УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ОБЛАСТИ ИНФОРМАТИКИ И ЭЛЕКТРОСВЯЗИ

Наталья ЛАЗАРЕВА

Кафедра уголовного права и криминологии

Măsuri în ce priveşte combaterea infracţiunilor în domeniul informaticii şi al reţelelor electronice se întreprind atât la nivel naţional, cât şi la nivel internaţional. Drept dovadă serveşte un şir de documente internaţionale, printre care un rol important îi revine Convenţiei cu privire la infracţiunile cibernetice. La nivel naţional, problema luptei cu infracţiunile în domeniul informaticii şi al reţelelor electronice a cerut legiuitorului includerea în Codul penal al Republicii Moldova a Capitolului XI – Infracţiunile în domeniul informaticii şi al reţelelor electronice. Fără îndoială, includerea acestuia în legea penală este un pas înainte în combaterea infracţiunilor computerizate. Totodată, persistă încă numeroase probleme de drept nerezolvate, care impiedică lupta cu infracţiunile în domeniul informaticii şi al reţelelor electronice, făcând-o inefectivă. În legătură cu aceasta, se fac propuneri întru perfecţionarea bazei teoretice a normelor existente în Codul penal al Republicii Moldova, avându-se în vedere experienţa adoptării de legi în acest domeniu.

Today the struggle against crimes in the field of computer science and telecommunications is undertaken at the national and international level. The Convention of Cyber Crimes is one of the most important laws at the international level. At the national level, the problem of counteracting computer 1and telecommunication crimes still requires that legislations adopt adequate legal measures. Criminal Code of RM Chapter XI: Crimes in the Filed of Computer Science and Telecommunication represent such an example. An analysis using Chapter XI reveals the contradictions, blanks, and leaks which do not fully provide for enforcement measures to counteract criminality in the fields of computer science and telecommunications. This respect, this analysis, using international experience and norms, offers an improvement of the theoretical basis of the legal norms within the criminal code of RM.

Меры по борьбе с преступлениями в области информатики и электросвязи предпринимаются сегодня как на национальном, так и на межгосударственном уровне. Об этом свидетельствует ряд международных документов, как то: Конвенция о киберпреступности, принятая 27 апреля 2000 года Советом Европы [1]; Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые в Бангкоке 25 апреля 2005 года на Одиннадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями [2]; Окинавская Хартия глобального информационного общества, принятая 23 июля 2000 года на Окинаве (Япония) на совещании руководителей глав государств и правительств стран «Группы Восьми» [3]. В рамках стран СНГ 17 февраля 1996 года на VII пленарном заседании Межпарламентской Ассамблеи был принят Модельный уголовный кодекс, в котором регламентируется ответственность за компьютерные преступления [4]; 1 июня 2001 года в Минске (Республика Беларусь) было принято Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. В России, в Республике Молдова и в некоторых других государствах – членах Содружества рассматриваемая проблема потребовала от законодателя принятия срочных адекватных правовых мер противодействия данным преступным посягательствам.

Решающим шагом в уголовно-правовом противодействии преступлениям в области информатики и электросвязи стало включение в Уголовный кодекс Республики Молдова новой главы XI – «Преступления в области информатики и электросвязи». Глава XI Уголовного кодекса РМ содержит четыре статьи: статью 259 – «Несанкционированный доступ к компьютерной информации», статью 260 – «Внесение или распространение вредоносных компьютерных программ», статью 261 – «Нарушение правил безопасности информационных систем», и, наконец, статью 261/1 – «Несанкционированный доступ к сетям и услугам электросвязи» [5].

В специальной литературе между тем неоднократно указывалось на наличие несоответствия норм главы XI Уголовного кодекса РМ современной ситуации. Существующее уголовное законодательство об ответственности за преступления в области информатики и электросвязи создает по существу лишь видимость решения проблемы преступности в области информатики и электросвязи. Но самое главное – в нём говорится только о преступлениях, совершаемых в отношении компьютеров и компьютерной

информации, но не затрагиваются другие преступления, совершаемые с их использованием. Разумеется, это не значит, что от законодателя требуется разместить в главе Уголовного кодекса, посвященной преступлениям в области информатики и электросвязи, нормы о преступлениях, совершаемых с помощью компьютера, но посягающих на другие объекты. На наш взгляд, в Уголовном кодексе РМ необходимо предусмотреть ответственность за несанкционированные операции с компьютерами и компьютерными данными, которые выполняются с целью сокрытия другого преступления или облегчения его совершения. Таким образом, законом будут охвачены не только деяния, объектом которых является безопасность функционирования компьютерных сетей и содержащейся в них информации, но и иные киберпреступления.

Анализ главы XI Уголовного кодекса РМ позволяет выявить следующие противоречия, пробелы или другие недостатки, касающиеся не только отдельных статей, но и главы в целом. Недостатком конструкции состава преступления, предусмотренного статьей 259 Уголовного кодекса РМ, является то, что законодатель устанавливает наступление уголовной ответственности за несанкционированный доступ к компьютерной информации, сопряженный с уничтожением, повреждением, модификацией, блокированием или копированием информации, нарушением работы компьютеров, компьютерных систем или их сетей. Между тем, просто несанкционированный доступ к информации – уголовно не наказуем. Таким образом, получается, что если информация была скопирована, то все признаки состава преступления есть, а если она была просто прочитана – то таковых нет. А между тем, по нашему мнению, прочтение информации не менее опасно, чем ее копирование. В некоторых случаях злоумышленнику достаточно увидеть и прочитать информацию – и она тогда утрачивает свою ценность или может быть применена им в дальнейшем без всякого копирования. Кроме того, существуют иные способы сохранения данных для дальнейшего использования – например, фотографирование экрана компьютера.

При построении диспозиции статьи 260 главы XI Уголовного кодекса РМ, предусматривающей ответственность за внесение или распространение вредоносных компьютерных программ, при описании объективной стороны преступления допущена синонимия единственного и множественного числа, недопустимая с точки зрения законодательной техники и явно искажающая волю законодателя. В диспозиции говорится о заведомом внесении в компьютерные программы вирусных модификаций либо распространении компьютерных программ или информации, выводящих из строя машинные носители информации, технические средства обработки данных или нарушающих систему защиты [6]. Если исходить из буквального толкования нормы, то получается, что уголовно наказуемым является только совершение указанных в диспозиции действий в отношении как минимум двух программ. Очевидно, что криминализировано все-таки распространение хотя бы одной программы, но дефект законодательной техники искажает волю законодателя, а также может привести к неправильному толкованию закона. Этот дефект необходимо устранить с изложением диспозиции статьи 260 УК РМ, исключив употребление множественного числа.

В Уголовном кодексе РМ ничего не сказано относительно создания вирусных компьютерных программ. На наш взгляд, было бы целесообразным криминализировать данное деяние.

Что касается нарушения правил безопасности информационных систем, то диспозиция статьи 261 УК РМ является бланкетной, поэтому для установления наличия состава преступления следует точно доказать, какие именно правила по сбору, обработке, хранению, распространению или распределению информации были нарушены и кем именно. Состав преступления, описанный в статье 261 УК РМ, сформулирован как материальный и считается оконченным при наступлении последствий, указанных в диспозиции: хищение, искажение и уничтожение информации или наступление иных тяжких последствий [7]. По нашему мнению, гораздо логичнее было бы криминализировать хищение, искажение и уничтожение информации или наступление иных тяжких последствий, независимо от того, было ли оно совершено с нарушением правил или нет.

В Уголовном кодексе РМ отсутствуют также нормы о так называемом «компьютерном мошенничестве» – хищении чужого имущества или приобретении права на чужое имущество, совершенном путем ввода, изменения, удаления или блокирования компьютерных данных или любого иного вмешательства в функционирование компьютерной системы. К тому же специалисты по уголовному праву Совета Европы предлагают криминализировать компьютерное мошенничество.

И законодатель, и правоприменительная практика в качестве обязательного признака мошенничества называют обман или злоупотребление доверием потерпевшего, в результате чего он добровольно передает имущество или право на имущество, то есть волевой признак. Поскольку хищение имущества или приобретение права на чужое имущество, совершенное путем вмешательства в функционирование компьютерной системы, не имеет этого признака, введение в уголовное законодательство нормы о «компьютерном мошенничестве» будет противоречить требованиям законодательной техники.

Таким образом, наиболее приемлемым представляется назвать предлагаемую норму о хищении имущества (или приобретении права на чужое имущество), совершенном путем манипуляций с компьютерной информацией. По сути, эта норма будет охватывать также деяния, называемые «компьютерными кражами», но не подпадающие под действие статьи 186 Уголовного кодекса РМ по уже указанным выше причинам.

Действующий Уголовный кодекс РМ не предлагает достаточно конкретного способа определения ценности информации, которой причиняется ущерб. С точки зрения уголовного закона, любая информация, содержащаяся на машинном носителе, в компьютере, компьютерной системе или сети настолько важна, что заслуживает правовой охраны. При этом не учитывается тот факт, что с распространением компьютеров сильно дифференцировалась и ценность содержащейся в них информации. Взламываемый компьютер в настоящее время с равной вероятностью может содержать как ценнейшую научную или финансовую информацию, так и компьютерные игры, фильмы, музыку или даже порнографические изображения. Однако в любом случае причинение ущерба такой информации будет уголовно наказуемым лишь в силу того, что она содержится в компьютерах. Такая ситуация, на наш взгляд, совешенно не способствует вынесению справедливых приговоров и единообразному применению статей 259-261 Уголовного кодекса РМ.

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, а глава XI Уголовного кодекса РМ стала называться «Преступления в области информатики и электросвязи».

К настоящему времени уголовное законодательство РМ претерпело существенные изменения, вызванные появлением преступности в области информатики и электросвязи. Однако остаётся еще множество неурегулированных правовых проблем, что не позволяет эффективно противодействовать преступлениям в области информатики и электросвязи. Полагаем, что следует продолжить научные исследования проблем криминализации и декриминализации противоправных деяний в области информатики и электросвязи для совершенствования и создания теоретической базы соответствующих норм Уголовного кодекса РМ с учетом международного опыта законотворчества в этой области.

Литература:

1. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. - Москва, 2002, с.375-414.
2. Меры по борьбе против преступлений, связанных с использованием компьютеров // Материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями: A/CONF.203/14. Бангкок, 18-25 апреля 2005 года.
3. Окинавская Хартия глобального информационного общества (принята 23.07.2000 г. на Окинаве (Япония) на совещании руководителей глав государств и правительств стран «Группы Восьми»).
4. Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» / Научн. ред. проф. Б.В. Волженкин. - СПб., 1998, с.20-21.
5. Уголовный кодекс Республики Молдова №985-XV от 18.04.2002 // Официальный Монитор Республики Молдова. - 2002. - № 128-129. - Ст.1012.
6. См. там же.
7. Макарь И.М. Уголовное право Республики Молдова. Часть Особенная. - Кишинев: CEP USM, 2004, с.318-319.

Prezentat la 10.05.2007