УДК 343.2/.7

Л.Ф. Татаринова

Университет «Туран», доцент кафедры «Юриспруденции и международного права», руководитель учебно-методического отдела, Республика Казахстан, г. Алматы
E-mail: Dove_2003@mail.ru

Проблемы определения субъективных признаков компьютерных преступлений по законодательству Республики Казахстан

С развитием компьютерных технологий, коммуникационных сетей появляются новые составы преступлений, которые, к сожалению, не предусмотрены действующим Уголовным кодексом Республики Казахстан. Более того, даже имеющиеся в нем нормы вызывают неоднозначное отношение к составу, предусмотренному статьей 227 УК РК, что способствует размытости и нечеткому регулированию правоотношений в сфере компьютерной техники, компьютерной информации и всех имеющихся на сегодняшний день коммуникационных сетей. Данная статья посвящена важным элементам состава преступления, а именно субъективным признакам.
Ключевые слова: компьютерные преступления, вина, мотив, цель, сеть, Интернет, компьютерная информация, неправомерный.

L.F. Tatarinova

Problems of definition of subjective symptoms of computer crime under the laws of the Republic of Kazakhstan

This article discusses the main problem of the definition of subjective symptom computer crimes. Analyzes the norms of the Criminal Code of the Republic of Kazakhstan regulating the fight against computer crime, and suggests ways to improve these standards by specifying the subject of the crime.
Keywords: computer crime, guilt, motive, purpose, network, Internet, computer information, illegal.

Л.Ф. Татаринова

Қазақстан Республикасының заңына сайкес компьютерлік қылмыстардың субъективті белгілерін анықтау мәселелері

Бұл мақалада Қазақстан Республикасының заңы бойынша компьютерлік қылмыстардың субъективті белгілерін негізгі анықтау мәселелері қарастырылады. Компьютерлік қылмыстармен күресу сұрақтарын реттейтін Қазақстан Республикасының қолданыстағы Қылмыстық кодексінің нормалары талданады, ал тағы қарастырылып жатқан қылмыстың субъектісін нақтылығы арқылы көрсетілген нормаларын жетілдіру әдістері ұсынады.
Түйін сөздер: компьютерлік қылмыс, кінә, мотив, мақсат, желі, ғаламтор, компьютерлік ақпарат, құқыққа қайшылық.

Введение. Компьютерные преступления являются относительно «молодым» видом правонарушений, это обусловлено широким распространением компьютерных технологий и не совершенством действующего уголовного законодательства. Сложность профилактики и борьбы с указанным видом преступлений видится в проблемах и спорных вопросах квалификации компьютерных преступлений, это касается как объективных, так и субъективных признаков.

Проблема определения субъективных признаков компьютерных преступлений, на наш взгляд, начинается с определения субъекта и заканчивается определением наличия мотива и целей совершения подобного преступления.

В этой связи актуальность темы представленной статьи не оставляет сомнений, учитывая транснациональный характер компьютерных преступлений.

Основной текст. К признакам, характеризующим субъективную сторону преступления, как известно, относятся вина, мотив и цель преступления, которые дают представление о внутреннем процессе, происходящим в психике лица, его совершающего, отражают связь сознания и воли лица с совершаемым общественно опасным деянием. В соответствии с ч. 1 ст. 19 УК РК «Лицо подлежит уголовной ответственности только за те общественно опасные деяния (действия или бездействие) и наступившие общественно опасные последствия, в отношении которых установлена его вина», а согласно ч. 4 этой же статьи: «Виновным в преступлении признается лишь лицо, совершившее деяние умышленно или по неосторожности» [1].

Так, компьютерные преступления могут совершаться умышленно (с прямым или косвенным умыслом). Виновный осознает, что осуществляет неправомерный доступ к компьютерной информации, предвидит неизбежность или возможность наступления хотя бы одного из указанных в законе последствий и желает их наступления либо не желает, но сознательно допускает эти последствия или относится к их наступлению безразлично. При этом по отношению к действию умысел может быть только прямым, о чем свидетельствует и использование законодателем термина «неправомерный», а к факту наступления последствий – как прямым, так и косвенным [2, с. 50].

На первый взгляд все достаточно регламентировано и не вызывает вопросов, однако если рассмотреть вопрос более детально, то становится очевидно, что данное преступление может быть совершено и с неосторожной формой вины, то есть неосторожная форма вины лица способна проявляться при оценке им правомерности своего деяния, а именно: доступа к ЭВМ, компьютерной информации, а также в отношении неблагоприятных последствий подобного доступа.

Таким образом, одна из особенностей квалификации компьютерных преступлений состоит в сложности установления субъективной стороны состава, поскольку в случае ограбления прохожего нет оснований полагать, что преступник это сделал по неосторожности, а если программист изменил последовательность операторов, в результате чего, например, остановился сборочный конвейер завода, доказать, что имел место умысел (даже если это нетрудно предположить), а не ошибка, практически невозможно.

Это доказывает, что необходимо разработать и внести соответствующие изменения в ст. 227 УК РК в виде примечания.

Кроме того, при квалификации преступлений, предусмотренных ст. 227 УК РК, необходимо решение проблемы отграничения и криминализации неосторожного, а также отграничения невиновного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в коммуникационных сетях и системах ЭВМ.

Что касается мотивов, то их можно классифицировать аналогично криминологической классификации субъектов преступления.

Как уже не раз отмечалось, мотивы и цели преступления являются субъективными факторами, влияющими на выбор средств и приемов достижения целей, способов совершения преступления.

В некоторых случаях мотив и цель являются специальными признаками субъективной стороны умышленных преступлений (например, корыстный мотив при злоупотреблении властью или служебным положением, цель – похищение денежных средств).

В отдельных случаях, предусмотренных Уголовный кодексом РК, мотив и цель преступления являются квалифицирующими признаками состава преступления. В других случаях мотивы могут рассматриваться судом как отягчающие или смягчающие обстоятельства (совершение преступления из корыстных и иных низменных побуждений, совершение преступления вследствие стечения тяжелых личных или иных семейных обстоятельств, под влиянием угрозы или принуждения, либо материальной, служебной или иной зависимости, совершение преступления в состоянии аффекта или невменяемости и другие).

Вместе с тем, для большинства умышленных преступлений мотив и цель не являются необходимым элементом субъективной стороны, однако при расследовании конкретного уголовного дела в каждом случае необходимо выяснить их мотив и цели преступления, так как это имеет важное значение не только для вынесения судом справедливого решения, но и способствует всестороннему и полному раскрытию и расследованию преступления.

Б.Х. Толеубекова характеризует мотивы и цели совершения компьютерных преступлений, исходя из анализа конкретного вида преступления и способа его совершения: «Под компьютерным саботажем понимается умышленное повреждение систем обработки входной информации путем незаконного стирания программ, выведения из строя электронных устройств обработки данных, нанесение повреждений электронным устройством обработки данных. Мотив саботажа – месть работодателю, отказавшемуся от услуг программиста» [3, с. 212].

Также хотелось бы обратить внимание на основные мотивы и цели, которыми руководствуются отдельные категории правонарушителей при совершении неправомерного доступа.

Так, в случае с неквалифицированными пользователями, мотивы и цели отсутствуют полностью. Их действия осуществляются по неведению и могут быть использованы преступниками в основном только в «темную». Как правило, это служащие предприятий, учреждений в отношении и в ущерб интересам, которых были осуществлены преступные действия, а также служащие, работающие с ними в компании.

Для «любителей» характерны хулиганские побуждения, самоутверждение, некоторый исследовательский интерес. Последнее характерно и для «профессионалов, поскольку для выяснения возможностей новых защитных систем и поиска путей их преодоления, а также для «шлифовки» мастерства требуется постоянное участие в этих экспериментах. В качестве мотива может выступить также месть как непосредственно разработчикам программ и средств защиты, так и самим программным продуктам, независимо от их разработчика, если преодоление защиты вызвало определенные сложности.

Целью для «профессиональных» компьютерных преступников является получение материальной выгоды или выполнение иных задач, в том числе связанных с посягательством на национальную безопасность. Это могут быть хищения материальных ценностей, товаров и услуг, денежных средств, продажа конфиденциальной информации, легализация преступных доходов, шпионаж, включая промышленный, терроризм и другие.

Мотивы и цели «пользователей» могут быть самыми разнообразными. Наиболее распространенными из них является месть руководству предприятия, фирмы, гражданам и фирмам, которые являются их клиентами или каким-либо образом зависят от них.

В качестве мотива у данной категории могут выступать также хулиганские побуждения, исследовательский интерес, связанные со стремлением еще глубже изучить программные и аппаратным средства ЭВМ, получение имущественной выгоды и другое.

Известны случаи неправомерного доступа к компьютерным системам и сетям юных любителей электроники и программирования просто из-за любопытства, удовлетворения самолюбия, ложного представления о своем превосходстве над другими программистами, тщеславных амбиций, из-за стремления показать неординарные способности узкому кругу знатоков.

Политические мотивы характерны для экстремистских, радикальных и террористических группировок, поскольку как средство политического протеста или как инструмент политических акций компьютер оказывается необычайно эффективным (особенно если это касается сети Internet).

Кроме того, проникновение в компьютерные сети государственных и коммерческих учреждений может позволить террористам получать компрометирующие сведения об их сотрудниках с целью шантажа и вербовки в качестве пособников и т. д.

Мотивы мести чаще всего характерны для недовольных руководителями служащих, которые, злоупотребляя своим положением, портят системы, допуская к ним посторонних или оставляя их в рабочем состоянии без присмотра, встраивают в программное обеспечение «логические» и «временные» бомбы и т. п. [2, с.60].

Однако, по нашему мнению, независимо от того отсутствовали ли полностью мотивы и цели у неквалифицированных или квалифицированных пользователей, но определенные действия

все же были совершены (например, запись или разглашение данных при незаконном перехвате) и наступили при этом общественно опасные последствия, то данные лица должны быть привлечены к уголовной ответственности. В связи с этим целесообразно Уголовный кодекс РК дополнить нормой, предусматривающей ответственность за запись и разглашение данных при незаконном перехвате, передаваемых по сетям глобальных телекоммуникаций с использованием служебного положения, составляющих государственную, коммерческую или иную тайну.

Далее, рассматривая субъекты преступления, предусмотренного ст.227 УК РК, можно выделить несколько категорий:

1. Лица, осуществляющие неправомерный доступ к компьютерной информации, – ч. 1 ст. 227 УК РК (общий субъект), отвечающие следующим признакам: вменяемое физическое лицо, достигшее 16 лет; любое лицо как работающее в автоматизированной информационной системе или сети либо пользующееся их услугами (законный пользователь), но не имеющее права работы с информацией определенной категории, так и постороннее лицо (лицо не являющееся законным пользователем).

Таким образом, в ч. 1 ст. 227 УК РК не требуется, чтобы лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование. Зарегистрировано несколько случаев, когда преступник вообще не имел каких-либо технических познаний.

Но чаще всего указанное преступление совершается лицами, имеющими достаточно высокую квалификацию, особенно если речь идет о неправомерном доступе к компьютерной информации в системе ЭВМ или сети ЭВМ, так как это требует проведения сложных технологических и информационных мероприятий. Поэтому чем сложнее и «хитрее» способ неправомерного доступа, тем уже круг предполагаемых преступников. В первую очередь, это технический персонал компьютерных систем или сетей, которые пострадали от неправомерного доступа – разработчики автоматизированных систем, их руководители, операторы, программисты, инженеры связи, специалисты по защите информации и т. п.

На наш взгляд, в дальнейшем может произойти снижение возраста уголовной ответственности за данное преступление, так как все чаще (в основном за рубежом) такого рода преступления совершаются несовершеннолетними лицами, не достигшими возраста уголовной ответственности (в основном из хулиганских мотивов и личностных амбиций). При этом источником повышенной опасности являются телекоммуникационные сети. Однако в настоящее время при совершении подобного рода деяний лицом, не достигшим 16 лет, ответственность будет наступать в соответствии с нормами гражданского права, а административная ответственность не установлена.

2. Лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой, – ч. 2 ст. 227 УК РК. В данном случае диапазон лиц, вовлекаемых в совершение данного преступления, может быть достаточно широк. Кроме того, к числу потенциальных преступников можно отнести лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными фобиями. В специальной литературе отмечается, что указанная категория заболеваний вызывается систематическим нарушением информационного режима человека: информационным голодом, информационными перегрузками, сбоями темпритма, неплановыми переключениями с одного информационного процесса на другой, дефицитами времени на настройку, информационным шумом. Изучением этих вопросов в настоящее время занимается отрасль медицины «информационная медицина». В связи с оснащением рабочих мест персональными компьютерами, в целях повышения скорости обработки данных и эффективности использования рабочего времени многие служащие подвергаются технострессу, который может привести к формированию компьютерной фобии. То есть компьютерные преступления могут совершаться лицами, страдающими данным видом психического заболевания. При этом отмечается, что преступные действия указанных лиц в основном направлены на физическое уничтожение или повреждение средств компьютерной техники без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями [4, с. 34-35]. Хотя, на наш взгляд, классификационные критерии выдерживаются не всегда, в юридической литературе предлагается достаточно много таких

классификаций. Например, предлагается следующая классификация:

а) нарушители правил пользования ЭВМ совершают преступления из-за недостаточного знания техники, желания ознакомиться с интересующей их информацией, похитить какую-либо программу или бесплатно пользоваться услугами ЭВМ;

б) «белые воротнички» – так называемые респектабельные преступники: бухгалтеры, казначеи, управляющие финансами различных фирм. Для них характерны: использование ЭВМ в целях моделирования планируемых преступлений, компьютерный шантаж конкурентов, фальсификация информации и т. д. Цель их действий получение материальной выгоды или сокрытие других преступлений;

в) «компьютерные шпионы» – хорошо подготовленные в техническом отношении специалисты, целью деятельности которых является получение стратегически важной информации в различных областях;

г) хакеры («одержимые программисты») – наиболее технически и профессионально подготовленные лица, отлично разбирающиеся в вычислительной технике и программировании. Их деятельность направлена на несанкционированное проникновение в компьютерные системы, кражу, модификацию или уничтожение имеющейся в них информации. Зачастую они совершают преступления, не преследуя при этом прямых материальных выгод [5, с. 234].

С появлением первых компьютерных преступлений возникла такая группа преступников, как хакеры. Хакер (от англ. – рубить, кромсать, разрубать), т. е. в буквальном переводе – рубщик, взломщик. Первоначально так называли программистов, которые при переходе на новую машину предпочитали не разбираться с уже установленными на ней программами, а все стереть («вырубить») и поставить новые, по своему усмотрению, программы. Постепенно термин распространился на всех фанатиков компьютеров, и среди них произошла специализация, т.е от вида деятельности хакеры подразделяются на несколько групп:

1. Крекеры – взломщики компьютерного обеспечения. Они взламывают защиту программ от неоплаченного использования. Это самая многочисленная группа хакеров, и ущерб от их деятельности измеряется миллионами долларов. Для коммерческого программного обеспечения это наиболее опасные враги. Если они имеют интерес во взломе того или иного программного обеспечения, то рано или поздно он будет сломан, несмотря на степень сложности защиты. Постоянным «рабочим инструментом» крекеров является программа-взломщик, с помощью которой злоумышленник получает доступ к системе.

2. Фрикеры – люди, предпочитающие альтернативные варианты оплаты теле- и прочих коммуникационных услуг. В основном занимаются обманом АТС: бесплатное пользование межгородом; если стоит блокиратор – организация оплаты абонентских услуг соседом вместо себя и т. д. К сфере действия фрикеров также можно отнести и т.н. «коробки» – специальные электронные устройства, выполняющие какие-либо специфические функции. Например, «световая коробка» позволяет управлять сигналами светофора; на телефонах с тоновым набором – позволяет не оплачивать разговор и т. д.

Однако с уголовно-правовой точки зрения не всякий фрикинг является компьютерным преступлением, например, подключение к телефонной линии абонента; сканирование радиоволны без шнурового телефона и т. п. При наличии необходимых признаков такие действия подпадают под обычное мошенничество, доказать которое весьма проблематично.

3. Картеры (разновидность фримеров) – оплачивают свои расходы с чужих кредитных карточек. Эта разновидность хакеров не так велика, так как для того чтобы успешно заниматься «кардерством», нужны глубокие познания в области радиоэлектроники и программирования микросхем.

4. Сетевые хакеры – в других источниках «информационные путешественники». Эта категория – разновидность фрикеров, появившаяся в связи с развитием сетевых технологий. Услуги провайдеров были довольно дорогими, и поэтому многие компьютерщики пытались пользоваться доступом нелегально, используя различные «дыры» в программных технологиях. Среди сетевых хакеров есть и бескорыстные профессионалы, и те, кто продает свою работу за деньги [6, с. 108-109].

В зависимости от мотивов; целей и методов действия всех хакеров можно подразделить на: некриминальных и криминальных хакеров, и в каждой из указанных выше групп выделить:

1. Хакеров-дилетантов, преследующих одну из трех целей: добиться доступа к системе, чтобы выяснить ее назначение; получить доступ к игровым программам; модифицировать или стереть данные, а также оставить преднамеренный след, например в виде непристойной записки. Побудительные мотивы получения доступа к системе у указанных субъектов могут быть различны: от желания испытать эмоциональный подъем при игре с компьютером до ощущения власти над ненавистным руководителем (провайдером и т. п.). Занимаются этим не только новички, но и профессиональные программисты. Значительную часть нарушителей составляют любители компьютерных игр, обычно в возрасте от 17 до 25 лет. Однако часть из них начинает не только просматривать, но и проявлять интерес к содержимому файлов, а это уже представляет серьезную угрозу, поскольку в данном случае трудно отличить безобидное баловство от умышленных действий.

2. Хакеров-профессионалов, прекрасно знающих вычислительную технику и системы связи, затрачивающих массу времени на обдумывание способов проникновения в системы и еще больше, экспериментируя с самими системами. Их цель – выявить и преодолеть систему защиты, изучить возможности вычислительной установки и затем удалиться, самоутвердившись в возможности достижения цели.

Благодаря высокой квалификации, эти люди понимают, что степень риска мала, так как отсутствуют мотивы разрушения или хищения.

К категории криминальных профессионалов обычно относят: преступные группировки, преследующие политические цели; лиц, стремящихся получить информацию в целях промышленного шпионажа и, наконец, группировки отдельных лиц, стремящихся к наживе. Профессиональные хакеры стремятся свести риск к минимуму, поэтому привлекают к соучастию работающих или недавно уволившихся с фирмы служащих, поскольку для постороннего риск быть обнаруженным при проникновении в банковские системы весьма велик.

Что касается возраста указанных лиц, то в юридической литературе приводятся различные возрастные границы: в основном не более 30-35 лет. При этом считается, что до 25 лет хакер небогат и бескорыстен, а с 30-35 лет начинает искать способы незаконного обогащения [7, с. 348].

Выводы. Таким образом, подводя итог всему сказанному, хотелось бы отметить, что, к сожалению, действующее уголовное законодательство Республики Казахстан в сфере борьбы с компьютерными преступлениями не соответствует современным реалиям, и его необходимо совершенствовать. И в первую очередь, это касается субъекта преступления, предусмотренного ст. 227 УК РК. То есть субъектом преступления признать вменяемое, физическое лицо, достигшее 16-летнего возраста. При этом нами выделяется несколько категорий субъектов преступления: 1) лица, осуществляющие неправомерный доступ к компьютерной информации, ч. 1 ст. 227 УК РК (общий субъект); 2) лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой, – ч. 2 ст. 227 УК РК; 3) лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения, – ч. 2 ст. 227 УК РК; 4) лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети, но осуществляющие неправомерный доступ к компьютерной информации, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, – ч. 3 ст. 227 УК РК.

Литература

1 Уголовный кодекс Республики Казахстан от 16 июля 1997 года № 167-1, по состоянию на 23 октября 2008 года // СПС «Юрист».

2 Нурпеисова А.К. Уголовно-правовые и криминологические аспекты компьютерной преступности: дис. … канд.юрид.наук: 12.00.08. – Алматы, 2010. – 167 с.

3 Толеубекова Б. Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники: дис д-ра юрид. наук. – Алматы, 1998. – 380 с.

4 Вехов В. Б. Компьютерные преступления: способы совершения, методы расследования. – М., 1996. – 296 с.

5 Компьютерные технологии в юридической деятельности: учебно-практическое пособие / под ред.: Н. Полевого, В. Крылова. – М., 1998.– 344 с.

6 Роберт Ричардсон. Хакеры: дьяволы или святые? // Журнал сетевых решений. – 1998. – Т. 4. – С. 108-109.

7 Скоромников К.С. Пособие для следователя. Расследование преступлений повышенной общественной опасности. – М., 2003. – 566 с.

References

1 Ugolovnyi kodeks Respubliki Kazakhstan to 16 iyulya 1997 goda No.167-1, po sostoyaniyu na 23 oktyabrya 2008 goda // SPS "Yurist"

2 Nurpeisova A.K. Ugolovno-pravovye i kriminologicheskie aspekty komp'yuternoy prestupnosti: dis. ... kand.yur.nauk: 12.00.08. – Almaty, 2010. – 167 s.

3 Toleubekova B.H. Problemy sovershenstvovaniya bor'by s prestupleniyami, sovershaemymi s ispol'zovaniem komp'yuternoy tehniki: dis d-ra yurid.nauk – Almaty, 1998. – 380 s.

4 Vehov V.B. Komp'yuternye prestupleniya: sposoby sovershеniya, metody rassledovaniya. – M., 1996. – 296 s.

5 Komp'yuternye tehnologii v yuridicheskoy deyatel'nosti: Uchebno-prakticheskoe posobie / Pod red. N. Polevogo, V.Krylova. – M., 1998. – 344 s.

6 Robert Richardson. Hakery: d'yavoly ili svyatye? // Zhurnal setevyh reshenii. – 1998. – T. 4. – S.108-109.

7 Skoromnikov K.S. Posobie dlya sledovatelya. Rassledovanie prestuplenii povyshennoy obshestvennoy opasnosti. – M., 2003. – 566 s.