УДК 343.3/.7
ББК 67.408.1

В.В. Хилюта,
кандидат юридических наук, доцент,
Гроднинский государственный университет им. Я. Купалы
(Республика Беларусь)

НЕОБХОДИМОСТЬ УСТАНОВЛЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

В статье рассматриваются вопросы квалификации хищений, совершаемых с использованием компьютерной техники. Автором обосновывается необходимость введения самостоятельной уголовной ответственности за «компьютерное хищение» и предлагается вариант данной уголовно-правовой нормы.

Ключевые слова: хищение; компьютерное мошенничество; хищение с использованием компьютерной техники.

V.V. Khilyuta,
Ph.D. in Law, Ass. Professor,
Yanka Kupala State University of Grodno (The Belarus Republic)

THE NECESSITY OF ESTABLISHING CRIMINAL LIABILITY FOR LARCENY COMMITTED WITH THE AID OF COMPUTER EQUIPMENT

The paper examines the qualification of larceny committed with the aid of computer equipment. The author proves the necessity of introducing a separate criminal liability for computer larceny and offers a variant of such a criminal law norm.

Key words: larceny; computer fraud; larceny with the aid of computer equipment.

Вторая половина XX века с бурным развитием информационных технологий принесла с собой качественный скачек: информация превратилась в один из главных элементов национального богатства. Совершенствование компьютерных технологий все более приближает нас к тому времени, когда значительная доля информационных ресурсов будет содержаться в технических средствах. Пожалуй, сегодня практически нет ни одной сферы человеческой деятельности, в которой бы не использовались компьютеры, позволяющие создавать, накапливать, хранить, обрабатывать и передавать огромные объемы информации [11, с. 5; 15, с. 2–3]. Создание электронно-вычислительной техники большой производительности, ее широкое внедрение в экономическую, социальную и управленческую деятельность привело к повышению значимости информации и информационных ресурсов.

В то же время динамичное внедрение новейших электронных систем и коммуникационных средств в различные сферы деятельности современного общества привело не только к развитию положительных тенденций, но и повлекло целый ряд проблем негативного характера. Всевозможные явления всеобщей криминализации сопровождаются массой негативных факторов, связанных со злоупотреблениями возможностями компьютерной техники. Многочисленные случаи выявления и установления закономерностей механизмов развития новых видов преступлений, связанных с использованием средств компьютерной техники и информационных технологий, показывают, что сама компьютерная техника может быть как предметом преступного посягательства, так и инструментом совершения преступления.

Условно подобного рода противоправные деяния можно разбить на несколько групп:

– преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых;

– преступления, направленные на получение несанкционированного доступа к ком-

пьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т. д., т. е. компьютерная информация является объектом преступного посягательства;

– преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве орудия или средства совершения корыстного преступления и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации.

В данном случае критерием разграничения предмета, орудия и средства совершения преступлений в сфере компьютерной информации является характер использования различных предметов в процессе совершения преступления. Поэтому следует различать компьютерную информацию, на которую осуществляется неправомерное воздействие (такая информация считается предметом преступления), и компьютерную информацию, которая служит орудием совершения преступления и с помощью которой осуществляется неправомерное воздействие на предмет преступления (например, денежные средства). В качестве предмета преступления в сфере компьютерной информации могут выступать различные банки данных, объекты авторского права, государственная, банковская, коммерческая тайны, персональные данные, тайна частной жизни и т. д. В роли же орудия совершения преступления в сфере компьютерной информации выступают команды, вводимые с клавиатуры или с помощью звуковых сигналов, различного рода «вирусные» и «троянские» программы, а также иная информация, способная осуществить неправомерное воздействие на предмет преступления против собственности [3, с. 12]. Специфические особенности орудия совершения преступления заставили многих утверждать о своеобразном способе совершения преступлений против собственности с использованием средств компьютерной техники.

Иными словами, при совершении хищения с использованием компьютерной техники можно говорить о том, что применяется новая совокупность приемов, методов, последовательности действий, которая придает преступлению уникальные свойства, не характерные для других имущественных преступлений.

Таким образом, компьютерная техника может являться как способом, так и средством совершения преступления. Двойственность значения в данном случае возможна благодаря самой природе компьютерной техники. Применительно к последней группе противоправных деяний, в законодательстве ряда зарубежных государств специально выделяются составы преступлений, охраняющие имущественные отношения от преступных посягательств, совершаемых с использованием компьютера.

Так, уголовное законодательство *США*, посвященное борьбе с компьютерными преступлениями, отличается своеобразием и постоянным обновлением. Основной закон США, касающийся компьютерных преступлений, был сформулирован в 1986 г. «О мошенничестве и злоупотреблениях, связанных с компьютерами», а впоследствии состав «мошенничества с использованием компьютеров» вошел в Свод законов США. В параграфе 1030 (а) (4) Свода законов США мошенничество с использованием компьютера определяется как доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени (т. е. бесплатное использование компьютерных сетей и серверов) стоимостью более 5 тыс. долларов США в течение года, т. е. без оплаты использования компьютерных сетей и серверов [13, с. 51].

В *Великобритании* ответственность за компьютерные преступления установлена в статутах, принятых Парламентом. К основным актам, устанавливающим ответственность за компьютерные преступления, можно отнести: Закон о злоупотреблениях компьютерами 1990 г., Закон о телекоммуникациях (обмане) 1997 г., Закон о защите данных 1998 г., Закон об электронных коммуникациях 2000 г. и др. Однако из перечня основных компьютерных преступлений специально не выделяется состав «компьютерного мошенничества», связанного с посягательством на чужое имущество. Как следует из содержания Закона 1990 г., к злоупотреблению компьютером законодатель относит: незаконный доступ к компьютерным материалам; незаконный доступ к

компьютерным материалам с намерением совершить или облегчить совершение другого преступления; незаконную модификацию компьютерных материалов [6, с. 31–32].

Среди законодательных актов *Японии,* регулирующих правоотношения в сфере информационных технологий, следует назвать Уголовный кодекс и Закон «О несанкционированном проникновении в компьютерные сети» 2000 г. Согласно ст. 246-2 УК Японии за компьютерное мошенничество наказывается «любое лицо, изготавливающее фальшивые электромагнитные записи, свидетельствующие о приобретении, изменении или потере имущественных прав, путем внесения в компьютер, используемый в деловых операциях иным лицом, ложных сведений или команд либо пускающее фальшивые электромагнитные записи в обращение в ходе деловых операций другого лица, и получающее от этого незаконный доход либо способствующее получению незаконного дохода третьим лицом». В соответствии с Законом «О незаконном проникновении в компьютерные сети» особо следует выделить такое правонарушение, как незаконное (несанкционированное) проникновение в компьютерные системы и информационные сети с целью кражи, порчи информации, ее использования с целью извлечения дохода и причинение ущерба законным владельцам сетей, систем и информационных баз данных [13, с. 49-51].

Ответственности за компьютерное мошенничество согласно параграфу 263а УК *ФРГ* подлежит лицо, которое, «действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействуя на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, путем неправомочного использования данных или иного неправомочного воздействия на процесс обработки данных». В данном случае компьютер используется как орудие совершения преступления, поскольку указанные в § 263а УК ФРГ формы реализации объективной стороны выступают именно в качестве способов достижения корыстной цели [10, с. 110–118]. Таким образом, немецкий законодатель четко разграничил два вида мошенничества: традиционное и компьютерное. Суть же компьютерного мошенничества заключается в том, что обману подвергается не человек, а программа, поскольку ущерб имуществу причиняется воздействием на процесс переработки информации и путем неправильного установления программы, использования неверных или неполных данных, а также путем неправомочного использования данных или неправомочного воздействия на процессы переработки данных [7, с. 463].

Уголовный кодекс *Франции* включает различные составы большого числа компьютерных преступлений: посягательства на деятельность по обработке данных автоматизированных систем; посягательства, связанные с использованием карточек и обработкой данных на ЭВМ; незаконные действия, совершаемые с компьютерной информацией в ущерб интересам государства, и т. д. Однако специально УК Франции не выделяет состав, посвященный охране имущественных отношений, посягательства на которые осуществляются с использованием компьютерной техники [9, с. 11]. В то же время нормы французского УК защищают сами информационные системы и их программное обеспечение как объекты собственности.

В соответствии со ст. 287 УК *Республики Польша* специфическим имущественным преступлением признаются действия лица, которое «с целью получения имущественной выгоды или причинения другому лицу вреда, не имея на то права, влияет на автоматизированное преобразование, собирание или передачу информации или изменяет, удаляет либо вводит новую запись на компьютерный носитель информации» [14]. Следует также отметить, что польский законодатель пошел по пути разделения компьютерных преступлений на две самостоятельные группы в зависимости от того, на что было направлено деяние субъекта – на получение информации или на получение имущественной выгоды.

В *Российской Федерации* в УК отсутствует специальная норма, предусматривающая ответственность за совершение «компьютерного хищения», и правоприменительная практика исходит из того, что хищения, совершаемые с использованием компьютерной техники, в ряде случаев рассматриваются либо как мошенничество, либо как кража по признаку незаконного проникновения в помещение либо в иное хранилище. Кроме этого такого рода противоправные действия дополнительно влекут уголовную ответственность по ст. 272 УК РФ [2, с. 80; 5, с. 32].

Таким образом, можно сказать, что развитие уголовного законодательства ряда государств по рассматриваемому вопросу происходит в трех направлениях: а) применяется более широкое толкование традиционных норм о преступлениях против собственности, и их правоприменение происходит по аналогии применительно к хищениям, совершаемым с помощью компьютеров (применение компьютерной техники во всех случаях предлагается рассматривать как средство, облегчающее совершение преступления); б) применение специальных квалифицирующих обстоятельств в общих нормах о преступлениях против собственности, где компьютерная техника выступает лишь как обозначенное средство основного способа хищения и не оказывает влияния на предусмотренный УК способ достижения преступной цели; в) применяются специальные нормы о компьютерных хищениях (здесь использование компьютерной техники рассматривается как отдельный способ достижения преступной цели).

В этой связи практика применения уголовного законодательства по делам о компьютерных хищениях свидетельствует о том, что возникающие в этой сфере проблемы обусловлены несовершенством уголовно-правовых норм, противоречивостью их толкования, отсутствием научно-методических рекомендаций и официальных руководящих разъяснений по квалификации компьютерных хищений. Применение к подобного рода деяниям традиционных норм о краже, присвоении либо растрате, мошенничестве и т. д. является не вполне удачным и допустимым в силу следующих обстоятельств.

1. Вряд ли можно говорить о том, что при неправомерном злоупотреблении с автоматизированными системами обработки данных присутствует обман, – компьютер, как и замок у сейфа, нельзя обмануть, поскольку технические устройства лишены психики [4; 8, с. 42] (замок не идентифицирует владельца ключа или отмычки как законного владельца имущества). «Обман компьютера» – понятие несколько эфемерное, потому что компьютер – это всего лишь механизм, и обмануть его в принципе невозможно. Кроме того, само понятие обмана предполагает, что потерпевший (собственник) вследствие применения к нему обмана сам выводит имущество из своего владения, т. е. «добровольно» передает его преступнику, предоставляя последнему в отношении имущества правомочия владения, пользования и даже распоряжения [1, с. 28]. В такой ситуации имеет место не обман собственника (владельца) имущества, а «обман» компьютерной системы. Подобный обман не характерен для мошенничества, поскольку он используется не для завладения чужим имуществом, а для облегчения совершения хищения путем получения доступа к компьютерной системе. А в таком случае, когда происходит воздействие на компьютерную систему с мошенническими намерениями, уместно говорить о манипуляциях, а не об обмане.

2. Не вполне обоснованно рассматривать такого рода хищения как кражу, ввиду того, что в компьютерной системе не хранятся вещи, денежные средства или иное имущество, на которые посягает преступник, в компьютерной системе хранится информация об этом имуществе или его передвижении. И если виновное лицо проникает в компьютерную систему с целью завладения денежными средствами либо иного имущества, то оно проникает в компьютерную систему путем манипуляций с программами, данными либо техническими средствами. Таким образом, лицо для совершения имущественного преступления умышленно искажает либо вносит ложные данные в компьютерную систему, манипулирует с программами, данными, аппаратной частью ЭВМ, обрабатывающими информацию о передвижении имущества, и тем самым добивается получения разрешения на использование имущества.

3. По тем же основаниям необоснованным будет выглядеть включение в состав кражи или мошенничества квалифицирующего признака «с использованием компьютерных технологий» или других («мошенничество, совершенное путем незаконных операций с использованием электронно-вычислительной техники», «с использованием результата автоматизированной обработки данных»). Хищение с использованием компьютерной техники не является частным случаем мошеннического обмана или кражи, поскольку при хищениях с использованием компьютерной техники выдаваемые ЭВМ команды и документы ничем не отличаются от подлинных по форме, являясь фальшивыми по сути. Лицо, работающее с системами автоматизированной обработки информации, объективно поставлено в такие условия, что

оно будет добросовестно заблуждаться относительно полученной информации (независимо от того, была ли она видоизменена или вовсе являлась ложной) ввиду отсутствия какого-либо контакта с виновным.

Очевидно, что применение таких терминов как «компьютерное мошенничество», «компьютерная кража» является юридической фикцией, поскольку ни одна из существующих форм хищений сегодня не отражает в полной мере той специфики общественных отношений, которые подвергаются посягательствам, совершаемым с использованием компьютерной техники.

Сказанное свидетельствует о том, что хищение путем использования компьютерной техники возможно лишь посредством компьютерных манипуляций. Компьютерное «хищение» предполагает перехват информации, несанкционированный доступ к средствам информации, проведение манипуляций с данными и управляющими командами. При манипулировании с процессами ввода, вывода информации компьютер согласно заложенной в него программе идентифицирует преступника как законного владельца денежных средств. Преступник не сам тайно изымает эти деньги, а компьютер, банкомат, другое электронное устройство передает их ему, внешне добровольно, но в связи с ошибкой в программе, которую сознательно вносит в эту программу виновный [12]. Завладение чужим имуществом в данном случае может происходить путем ввода, изменения, удаления или блокирования компьютерных данных либо путем другого вмешательства в функционирование компьютерной системы.

Таким образом, суть хищения, совершаемого с использованием средств электронной техники, состоит в модификации автоматизированной обработки данных компьютерной системы, в результате чего происходит воздействие на результат вводимой и выводимой информации, и как следствие этого видоизменяется информация о переходе имущества либо прав на имущество собственника или иного законного владельца. Такого рода модификация представляет собой: а) изменение информации, обрабатываемой в компьютерной системе, хранящейся на материальных носителях (машинных, пластиковых) или передаваемой по сетям передачи данных; б) введение в компьютерную систему заведомо ложной информации.

Безусловно, можно сказать, что хищение путем использования компьютерной техники в чем-то схоже с кражей и мошенничеством, однако в отличие от названных составов преступлений противоправное деяние виновным осуществляется путем информационного воздействия не на человека, а на компьютерную систему, которая и принимает решение о совершении тех или иных операций (как бы, с одной стороны, завладение происходит тайно, а с другой – вроде используется и обман). Вот почему при квалификации хищений, совершаемых с использованием компьютерной техники, должны учитываться не составные элементы этой самой техники, и даже не всегда ее использование (поскольку использование компьютерной техники может выступать как средство для совершения хищения), а воздействие на результат автоматизированной обработки данных в целях завладения чужим имуществом.

В настоящее время информационные технологии включают в себя и автоматизированный (машинный) элемент обработки информации, и социальный (человеческий), который является определяющим в данной системе и от которого непосредственно зависит развитие той или иной технологии, применяемой для решения конкретной задачи. Такая специфика обусловливает и необходимость введения самостоятельной уголовной ответственности за имущественное посягательство на отношения собственности с использованием специфического информационного способа совершения преступления – хищения с использованием компьютерной техники.

В заключение отметим, что сегодня перед современными учеными-правоведами поставлена проблема конкретизации рассматриваемого способа имущественного преступления. Принимая во внимание, что к компьютерным преступлениям должны относиться только противозаконные действия в сфере автоматизированной обработки информации, полагаем, что УК должен содержать норму, которая бы предусматривала ответственность за «*хищение имущества путем модификации результатов автоматизированной обработки данных компьютерной системы*». Предполагаемой нормой охватывались бы противоправные деяния, совершаемые с использованием средств компьютерной техники, сотовой связи, сети Интернет, поддельных банковских пластиковых карточек и т. д.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Борунов О.Е.* Проблемы квалификации хищения денежных средств со счетов банка с использованием средств компьютерной техники // Российский судья. – 2004. – № 6. – С. 28.

2. *Бражник С.Д.* Проблемы совершенствования норм об ответственности за преступления, связанные с компьютерной техникой // Налоговые и иные экономические преступления : сб. науч. ст. – Вып. 2. – Ярославль, 2000. – С. 80.

3. *Воробьев В.В.* Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация) : автореф. дис. … канд. юрид. наук. – Н. Новгород, 2000. – С. 12.

4. *Воронцова С.В.* К вопросу о квалификации преступлений в сфере электронных платежей // Банковское право. – 2009. – № 1.

5. *Гончаров Д.* Квалификация хищений, совершаемых с помощью компьютеров // Законность. – 2001. – № 11. – С. 32.

6. *Громов Е.В.* Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании и ФРГ, Нидерландах, Польше) // Вестник ТГПУ. – 2006. – № 11. – С. 31–32.

7. *Жалинский А.Э.* Современное немецкое уголовное право. – М., 2006. – С. 463.

8. *Клепицкий И.* Мошенничество и правонарушения гражданско-правового характера // Законность. – 1995. – № 7. – С. 42.

9. *Мазуров В.А*. Компьютерные преступления: классификация и способы противодействия. – М., 2002. – С. 11.

10. *Орловская Н.А.* Зарубежный опыт противодействия компьютерной преступности (проблемы криминализации и наказуемости) // Информационные технологии и безопасность : междунар. конф. – Вып. № 1. – Киев, 2003. – С. 110–118.

11. *Панфилова Е.И., Попов А.С.* Компьютерные преступления: междунар. конф. – СПб., 1998. – С. 5.

12. *Петров С.А.* Особенности квалификации хищений, совершаемых с использованием компьютерной техники // Российский следователь. – 2008. – № 15.

13. *Степанов-Егиянц В.* Ответственность за компьютерные преступления // Законность. – 2005. – № 12. – С. 49–51.

14. Уголовный кодекс Республики Польша / под общ. ред. Н.Ф. Кузнецовой. – Минск, 1998.

15. *Ушаков С.И*. Преступления в сфере обращения компьютерной информации: теория, законодательство, практика: автореф. дис. … канд. юрид. наук. – Ростов н/Д, 2000. – С. 2–3.

REFERENCES

1. Borunov O.E. *Rossijskij sud'ya* [Russian Judge]. 2004, no. 6, pp. 28.

2. Brazhnik S.D. *Nalogovye i inye ekonomicheskie prestupleniya* [Tax and Other Economic Crimes]. Yaroslavl, 2000, pp. 80.

3. Vorob'ev V.V. *Prestupleniya v sphere komp'yuternoj inphormatsii (yuridicheskaya kharakteristika sostavov i kvaliphikatsiya) (Cand. Dis. Thesis)*[Crimes in the Sphere of Computer Information (legal characteristics of corpus delicti and qualification (Cand. Dis. Thesis)]. Nizhny Novgorod, 2000, pp. 12.

4. Vorontsova S.V. *Bankovskoe pravo* [Bank Law]. 2009, pp. 1.

5. Goncharov D. *Zakonnost'* [Legality]. 2001, no. 11, pp. 32.

6. Gromov E.V. *Vestnik TGPU* [Bulletin of Tomsk State Pedagogical University]. 2006, no. 11, pp. 31-32.

7. Zhalinskij A.E. *Sovremennoe nemetskoe ugolovnoe pravo* [Contemporary German Criminal Law]. Moscow, 2006, pp. 463.

8. Klepitskij I. *Zakonnost'* [Legality]. 1995, no. 7, pp. 42.

9. Mazurov V.A. *Komp'yuternye prestupleniya: klassiphikatsiya i sposoby protivodejstviya* [Computer Crimes: Classification and Ways of Counteracting]. Moscow, 2002, pp. 11.

10. Orlovskaya N.A. *Inphormatsionnye tekhnologii i bezopasnost'* [Information Technologies and Safety]. Kiev, 2003, pp. 110-118.

11. Panphilova E.I., Popov A.S. *Komp'yuternye prestupleniya* [Computer Crimes]. Saint-Petersburg, 1998, pp. 5.

12. Petrov S.A. *Rossijskij sledovatel'* [Russian Investigator]. 2008, pp. 15.

13. Stepanov-Egiyants V. *Zakonnost'* [Legality]. 2005, pp. 12, pp. 49–51.

14. *Ugolovnyj kodeks Respubliki Pol'sha* [The Criminal Code of the Republic of Poland]. Minsk, 1998.

15. Ushakov S.I. *Prestupleniya v sphere obrashcheniya komp'yuternoj inphormatsii: teoriya, zakonodatel'stvo, praktika (Cand. Dis. Thesis)* [Crimes in the Sphere of Computer Information: Theory, Legislation, Practice (Cand. Dis. Thesis)]. Rostov-on-Don, 2000, pp. 2–3.

Информация об авторе

Хилюта Вадим Владимирович (Гродно, Республика Беларусь) – кандидат юридических наук, доцент, заведующий кафедрой уголовного права и криминологии. Гроднинский государственный университет им. Я.Купалы, Республика Беларусь (230005, Республика Беларусь, Гродно, ул. Дзержинского, 131, e-mail: tajna@tut.by)

Information about the author

Khiluta, Vadim Vladimirovich (Grodno, the Belarus Republic) – Ph.D. in Law, Ass. Professor, Head, Chair of Criminal Law and Criminology. Yanka Kupala State University of Grodno (Dzerdzhinskogo st., 131, Grodno, 230005, Belarus Republic, e-mail: tajna@tut.by)