, воздействием информационно-коммуникационных технологий на все сферы человеческой деятельности и общество в целом.

Развитие информационного общества является одним из национальных приоритетов республики и рассматривается как общенациональная задача,

требующая объединения усилий государства, бизнеса и гражданского общества. В настоящее время в республике завершилось формирование основ информационного общества. Заложена правовая основа информатизации. Успешно развивается национальная информационно-коммуникационная инфраструктура. В 1999 г. принимается Концепция государственной политики в области информатизации. Целью государственной политики в области информатизации является обеспечение перехода к новому этапу развития страны – построению информационного общества и вступлению республики в мировое информационное сообщество. Основой этого перехода является создание единого информационно-телекоммуникационного пространства Республики Беларусь как базы для решения задач социально-экономического, политического и культурного развития страны и обеспечения ее безопасности.

Информационные технологии нашли широкое применение в управлении важными объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

В соответствии с указом Президента Республики Беларусь от 9 ноября 2010 г. «Об утверждении концепции национальной безопасности Республики Беларусь» в информационной сфере одними из внутренних источников угроз национальной безопасности являются рост преступности с использованием информационно-коммуникационных технологий; несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В 2001 г. вступает в силу новый Уголовный кодекс (УК). Как следует из Особенной части УК Республики Беларусь, информационные правоотношения в целом получили в нем широкую уголовно-правовую защиту. Новый УК Республики Беларусь содержит ряд статей, предусматривающих ответственность за преступления против собственности (ст. 212) и информационной безопасности (ст. 349–355), совершенные с использованием компьютерных технологий. Среди преступлений, впервые введенных в УК нашей республики, законодателем определены шесть преступлений, предметом преступного посягательства которых является компьютерная информация. К ним относятся несанкционированный доступ к компьютерной информации (ст. 349); модификация компьютерной информации (ст. 350); компьютерный саботаж (ст. 351); неправомерное завладение компьютерной информацией (ст. 352); разработка, использование либо распространение вредоносных программ (ст. 354); нарушение правил эксплуатации компьютерной системы или сети (ст. 355), которые составили новую главу – «Преступления против информационной безопасности».

Если с преступными деяниями, квалифицируемыми ст. 212 УК Республики Беларусь, картина ясна, то с преступлениями против информационной безопасности ситуация не однозначна. Согласно официальной статистики пик регистрации преступлений против информационной безопасности пришелся на 2002 г. (рис. 1). В остальные годы регистрировалось в среднем 105 таких преступных деяний.

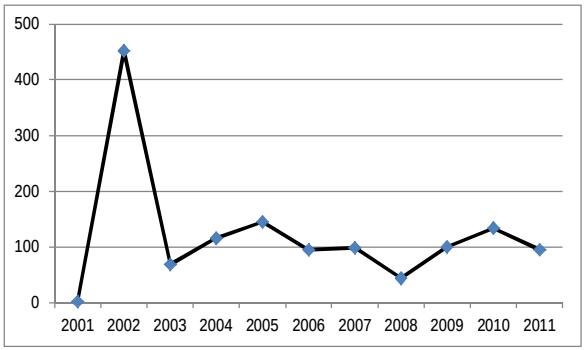

Рис. 1. Количество зарегистрированных преступлений, предусмотренных ст. 349–355 УК Республики Беларусь

Может показаться, что достигнута относительная стабильность показателя состояния преступности, но это не так. На взгляд автора, в связи с развитием информационного общества, увеличением числа использующихся компьютеров во всех сферах жизнедеятельности человека, возросло число совершаемых преступлений в сфере информационной безопасности.

Таким образом, необходимы криминологические исследования преступлений в сфере информационной безопасности, которые, подкрепленные результатами имперических исследований, могут быть положены в основу концепции предупреждения и профилактики преступлений в этой сфере.

УДК 347.775

Е.А. Левкина

ПРОБЛЕМА ПРАВОВОЙ ОХРАНЫ И ОСОБЕННОСТИ ЗАЩИТЫ ПРАВ ОБЛАДАТЕЛЯ СЕКРЕТА ПРОИЗВОДСТВА (НОУ-ХАУ) В РЕСПУБЛИКЕ БЕЛАРУСЬ

Исследование проблемы правовой охраны и защиты прав обладателей секрета производства (ноу-хау) в настоящее время представляется важной теоретической задачей, которая комплексно не изучалась белорусскими учеными-юристами. Актуальность исследования обусловлена тем, что действующее законодательство только обозначает категорию «секрет производства» (ноу-хау), но надлежащей регламентации связанных с ней отношений не содержит. В настоящее время активно обсуждается проект зако-