13. Федеральный закон от 21.10.2013 № 270-ФЗ «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» – [Электронный ресурс] – Режим доступа. – URLhttp://www.consultant.ru/document/cons_doc_LAW_153467/ (Дата обращения 29.01.2016).
14. Федеральный закон от 07.12.2011 № 420-ФЗ (ред. от 28.12.2013) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» – [Электронный ресурс] – Режим доступа. – URL: https://www.consultant.ru/document/cons_doc_LAW_122864/ (Дата обращения 30.01.2016).

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ (КОМПЬЮТЕРНЫХ) ПРЕСТУПЛЕНИЙ

Расулев Абдулазиз Каримович

канд. юрид. наук, самостоятельный соискатель кафедры «Уголовное право и криминология» Ташкентского государственного юридического университета, Республика Узбекистан, г. Ташкент
E-mail: intertoto50@gmail.com

THE CRIMINOLOGICAL CHARACTERISTIC OF CRIMES IN THE SPHERE OF INFORMATION (COMPUTER) CRIMES

Abdulaziz Rasulev

candidate of Science, independent competitor of "Criminal law and Criminology" department of Tashkent State Law University, Uzbekistan, Tashkent

АННОТАЦИЯ

В данной статье были проанализированы основные элементы, составляющие криминологическую характеристику преступлений в сфере информационных (компьютерных) преступлений, мнения различных ученых и специалистов, приведены некоторые статис-

тические данные. Определено, что рассматриваемые преступления посягают на информационную безопасность в сфере экономики, политики, социально-духовной сфере, а также обосновано мнение о разработке комплексного подхода по противодействию компьютерным преступлениям.

ABSTRACT

In this article the basic elements making the criminological characteristic of crimes in the sphere of information (computer) crimes, opinions of various scientists and experts were analysed, some statistical data are provided. It is defined that the considered crimes encroach on information security in the sphere of economy, policy, the social and spiritual sphere, and also the opinion on development of an integrated approach on counteraction to computer crimes is proved.

Ключевые слова: компьютерное преступление; информационная безопасность; криминологическая характеристика.

Keywords: computer crime; information security; criminological characteristic.

Понятие компьютерная преступность (или преступность в сфере высоких технологий, преступление в сфере компьютерной информации) наряду с такими понятиями как экономическая преступность, организованная преступность, коррупция, легализация криминальных доходов прочно вошло в понятийный аппарат криминологов и практических работников правоохранительных органов и судов.

В национальной криминологической науке до сих пор не оказывают должного внимания факту наличия и увеличения компьютерной преступности, не достаточно проводятся с учетом современных вызовов и угроз научно-исследовательские работы по криминологической характеристике исследуемых преступлений. До недавнего времени компьютерной преступности, как явлению, не придавали особого значения и в других государствах СНГ, и преступления, совершаемые в сфере компьютерной информации, рассматривались в совокупности с отдельными видами экономической преступности [10, с. 489].

Однако, компьютерная преступность – это бомба замедленного действия колоссальной разрушительной силы. Как отмечает Р. Гасанов: «компьютерные махинации, как правило, остаются незамеченными на фоне кровавой уличной преступности. Даже по неполным оценкам экспертов, эти преступления обходятся человечеству

минимум в 200 млрд. долл. США ежегодно. Банковский грабитель рискует жизнью за 10 тыс. долл., а электронный, манипулируя компьютером и ничем, по сути, не рискуя, может получить миллионы долларов» [5, с. 155]. Как показали многочисленные социологические опросы, проводимые специалистами, для большинства компьютерных преступлений характерны корыстные мотивы, хотя после 70-х годов XX века все больше стали появляться и другие цели (в том числе политические, террористические и т. д.). Было бы неверно думать, что компьютерная преступность охватывает собой только сферу быта, торговли, транспорта и т. д., то есть все то, что в целом составляет экономическую часть деятельности государства. Спектр преступного использования компьютерных технологий практически равен спектру его применения по прямому назначению. Это означает, что преступное вторжение через ЭВМ может быть и в сферу оборонной, космической индустрии, политики и международных отношений [17, с. 28].

В этой связи, автор считает, что компьютерные преступления в криминологическом аспекте следует рассматривать, разделив их по крупным блокам, характеризующим собой отдельные сферы общественной жизни. В частности, речь идет о преступных посягательствах на информационную безопасность в сфере экономики, политики, социально-духовной сфере. На взгляд автора, считается целесообразным характеризовать компьютерные преступления как социальное явление, установить закономерность его развития, а также социально опасные последствия, к которым может привести отсутствие мер предупредительного и противодействующего характера. В сфере экономики, в банковской и кредитно-финансовой системе особое распространение получили такие виды компьютерных преступлений как мошенничество, кражи денежных средств, несанкционированный доступ в информационную систему, коммерческий шпионаж. Однако, с развитием финансово-банковской системы особую опасность для Узбекистана представляют такой вид компьютерного преступления как кардинг [15, с. 25–28] (компьютерное мошенничество с электронными пластиковыми карточками). В Республике Узбекистан, стремительно входящей в область мировой электронной торговли, финансов и кредитов, испытывающей новейшие интеграционные процессы в этой сфере, как никогда остро стоит задача обеспечить информационную безопасность в общественных отношениях по поводу функционирования кредитно-финансовых, банковских, информационных систем и баз данных. Это тем более необходимо, принимая во внимание довольно слабые системы защиты в этих учреждениях.

Однако, наибольшая угроза информационной безопасности ощущается в посягательствах, осуществляемых в сфере политических отношений, национальной безопасности, обороны и других важнейших отраслях политической сферы общества. Информационная безопасность общества в настоящее время подвергается серьезным испытаниям в связи с участившимися, особенно в глобальной сети Интернет нападениями и информационными атаками, потенциально способными привнести в жизнь людей хаос, панику, дезориентацию, вплоть до полного подавления здорового общественного сознания. В подтверждение слов автора можно привести трагические события в некоторых странах постсоветского пространства – Грузия, Украина, Кыргызстан (тюльпановые и оранжевые революции), «арабская весна» в Северной Африке и Ближнем Востоке, – когда агрессивная группа религиозных экстремистов делала свое черное дело, убивая невинных людей, взрывая и внося разрушения, на население стран буквально обрушилась дезинформационная, откровенно клеветническая атака, особенно в Интернете велась информационная война с целью попытки дискредитации в глазах населения авторитета власти, правоохранительных органов, вызова недоверия к властям и их, якобы, бессилия против «народной воли».

В глобальных сетях имеется огромное число экстремистских сайтов, где нередко ведется информационная пропаганда соответствующих антиобщественных взглядов и идей, публикуются призывы к свержению законных органов власти, к силовому захвату власти и другие. Многие развитые страны всерьез обеспокоены возможностью крупных терактов в информационном пространстве, в частности против объектов энергетики, телекоммуникаций, авиационных служб, правительственных структур и военных объектов, могущих блокировать деятельность целых отраслей, крупных предприятий, парализовать службу правительственных органов, спровоцировать техногенные катастрофы, аварии, вызвать панику среди населения, привести к другим деструктивным результатам.

В стране имеются стратегически важные объекты, где ведутся исследования секретного характера. Они представляют определенный интерес для компьютерных преступников, специализирующихся на компьютерном шпионаже. Информация о состоянии защищенности этих объектов закрыта для исследования, но по мнению автора, существует потенциальная опасность для информационных систем объектов и необходимость более тщательной их защиты.

Распространенным и прибыльным является компьютерный шпионаж, осуществляемый в наиболее наукоемких и дорогостоящих

сферах обороной деятельности: научных исследованиях, создании новых видов оружия и военной техники, сложных технологических процессах и т. д.

В социально-духовной сфере компьютерные преступления посягают на не менее важные и значимые объекты уголовно-правовой охраны – честь и достоинство личности, нравственные и духовные устои общества, право личности на интеллектуальное творчество и его плоды. Возможность анонимности, широкий охват аудитории, несовершенство механизмов уголовного преследования в глобальных сетях способствует распространению в информационном пространстве таких опасных преступных деяний, как клевета, возбуждение ненависти или вражды из расовых, национальных и иных побуждений, нарушение неприкосновенности частной жизни и т. д. Особую тревогу вызывают факт, что в компьютерных сетях практически беспрепятственно распространяются материалы, содержащие порнографию, в том числе с изображением несовершеннолетних и детей. По оценкам специалистов, в сети Интернета насчитывается более ста тысяч сайтов, имеющих отношение к детской порнографии [7, с. 120–128]. Массовое распространение во всем мире получило компьютерное пиратство. По данным Ассоциации производители компьютерного обеспечения, уровень компьютерного пиратства в России составляет 90–94 %, в Германии – 50 %, В США – 35 %, в Швейцарии – 28 %, в Лихтенштейне – 18 %, в Китае – 98 % [16, с. 9]).

Таким образом, компьютерная преступность – это сложная совокупность нескольких десятков составов преступлений, предусмотренных различными разделами уголовного закона (хищение, несанкционированный доступ, компьютерная фальсификация и мошенничество, компьютерное пиратство, компьютерный шпионаж, компьютерный терроризм и т. д.), а также не представленных пока в уголовном законе, в большинстве своем, связанных с неправильным использованием информационных ресурсов Интернета.

Латентность компьютерных преступлений весьма велика. Незначительность судебно-следственной практики и руководящих указаний Верховного суда Республики Узбекистан по применению норм уголовного законодательства в этой сфере, зачастую приводят к тому, что даже в случаях явного ущерба общественным отношениям, интересам личности, общества и государства, принятие юридического решения весьма затруднительно.

Кроме того, данное явление может диктоваться, на взгляд автора, следующими обстоятельствами во-первых, компьютерные или преступления в сфере информационных технологий, представляя

собой один из самых высокотехнологичных видов преступлений, создают большие сложности при их выявлении и раскрытии; во-вторых, не все потерпевшие – особенно частные структуры, обращаются в правоохранительные органы (из-за боязни раскрыть свои коммерческие секреты, возможной утечки информации о незащищенности, а порой и с целью скрыть махинации) [2, с. 4]; в-третьих, недостаточная степень правовой регламентации, несомненно, влияет на то, что большинство криминальных деяний не подвергнуты криминализации. Помимо этого, несоответствующая в достаточной степени современным вызовам и угрозам в уголовном законодательстве норм, регулирующих соответствующие правоотношения, приводит к тому, что следователи нередко квалифицируют компьютерные преступления по ст. УК Республики Узбекистан, предусматривающего ответственность за обычные преступления, игнорируя совершение этих преступлений с использованием компьютерных средств [18]. Это также приводит к искажению статистических данных о количестве совершаемых компьютерных преступлений.

Трансграничный (транснациональный) характер компьютерных преступлений представляет серьезную проблему для правоохранительных органов. Эта особенность многих компьютерных преступлений обуславливает отмечаемое специалистами постоянное усложнение в международном масштабе правовых и технических проблем, связанных с обнаружением и идентификацией преступников, проведением расследований и судебных преследований по фактам трансграничных компьютерных преступлений [6, с. 245]. Серьезные проблемы возникают относительно того, в соответствии с законом какого государства должно нести ответственность лицо, совершившее преступление, находясь в одном государстве, в то время как объект преступного посягательства располагается в другом. Как замечают эксперты «реальные пространства сжимаются в виртуальной реальности, и совершенно бессмысленно выстраивать в ней государственные границы» [4, с. 15]. Соответственно, применение к возникающим в глобальной сети правоотношениям локальных правовых норм внутреннего законодательства не может быть эффективно без учета и связи с законодательством других стран, международным правом.

Компьютерная преступность, в значительно большей степени, чем общеуголовная, способна составлять образ жизни значительной части населения и формировать полукриминальный менталитет. Количество преступлений в сфере компьютерной информации стремительно растет по мере развития телекоммуникационных сетей и увеличения числа персональных компьютеров. По данным

ЮНЕСКО сохраняется позитивная динамика развития телекоммуникационных систем. В частности, с 1995 по 2000 гг. число телекоммуникационных линий увеличилось в США с 165 тыс. до 199 тыс., в ФРГ – с 41 тыс. до 51 тыс., в Китае – с 41 тыс. до 141 тыс., В России – с 25 тыс. до 35 тыс. За это же время было инвестировано в развитие этой сферы в США – 51 млрд. долл., в ФРГ – 16 млрд. долл., в Китае – 302 млрд. долл., в России – 8 млрд. долл. [8, с. 12]. Распространенность компьютерных преступлений обусловлена расширением сферы применения средств ЭВМ, ростом доверия к автоматизированным системам обработки данных. Ныне ЭВМ управляют технологическими процессами на предприятиях и АЭС, движением самолетов и поездов, контролем финансовых потоков, обрабатывают секретную информацию. В этих процессах участвует большое количество людей, удобность несанкционированного доступа к информационным системам в силу своей относительной простоты, скоротечности, анонимности, отсутствия непосредственного контакта с объектом преступления, подвигает людей к совершению такого рода преступлений. Например, четыре из пяти преступлений, расследованных ФБР США, имели отношение к неправомерному доступу [3, с. 49].

Важно учитывать социально-психологические условия, в которых ведется расследования. Настрой общества по отношению к информационным преступлениям, под воздействием СМИ периодически меняется. Это обстоятельство влияет на поведение участников расследования. Их отношения могут быть совершенно полярны – от полного неприятия преступных действий, повлиявших на интересы некоторых слоев общества в конкретной стране, до возвеличивания отдельных преступников. В судах и СМИ к компьютерным преступникам редко подходят с той же строгостью, как и к лицам, совершившим обычные преступления, в действительности их часто превращают в героев [1, с. 19].

Вынуждены отметить, что правовая культура общества, не достаточная осведомленность о криминальности подобных деяний, о существовании в целом компьютерных правонарушений и понимании того, какие последствия это влечет, резко снижает эффективность противодействия компьютерным преступлениям. Компьютерная преступность, нося по своей природе индивидуальный, сущностный признак, тем не менее, в последнее время приобретает более организованный и опасный характер [14, с. 131]. Организованность проявляется как в координации действий технического характера, так и в распределении ролей в группах. В компьютерных преступлениях экономической направленности высока вероятность

сговора с персоналом информационных систем банков, финансовых учреждений и структур, что позволяет эффективно скрыть следы преступной деятельности. Нередки случаи, когда членом группы являются бывший сотрудник фирмы, хорошо осведомленный о системе кодов и паролей.

Организованные преступные группировки часто используют Интернет не только для осуществления преступной деятельности, но и для проведения разведки противодействующих мер против правоохранительных органов, поиска жертв и оказания на них давления. В последнее время наметился еще один политический оттенок в деятельности организованных групп – поддержка, в том числе финансовая, антигосударственных процессов, течений и подобного рода организаций [11, с. 55]. Политизация организованной преступности, замешанной на национализме и экстремизме, с учетом доступа к глобальным коммуникациям, представляет серьезную опасность. Ярким примером могут выступать события в Грузии, Кыргызстане, Украине.

Важную роль в усложнении борьбы с компьютерной преступностью играет интеллектуализация и профессионализация криминалитета. В результате расслоения общества, сохранения относительно высокой безработицы, сокращения государственных предприятий и учреждений в криминальную сферу вытесняется значительное число высококвалифицированных специалистов в области ИТ [13, с. 465]. Они широко используют в преступной деятельности, полученной ими ранее профессиональные навыки и знания, выполняя криминальные заказы по взлому либо изготовления специальных приспособлений, облегчающих несанкционированный доступ или перехват информации. Можно отметить в связи с этим, что согласно доклада ASIS о проблемах компьютерного шпионажа, 40 % всех атак на компьютерные системы исходят от «чужаков – одиночек», 20 % – от своих людей, действующих в сговоре с посторонними лицами, а остальные 40 % приходятся на сотрудников организаций, действующих на свой страх и риск [12, с. 90]. Поскольку львиная доля брандмауэров – выделенных компьютеров, предназначенных для подключения различных сетей к Интернет и обеспечивающих защиту от несанкционированного доступа, обеспечивают защиту только от посторонних компьютерных взломщиков, большинство этих атак нельзя предотвратить, так как в них участвуют «свои».

Мнения некоторых специалистов о том, что в Узбекистане нет компьютерной преступности, а значит, нет необходимости в превентивных мерах, на взгляд автора, глубоко ошибочны. На деле, компьютерная преступность в Республике Узбекистан имеется,

но в силу латентности и в связи с тем, что она еще не достигла заметных масштабов, она на фоне обычных преступлений теряется. Следует отметить, что волна компьютерной преступности, бушевавшая в США и Канаде, странах ЕС и АТР, а в настоящее время бушующая в странах СНГ-России, Украине, Казахстане непременно скажется и в Узбекистане, это лишь вопрос ближайшего времени. Компьютеризация буквально всех отраслей, быстрое развитие интеграционных процессов, широкое открытие информационно-телекоммуникационных каналов, переход финансово-кредитной системы и системы государственных органов от бумаготворчества к электронному документообороту, электронным средствам платежей – это объективные процессы, которые необходимы для поступательного и динамичного развития Узбекистана. Однако, эти благоприятные тенденции, не сопровождаются соответствующим укреплением систем защиты информации, своевременным принятием упреждающих нормативно-правовых актов, регламентирующих обеспечение безопасности информационных систем. Кроме того, кадровый потенциал правоохранительных органов требует дальнейшего совершенствования, а соответствующие уголовно-правовые нормы – требуют дальнейшей модернизации по пути к полноценной охране информации и информационных систем.

Это указывает о том, что Узбекистан стоит на пороге «всплеска» компьютерной преступности. В подтверждение мнения автора, обратимся к российской статистике. В 1997 г. в России было зарегистрированы 17 преступлений в сфере компьютерной информации, в 1998 г. – 67, в 1999 г. – 284, а в 2000 г. – 748 преступлений [14, с. 133], т. е. каждый последующий год количество преступлений растет, в среднем, в 4 раза. По информации экспертно-аналитических кругов, на данный момент в России совершается несколько тысяч преступлений только за один квартал сего года. Причем нарастание здесь идет значительно быстрее, чем по другим видам преступлений. Подобная картина наблюдается практически во всех промышленно развитых странах.

Однако, по мнению автора, совершенно справедливы утверждения некоторых специалистов, что криминологические прогнозы должны быть все же преимущественно не количественными, а качественными [9, с. 21]. Основными тенденциями качественного изменения компьютерных преступлений, на взгляд автора, следует выделить следующие (с учетом критической оценки состояния нормативно-правовой базы, необходимости совершенствования правоохранительных органов и их кадров, увеличения технической оснащенности производственных и непроизводственных отраслей,

интенсификации интеграционных процессов, увеличения доли владельцев персональных компьютеров) – дальнейший рост организованности и профессионализма компьютерных преступников, усложнение способов совершения этих преступлений и сокрытия их следов, заимствование преступными элементами новейших «достижений» у своих зарубежных собратьев (рост криминального интернационала), сохранение высокого уровня латентности; увеличение доли несовершеннолетних преступников, повышение общественной опасности компьютерных преступлений.

Следует отметить, что в случае, если не будет нового комплексного подхода в юридической науке по решению вопросов противодействия компьютерным преступлениям, дальнейших современных системных преобразований в данной сфере, и борьба с компьютерной преступностью будет вестись правоохранительными органами без широкого привлечения общественности, позитивных изменений в криминогенной ситуации в ближайшее время не произойдет, скорее наоборот, будет наблюдаться резкий рост компьютерных правонарушений, а информационная безопасность общества будет поставлена под определенную угрозу.

Принимая во внимание, что в Узбекистане ведется широкомасштабная работа по совершенствованию общественно-политической, социально-экономической и судебно-правовой сферах, а также дальнейшей модернизации государственных программ, в том числе по противодействию компьютерной преступности, включающей в себя весь комплекс правовых и организационно-технических, социальных вопросов, борьба с компьютерной преступностью может быть более эффективной.

Список литературы:

1. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М.: МИР, 1999. – 90 с.
2. Андреев В.А., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. – М.: Юрлит Информ, 2001. – 182 с.
3. Анин В. Наиболее серьезные нарушения в области информационной безопасности в 1996 году // – Ж. Конфидент – 1997. – № 6. – С. 48–52.
4. Волчинская Е.К. Есть ли в России компьютерное право? // – Ж. Юридический консультант. – 1997. – № 2. – С. 14–16.
5. Гасанов Р.М. Шпионаж особого рода – М.: Юридическая литература, 1989. – 288 с.

6. Горяинов К.К., Исеченко А.П., Кондратюк Л.В. Транснациональная преступность: проблемы и пути решения – М.: ИНФРА–М, 1997. – 386 с.
7. Джейсон Т. Порнография в Интернете // Компьютер-Пресс, 1998. – № 3. – С. 120–128.
8. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др. Под общ. ред. А.В. Федорова, В.Н. Цигичко. – М.: ПИР- Центр, 2001. – 160 с.
9. Клейменов М.П., Харитонов А.М. Прогнозирование преступности / Лекция – Омск, 1995. – 120 с.
10. Криминология: Учебник для юрид. вузов / под общей ред. Долговой А.И. – М.: Инфра-М, 1997. – 612 с.
11. Курбанали Таджибаев Организованная преступность (учебно-методическое пособие) / ТГЮИ Ташкент, 2004 – 102 с.
12. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность – М.: Новый Юрист, 1998. – 180 с.
13. Лунев В.В. Преступность XX века: мировые, региональные и российские тенденции. – М.: МОСКВА, 1997 – 576 с.
14. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. – М.: Норма, 2004. – 188 с.
15. Осташева Н.А. Carding: реальное мошенничество в виртуальном мире // – Ж. ЮРИСТ – 1999. – № 4 – С. 25–28.
16. Симкин Л.С. Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства) – М.: Городец, 1998. – 92 с.
17. Толеубекова Б.Х. Социология компьютерной преступности – Караганда, 1992. – 122 с.
18. Уголовный кодекс Республики Узбекистан // – [Электронный ресурс] – Режим доступа. – URL: http://www.lex.uz/ (Дата обращения 17.02.16).