УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В ОБЛАСТИ ИНФОРМАТИКИ И ЭЛЕКТРОСВЯЗИ

Наталья ЛАЗАРЕВА

Кафедра уголовного права и криминологии

Codul penal al Republicii Moldova conţine Capitolul XI „Infracţiunile în domeniul informaticii şi reţelelor electronice". Autorul cercetează incriminările faptelor prevăzute de art.259-261/1 ale Codului penal al Republicii Moldova. Sunt descrise obiectul şi latura obiectivă, subiectul şi latura subiectivă ale acestor infracţiuni. Analiza prevederilor cuprinse în Capitolul XI permite autorului să dezvăluie contradicţiile, scăpările şi neajunsurile referitoare nu numai la unele articole, dar şi la întregul capitol. Astfel, se poate constata că în prezent punerea în aplicare a normelor ce se conţin în art.259-261/1 ale Codului penal al Republicii Moldova este limitată din cauza imperfecţiunilor juridice şi practice, legate de utilizarea şi securitatea informaţiei computerizate, ceea ce, în rezultat, nu asigură lupta efectivă împotriva faptelor infracţionale în domeniul informaticii şi reţelelor electronice.

The Criminal Code of RM contains chapter XI «Crimes in the Field of Computer Science and Telecommunication». The author investigates corpus delicti in articles 259-261/1 CC RM, describes the object and the objective side, subject and the subjective side of crimes. The analysis of chapter XI allows the author to reveal contradictions, blanks and lacks concerning not only separate articles, but also the whole chapter. Thus, it is possible to establish, that application of norms contained in articles 259-261/1 of Criminal Code of RM is limited by the legal and practical undevelopment, connected with the use and protection of the computer information that does not give an opportunity effectively to counteract criminality in the field of computer science and telecommunication.

Уголовный кодекс РМ в главе XI предусматривает ответственность за совершение преступлений в области информатики и электросвязи. Данная глава включает четыре статьи: 259 (Несанкционированный доступ к компьютерной информации), 260 (Внесение или распространение вредоносных компьютерных программ), 261 (Нарушение правил безопасности информационных компьютерных систем), 261/1 (Несанкционированный доступ к сетям или услугам электросвязи).

Целесообразно исследовать составы преступлений, предусмотренных ст. ст. 259-261/1 УК РМ.

Статья 259 УК РМ предусматривает ответственность за несанкционированный доступ к компьютерной информации, то есть к информации на машинных носителях, в компьютерной системе или сети, сопряженный с уничтожением, повреждением, модификацией, блокированием или копированием информации, с нарушением работы компьютеров, компьютерных систем или сетей.

Объектом данного преступления являются общественные отношения, охраняющие права собственника компьютерной информации на ее неприкосновенность, а также интересы относительно правильной (безопасной) эксплуатации компьютеров, компьютерных систем или сетей.

Обособление данной уголовно-правовой нормы вызвано специфичностью компьютерной информации как предмета преступного посягательства.

Объективная сторона характеризуется действием (несанкционированным доступом к компьютерной информации), выражается в преднамеренном доступе лица, не уполномоченного владельцами информации или администраторами системы (операторами) к данным, закрепленным в данном компьютере, машинном носителе, в компьютерной системе или сети, сопряженном с уничтожением, блокированием или копированием информации, с нарушением работы компьютеров, компьютерных систем или сетей.

На практике встречаются трудности при трактовке понятия „несанкционированного доступа к компьютерной информации". Вместе с тем, четкое понимание данного термина является необходимым условием правильной квалификации.

По нашему мнению, нельзя рассматривать как „доступ к компьютерной информации" простое физическое завладение (тайное или открытое) машинным носителем, содержащим информацию, с целью его продажи, а не содержащейся на нем компьютерной информации (например, жестким диском-hard). Такое деяние квалифицируется как традиционное посягательство на собственность (например, на кражу – ст. 186 УК РМ).

Точно также не образует объективной стороны данного преступления уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами и другими подобными методами.

В соответствии с Законом РМ «Об информатике», доступ к информации, осуществляемый с нарушением рабочего режима, считается несанкционированным [1]. В то же время понятие несанкционированного доступа содержится в законе РМ «Об электросвязи»: согласно ст. 2 несанкционированный доступ определяется как «использование физическим или юридическим лицом сети и/ или услуг оператора без заключения какого-либо договора на использование или без иных законных оснований, определяющих условия осуществления санкционированного доступа» [2]. Следовательно, доступ к компьютерной информации можно считать несанкционированным, если:

- лицо не обладает законными основаниями на доступ к данной информации;
- лицо обладает законными основаниями на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением мер ее защиты.

Состав преступления, описанный в статье 259 УК РМ, сформулирован как формальный, и деяние считается оконченным с момента совершения хотя бы одного действия, указанного в диспозиции ст. 259 УК РМ.

Вместе с тем, представляет интерес рассмотрение этих действий, без совершения которых преступление не может считаться оконченным. Причем, заметим, что законодатель только перечисляет их, не раскрывая при этом их понятия, в связи с чем в настоящее время по поводу их содержания дискутируются различные точки зрения. Кратко рассмотрим основные из них.

С.А. Пашин определяет *уничтожение компьютерной информации* как "стирание ее в памяти ЭВМ" [3]. Однако он почему-то забывает при этом о других машинных носителях, находящихся автономно от ЭВМ, на которых охраняемая законом компьютерная информация также может быть уничтожена, например – на дискете или компакт-диске. И.А. Попов, учитывая это, предлагает под уничтожением компьютерной информации понимать "такое изменение ее первоначального состояния (полное либо частичное удаление информации с машинных носителей), при котором она перестает существовать в силу утраты основных качественных признаков" [4]. Вместе с тем он не называет эти „качественные признаки”, по которым правоприменитель может установить фактическое наличие исследуемого квалифицирующего признака.

Более правильную позицию по содержанию исследуемой дефиниции заняли А.Н. Попов, А.В. Пушкин, М.Ю. Дворецкий, К.С. Скоромников и В.С. Комиссаров, которые под уничтожением компьютерной информации понимают приведение ее частично или полностью в такое состояние, когда она не может быть восстановлена и использована по назначению.

С учетом рассмотренных позиций можно заключить, что *уничтожение компьютерной информации состоит в ее ликвидации любыми способами, которая приводит к невозможности использования информации по целевому назначению и не зависит от возможности ее восстановления средствами и методами, которыми располагает потерпевший.* Одним из таких способов является *стирание информации с машинного носителя* – частичное уничтожение компьютерной информации с машинного носителя, заключающееся в ликвидации отдельных признаков, позволяющих ее идентифицировать как документ.

Содержание понятия *"блокирование компьютерной информации"* также является дискуссионным. Так, С.И. Никулин определяет его как "создание препятствий к свободному ее использованию при сохранности самой информации" [5]. В.С. Комиссаров развивает эту мысль: "создание недоступности к компьютерной информации, т. е. невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, а равно выключения реакции какого-либо устройства ЭВМ при сохранениии информации" [6]. Представляется, что избранный автором методологический подход, основанный на перечислении способов блокирования информации, ошибочен, поскольку никогда невозможно будет все их перечислить.

И.А. Попов в принципе верно под блокированием понимает "закрытие информации, характеризующееся недоступностью ее использования по прямому назначению со стороны законного пользователя, собственника или владельца" [7]. Однако сразу возникает вопрос относительно понятия "закрытие", поскольку не ясно, как можно "закрыть информацию". Представляется, что этот термин к исследуемой дефиниции неприменим.

Относительно правильно понимает содержание рассматриваемого признака В.В. Крылов. "Блокирование, – отмечает он, это временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией в ЭВМ как результат воздействия на ЭВМ и ее элементы" [8]. Принимая за основу его методологический подход, определим ***блокирование компьютерной информации*** как *физическое воздействие на компьютерную информацию, ее машинный носитель и (или) программно-технические средства ее обработки и защиты, результатом которого явилась временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией.*

В настоящее время в юридической литературе не существует сколь-нибудь устоявшейся позиции относительно содержания понятия "модификация компьютерной информации". Например, достаточно оригинально изложил его П.Н. Панченко: "Модификация информации–это изменение логической и физической организации базы данных" [9]. Остается загадкой, почему автор выделил только одну из возможных документированных форм компьютерной информации, тогда как остальные оставил без внимания?

В свою очередь С.А. Пашин подошел к признаку "модификация компьютерной информации" с позиций авторского права и определил его как "внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных" [10].

И.А. Попов понимает под исследуемым термином "изменение первоначального состояния информации, не меняющей сущности объекта" [11], но опять же не акцентирует того, кем такие действия могут быть осуществлены в рамках действующего законодательства, а кем не могут (соответственно действия данного лица будут считаться неправомерными).

Оригинальный взгляд на проблему высказал С.В. Бородин: модификация информации – это "изменение ее содержания по сравнению с той информацией, которая первоначально до совершения деяния была в распоряжении собственника или законного владельца" [12]. Представляется, что существенным упущением данного определения является отсутствие указания на характер и объем вносимых изменений.

М.М.Карелина исключила из своего определения имущественный признак информации, ее принадлежность какому-либо лицу: "Модификация информации – внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе" [13]. Ее точку зрения поддержал и развил А.Г. Волеводз: "Модификация информации – внесение изменений в программы, базы данных, текстовую и любую другую информацию, находящуюся на материальном носителе, кроме ее легальной модификации (адаптации и декомпиляции)" [14].

А.В. Пушкин учел вышеуказанные недочеты, в результате чего появилось следующее определение: "Модификация заключается в переработке первоначальной информации, не санкционированной ее законным собственником или владельцем, если такая переработка включает в себя любые изменения, – это любое изменение информации, не направленное на обеспечение интересов собственника или иного владельца информации" [15]. Мы присоединяемся к указанной точке зрения и предлагаем под ***модификацией компьютерной информации*** понимать *внесение в нее любых несанкционированных собственником, владельцем или уполномоченным ими лицом изменений.*

Термин *"копирование компьютерной информации"* также имеет различные юридические толкования. Так, П.Н. Панченко рассматривает копирование как "изготовление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись в память ЭВМ" [16], В.С. Комиссаров – "снятие копии с оригинальной информации с сохранением возможности ее использования по назначению" [17], С.А. Пашин – "повторение и устойчивое запечатление ее на машинном или ином носителе, включая запись в память ЭВМ" [18], И.А. Попов –"перенос информации или части информации с одного физического носителя на другой" [19], М.М. Карелина – "перенос информации на другой материальный носитель, при сохранении неизменной первоначальной информации" [20], а С.В. Бородин – "ее перезаписывание, а также тиражирование при сохранении оригинала, а также и ее разглашение" [21].

Вместе с тем представляется спорной позиция К.С. Скоромникова, А.Н. Попова и А.Г. Волеводза, считающих, что копирование – это воспроизведение информации в любой материальной форме, в том числе копирование компьютерной информации от руки, съемка текста с экрана дисплея, а также считывание информации путем перехвата излучений ЭВМ, расшифровка шумов принтера и т. д. [22], [23]. По поводу содержания этого положения подчеркнем, что в случае воспроизведения ("копирования")

компьютерной информации не на машинный, а на иной материальный носитель, она становится обычной информацией и теряет свои "компьютерные" признаки и свойства, в результате чего данное деяние не будет подпадать под признаки преступлений в области информатики и электросвязи и должно квалифицироваться по другим, "не компьютерным" статьям УК РМ.

С учетом вышеизложенного, определим **копирование компьютерной информации** как повторение и устойчивое запечатление компьютерной информации любыми способами на отличном от оригинала машинном носителе при одновременной сохранности признаков, идентифицирующих ее.

Нарушение работы компьютеров, компьютерных систем или сетей включает в себя сбой в работе компьютеров, компьютерных систем или сетей, препятствующий нормальному функционированию вычислительной техники при условии сохранения ее физической целостности и обязательности восстановления работоспособности (например, отображение неверной информации на мониторе, нарушение порядка выполнения команд, разрыв сети и др.).

Субъективную сторону любого преступления характеризуют такие признаки, как вина, мотив и цель общественно опасного противоправного поведения субъекта. [24]. Несмотря на то, что диспозиция ст.259 УК РМ не дает прямых указаний о субъективной стороне анализируемого преступления, можно с уверенностью говорить об умышленной форме вины в виде прямого или косвенного умысла. В литературе высказывалась и другая точка зрения, согласно которой несанкционированный доступ к компьютерной информации может быть совершен только с прямым умыслом [25]. Между тем закон вовсе не ограничивает привлечение лица к уголовной ответственности по ст. 259 УК РМ в случае совершения этого преступления с косвенным умыслом. Как показывает практика, преступник не всегда желает наступления вредных последствий. Особенно это характерно при совершении данного преступления из озорства или так называемого „спортивного интереса".

Мотивы и цели несанкционированного доступа к компьютерной информации могут быть самыми разнообразными. Как правило, побуждающим фактором к совершению несанкционированного доступа к компьютерной информации является корысть, что, естественно, повышает степень общественной опасности указанного преступления. В качестве иллюстрации корыстного доступа к компьютерной информации может служить пример, когда лицо путем подбора идентификационного кода (пароля) внедряется в компьютерную сеть, обслуживающую банковские операции, и незаконно перечисляет определенную сумму денежных средств на свой текущий счет.

Наряду с корыстью анализируемое преступление может совершаться из чувства мести, зависти, хулиганства, желания испортить деловую репутацию конкурента, „спортивного интереса" или желания скрыть другое преступление и т.д.

Субъектом преступления, предусмотренного ст. 259 УК РМ, может быть вменяемое физическое лицо, которое в момент совершения преступления достигло шестнадцати лет, а также юридическое лицо.

Физические лица, виновные в совершении преступления, предусмотренного ч. (1) ст. 259 УК РМ, наказываются штрафом в размере от 200 до 500 условных единиц или неоплачиваемым трудом в пользу общества на срок от 150 до 200 часов, или лишением свободы на срок до 2 лет, а юридические лица – штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

Часть (2) ст. 259 УК РМ предусматривает ответственность при наличии следующих отягчающих обстоятельств: a) совершенное повторно; b) совершенное двумя или более лицами; c) совершенное с нарушением систем защиты; d) совершенное путем подключения к каналам связи, e) совершенное с использованием специальных технических средств.

Физические лица, виновные в совершении преступления, предусмотренного ч. (2) ст. 259 УК РМ, наказываются штрафом в размере от 500 до 1000 условных единиц или неоплачиваемым трудом в пользу общества на срок от 180 до 240 часов, или лишением свободы на срок до 5 лет, а юридические лица – штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или с ликвидацией предприятия.

Статья 260 УК РМ устанавливает уголовную ответственность за внесение и распространение вредоносных программ.

Данная уголовно-правовая норма представляет огромную сложность для практического использования и квалификации. Об этом свидетельствует то, что до сих пор не дано формального общепринятого определения сущности вредоносных программ. Одно из наиболее удачных определений вредоносной

программы предложено Ю.И. Ляпуновым и А.В. Пушкиным. Под вредоносной программой названные авторы понимают специально написанную (созданную) программу, которая, получив управление, способна совершать несанкционированные пользователем действия и вследствии этого причинять вред собственнику или владельцу информации, а также иным лицам в виде уничтожения, блокирования, модификации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети [26].

Вредоносность или полезность соответствующих компьютерных программ определяется не в зависимости от их назначения, способности уничтожать, модифицировать, копировать информацию (это вполне типичные функции вполне легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу вредоносной [27].

Следует обратить внимание, что некоторые авторы отождествляют понятия вредоносной программы и компьютерного вируса. Так, И.Макарь в учебнике «Уголовное право Республики Молдова. Часть Особенная» прямо указывает: «Под вредоносной компьютерной программой следует понимать создание так называемой вирусной программы или внесение изменений в уже существующие программы» [28]. С подобным подходом вряд ли можно согласиться.

Представляется, что многообразие вредоносных программ только лишь компьютерными вирусами не ограничивается. Любая вредоносная программа, чтобы являться таковой, должна обладать как минимум следующими признаками: во-первых, она должна совершать несанкционированные пользователем действия, и, во-вторых, результатом этих действий должно быть уничтожение, блокирование, модификация или копирование компьютерной информации, нарушение работы компьютеров, компьютерных систем или сетей.

Вирус же, отвечая названным условиям, обладает дополнительной функцией – он способен самовоспроизводиться, то есть размножаться, присоединяться к другим программам и пр. Программу-вирус, таким образом, можно определить как специально созданную программу, способную к самовоспроизведению, выполняющую незапланированные законным пользователем функции. Эти функции могут быть различными: порча файлов, приводящая к блокированию, модификации или уничтожению содержащейся в них информации; засорение памяти компьютера, влекущее замедление его работы; вывод на экран посторонних сообщений и пр.

Таким образом, понятие «вредоносная программа» является родовым по отношению к понятию «программа-вирус». Помимо программ-вирусов к категории вредоносных программ относятся: программы-эмуляторы электронных ключей, программы-взломщики парольной защиты, программы типа «троянский конь», программы – «черви» и др.

Непосредственным объктом этого преступления являются общественные отношения по обеспечению безопасности владения, пользования и распоряжения компьютерной информацией, а также пользования средств ее обработки – средств электронно-вычислительной техники.

В качестве **дополнительного объекта** данного преступления выступают материальные (имущественные) интересы потерпевшего.

Объективная сторона рассматриваемого состава преступления характеризуется такими действиями, как заведомое внесение в компьютерные программы вирусных модификаций, либо распространение компьютерных программ или информации, выводящих из строя машинные носители информации, технические средства обработки данных или нарушающих систему защиты.

Внесение в компьютерные программы вирусных модификаций – это несанкционированная законным пользователем или собственником программы ее модификация (переработка программы путем изменения, добавления или удаления ее отдельных фрагментов) до такого состояния, когда эта программа способна выполнить новые, изначально незапланированные функции и приводить к последствиям, предусмотренным ст. 260 УК РМ.

„Распространение вредоносных программ" возможно как в активной форме (внедрение вредоносной программы в компьютеры, их систему или сеть любым способом, предоставляющим свободный доступ к ней), так и в пассивной (невоспрепятствование самораспространению вредоносной программы или распространению ее третьими лицами).

„Распространение вредноносных программ" – это предоставление доступа к воспроизведенной в любой материальной форме компьютерной программе, в том числе сетевыми и иными способами, а

также путем продажи, проката, сдачи в наем, предоставления взаймы, обмена, дарения, безвозмездная передача другим лицам.

Состав рассматриваемого преступления является формальным и считается оконченным с момента введения программы в компьютер, систему компьютеров или их сеть либо с момента передачи программы хотя бы одному лицу.

О характере **субъективной стороны** анализируемого преступления свидетельствует указание в законе на *заведомое* внесение в компьютерные программы вирусных модификаций либо распространение компьютерных программ или информации, выводящих из строя машинные носители информации, технические средства обработки данных или нарушающих систему защиты. Таким образом, виновное лицо сознает, что его действия по внесению в компьютерные программы вирусных модификаций либо по распространению компьютерных программ или информации носят общественно опасный характер, предвидит возможность или неизбежность вывода из строя машинных носителей информации, технических средств обработки данных или нарушающих систему защиты и желает их наступления (прямой умысел) или не желает, но сознательно допускает эти последствия либо относится к ним безразлично (косвенный умысел).

В юридической литературе на данный счет имеются различные точки зрения. Так, Ю.И. Ляпунов, А.В. Пушкин, И. Макарь считают, что данное преступление совершается лишь с прямым умыслом. Однако как же тогда квалифицировать действия лица, осуществляющего распространение машинных носителей информации (дискет, CD-дисков), содержащих вредноносные программы, достоверно знающего о вредноносных последствиях такой программы (хотя бы по этикетке компакт-диска), но вместе с тем абсолютно безразлично к ним относящегося? На наш взгляд, данное лицо совершает распространение вредоносных компьютерных программ именно с косвенным умыслом.

Вместе с тем нельзя согласиться с мнением профессора С. В. Бородина, считающего возможным совершение анализируемого преступления по неосторожности в виде легкомыслия [29]. Как минимум, законодатель в диспозиции ст. 260 дал четкое указание на заведомый характер деятельности виновного. Уже это не позволяет признать возможным совершение данного преступления по неосторожности.

Факультативные признаки субъективной стороны: мотивами совершения анализируемого деяния чаще всего бывают корысть либо хулиганские побуждения, но могут быть и соображения интереса, чувство мести; не исключено совершение их с целью скрыть другое преступление и т.д.

Субъектом анализируемого состава преступления может быть любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, а также юридическое лицо.

Физические лица, виновные в совершении преступления, предусмотренного ч. (1) ст. 260 УК, наказываются штрафом в размере от 300 до 800 условных единиц или неоплачиваемым трудом в пользу общества на срок от 180 до 240 часов, или лишением свободы на срок до 5 лет, а юридические лица наказываются штафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

Часть (2) ст. 260 УК предусматривает ответственность за распространение вирусных компьютерных программ при оттягчающих обстоятельствах: распространение вирусных программ, повлекшее тяжкие последтвия. К тяжким последствиям могут быть отнесены гибель людей, причинение тяжкого вреда их здоровью, дезорганизация производства на предприятии или в отрасли промышленности, дезорганизация деятельности банка либо системы банков и т.п. [30].

Часть (2) ст. 260 УК для физических лиц предусматривает ответственность в виде лишения свободы на срок от 4 до 8 лет, а для юридических лиц – штаф в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия.

Вызывает немалые споры **статья 261 УК РМ,** которая предусматривает ответственность за нарушение правил безопасности информационных систем.

Объектом этого преступления являются интересы собственника информационной системы или сети относительно их правильной эксплуатации.

Объективная сторона рассматриваемого состава преступления выражается в нарушении правил сбора, обработки, хранения, распространения, распределения информации или правил защиты информационных систем, предусмотренных в соответствии с видом информации или степенью ее защиты, если это действие способствовало хищению, искажению, уничтожению информации или повлекло иные тяжкие последствия.

Диспозиция ст. 261 УК является бланкетной, поэтому для установления наличия состава преступления следует точно доказать, какие именно правила по сбору, обработке, хранению, распространению или распределению были нарушены. Для установления вышеизложенного следует обратиться к соответствующим нормативным актам.

Кроме того, следует установить конкретные последствия, которые наступили в результате нарушения вышеизложенных правил.

Установление степени тяжести наступивших преступных последствий является компетенцией сотрудников органов правосудия, рассматривающих конкретное уголовное дело.

Состав преступления, предусмотренного ст. 261 УК РМ, является материальным и считается оконченным при наступлении последствий, указанных в диспозиции: хищение, искажение и уничтожение инфомаци или наступление иных тяжких последствий (остановка деятельности предприятия, дезорганизация работы банка, причинение вреда здоровью людей и т.п.).

С субъективной сороны деяние характеризуется умышленной виной (как правило, с косвенным умыслом). Виновный осознает, что нарушает правила безопасности информационных систем, что наступят указанные в законе последствия, но безразлично к этому относится. Мотив и цель могут быть разными, но они не влияют на квалификацию содеянного.

Субъкт преступления – это физическое вменяемое лицо, достигшее 16 лет, а также юридическое лицо. При этом закон не требует, чтобы физическое лицо занимало определенную должность, осуществляло определенную деятельность или получило определенное образование в сфере компьютерной информации и (или) ее защиты.

Физические лица наказываются штрафом в размере до 400 условных единиц или неоплачиваемым трудом в пользу общества на срок от 200 до 240 часов, или лишением свободы на срок до 2 лет с лишением или без лишения во всех случаях права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, а юридические лица наказываются штафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

Статья 261/1 УК РМ была введена сравнительно недавно в отечественное уголовное законодательство. Ввиду того, что от оперативных подразделений МВД РМ поступала информация о распространенности несанкционированного доступа к сетям и/или услугам электросвязи, законодатель 22 октября 2004 г. дополнил Уголовный кодекс РМ статьей 261/1, предусматривающей уголовную ответственность за несанкционированный доступ к сетям и/или услугам электросвязи.

Объектом несанкционированного доступа к сетям и/или услугам электросвязи являются общественные отношения, связанные с владением, пользованием и распоряжением сетями и / или услугами электросвязи.

Объективная сторона преступления, предусмотренного ч.(1) ст. 261/1 УК РМ, выражается в несанкционированном доступе к сетям и/или услугам электросвязи с использованием сетей и/или услуг электросвязи других операторов, повлекшем причинение ущерба в крупных размерах. Исходя из данного законодателем определения, можно выделить три обязательных признака несанкционированного доступа к сетям и/или услугам электросвязи, характеризующих это преступление с его внешней, объктивной стороны. Такими признаками являются:

1) общественно опасное действие, к которому законодатель относит несанкционированный доступ к сетям и/или услугам электросвязи с использованием сетей и/или услуг электросвязи других операторов;

2) общественно опасные последствия в виде причинения ущерба в крупных размерах;

3) причинная связь между совершенным деянием и наступившими последствиями. Отсутствие хотя бы одного из перечисленных признаков означает и отсутствие уголовной ответственности по ст. 261/1 УК РМ.

К объективным признакам анализируемого преступления относится общественно опасное деяние, которое всегда проявляется в активной форме поведения виновного. Совершить несанкционированный доступ к сетям и/или услугам электросвязи путем бездействия невозможно.

Субъективная сторона несанкционированного доступа к сетям и/или услугам электросвязи характеризуется прямым и косвенным умыслом.

Субъектом преступления, предусмотренного ч.(1) ст. 261/1 УК РМ, может быть любое физическое лицо, достигшее к моменту преступной деятельности шестнадцатилетнего возраста. Обязательным условием привлечения лица к уголовной ответсвенности за совершенное общественно опасное и противоправ-

ное деяние является вменяемость. Субъктом вышеназванного преступления может быть также и юридическое лицо. Физическое лицо наказывается штрафом в размере от 200 до 1000 условных единиц или лишением свободы на срок от 1 до 3 лет, а юридическое лицо наказывается штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

В ч.(2) ст. 261/1 УК РМ предусмотрены обстоятельства, отягчающие ответственность за совершение вышеназванного преступления. К числу отягчающих законодатель относит следующие обстоятельства:

несанкционированный доступ к сетям и/или услугам электросвязи с использованием сетей и/или услуг электросвязи других операторов, совешенный

a) повторно;

b) двумя или более лицами;

c) с нарушением систем защиты;

d) с использованием специальных технических средств;

e) повлекший причинение ущерба в особо крупных размерах.

При наличии вышеназванных оттягчающих обстоятельств преступление признается более опасным и поэтому влечет более суровое наказание в виде штрафа в размере от 1000 до 3000 условных единиц или лишения свободы на срок до 5 лет, а юридическое лицо наказывается штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью.

Подводя итог вышеизложенному, можно констатировать, что в настоящее время применение норм, содержащихся в статьях 259-261/1 Уголовного кодекса РМ, ограничено правовой и практической неразработанностью отдельных понятий, связанных с использованием и охраной компьютерной информации. Тем не менее принятие нового Уголовного кодекса, безусловно, является шагом вперед в определении понятия «компьютерное преступление» и в квалификации отдельных нарушений. То есть правовая основа для деятельности правоохранительных органов уже заложена.

Литература:

1. Закон РМ «Об информатике» № 1069-XIV от 22.06.2000 г. // Monitorul Oficial al Republicii Moldova. - 2001. - №74/547. - ст.2.
2. Закон РМ «Об электросвязи» № 520 – XIII от 07.07.1995 // Monitorul Oficial al Republicii Moldova. - 1995. - № 65- 66/713. - ст.2.
3. Комментарий к Уголовному кодексу Российской Федерации. 2-е изд., изм. и доп. / Под общ. ред. проф. Ю.И. Скуратова, В.М. Лебедева. - Москва, 1998. - 635 с.
4. Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно-правовой анализ. / Под общ. ред. В.В. Мозякова. - Москва, 2002. - 647 с.
5. Уголовное право. Часть Особенная: Учебник / Под ред. проф. А.И.Рарога. - Москва, 1996. - 324.с.
6. Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой. 2-е изд. / Под общ. ред. С. И. Никулина. - Москва, 2002.- 903 с.
7. Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно- правовой анализ / Под общ. ред. В.В. Мозякова. - Москва, 2002. - 647 с.
8. Крылов В.В. Расследование преступлений в сфере компьютерной информации. - Москва, 1998. - 108 с.
9. Научно-практический комментарий к Уголовному кодексу Российской Федерации: В 2-х т. Т.2 / Под ред. проф. П.Н. Панченко. - Н.Новгород, 1996. - 235 с.
10. Комментарий к Уголовному кодексу Российской Федерации. 2-е изд., изм. и доп./ Под общ.ред. проф. Ю.И. Скуратова, В.М. Лебедева. - Москва, 1998. - 637 с.
11. Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно-правовой анализ / Под общ. ред. В.В. Мозякова. - Москва, 2002. - 647с.
12. Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. А.В. Наумова. - Москва, 1996. - 664 с.
13. Уголовный кодекс Российской Федерации: Науч.-практ. комментарий / Отв. ред. В.М. Лебедев. - Москва, 1998. - 584 с.
14. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. - Москва, 2002. - 69 с.
15. Комментарий к Уголовному кодексу Российской Федерации: В 2-х т. Т.2 / Под ред. проф. О.Ф. Шишова. - Москва, 1998, с. 355-356 .
16. Научно-практический комментарий к Уголовному кодексу Российской Федерации: В 2-х т. Т.2 / Под ред. проф. П.Н. Панченко. - Н. Новгород, 1996. - 235 с.
17. Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой. 2-е изд. / Под общ. ред. С.И. Никулина. - Москва, 2002. - 903 с.

18. Комментарий к Уголовному кодексу Российской Федерации. 2-е изд., изм. и доп. / Под общ. ред. проф. Ю.И. Скуратова, В.М. Лебедева. - Москва, 1998. - 637 с.
19. Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно-правовой анализ / Под общ. ред. В.В. Мозякова. - Москва, 2002. - 647с.
20. Уголовный кодекс Российской Федерации: Науч.-практ. комментарий / Отв. ред. В.М. Лебедев. - Москва, 1998. - 584 с.
21. Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. А.В. Наумова. - Москва, 1996. - 664 с.
22. Скромников К.С. Понятие, виды компьютерных преступлений, их уголовно-правовая характеристика // Расследование преступлений повышенной общественной опасности: Пособие для следователей / Под ред. проф. Н.А. Селиванова, канд. юрид. наук А.И. Дворкина. - Москва, 1998. - 340 с.
23. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. - Москва, 2002. - 69 с.
24. Ветров Н.И. Субъективная сторона преступления. Уголовное право. Общая часть / Под ред. Н.И. Ветрова, Ю.И Ляпунова. - Москва, 1997. - 239 с.
25. Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. А.В. Наумова. - Москва, 1996.- 665 с.
26. Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации // Уголовное право. Часть Особенная / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. - Москва, 1998. - 554 с.
27. Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание: Учебное пособие. - Москва, 2003. - 35 с.
28. Макарь И. Уголовное право РМ. Часть Особенная. - Кишинев, 2004. - 317 с.
29. Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. А.В. Наумова. - Москва, 1996. - 666 с.
30. Макарь И. Уголовное право РМ. Часть Особенная. - Кишинев, 2004. - 317 с.

Prezentat la 10.05.2007