УДК 349.9:004

Солнцев М.Н.,
студент юридического факультета
Орловского филиала ФГБОУ ВПО «Российская академия
народного хозяйства и государственной службы
при Президенте РФ»

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В статье рассмотрены проблемы борьбы с компьютерными преступлениями, выделены тенденции компьютерных преступлений за рубежом. Представлен анализ отечественного законодательства в сфере компьютерной информации в России.

Ключевые слова: безопасность компьютерной информации; информационная безопасность; компьютерная преступность.

Экономика и обороноспособность ведущих государств мира во многом зависят от нормального функционирования глобальных компьютерных сетей. Нарушение их работоспособности может повлечь серьезные последствия, а национальные и международные правовые институты и организационные структуры практически не готовы к адекватному противодействию новым угрозам[6]. Современная компьютерная преступность характеризуется разнообразием объектов преступного посягательства. Известны неоднократные случаи незаконного проникновения "компьютерных вундеркиндов" к закрытой информации ряда государств, составляющей государственную тайну. Распространяемые вредоносные программы приводят к утрате компьютерной информации у тысяч владельцев этой информации. Объектом компьютерных преступлений выступает целый круг охраняемых любым государством общественных отношений в сфере национальной, общественной, информационной безопасности, экономики, соблюдения чести и достоинства личности и т.д.

В последнее время наибольшее распространение в отечественной юридической литературе получил термин «компьютерное преступление». Анализ различных точек зрения на это явление позволяет выделить, как минимум, три основных устоявшихся подхода. Приверженцы первого считают компьютерным преступлением противоправные деяния, в которых компьютеры (системы, сети, компьютерная информация) могут выступать как объектом, так и орудием преступного посягательства. Сторонники второго ограничивают компьютерные преступления только противоправными деяниями в сфере автоматизированной обработки информации, для которых орудием является компьютер, а в качестве объекта посягательства выступает компьютерная информация. Представители третьего подхода, обоснованно полагая, что в строго юридическом смысле термин «компьютерное преступление» весьма уязвим, предлагают заменить его другим. Более удачным им представляется термин «информационное преступление», в силу того что объектом преступных посягательств является не техника, а информация, хранящаяся, обрабатываемая, передаваемая этой техникой.

Изучение показывает, что теория уголовного права в различных странах поразному подходит и к закреплению обязательных и факультативных элементов компьютерного преступления как самостоятельной категории; отсутствует единство в понимании его уголовно-правовых признаков и, следовательно, в определении круга деяний, которые должны быть отнесены к компьютерным преступлениям.

Таким образом, понятие «компьютерное преступление» представляется в настоящее время не вполне определенным, не имеющим четких границ, но широко используемым в специальной литературе.

В настоящее время в нашей стране накоплена богатая научно-теоретическая и законодательная база, которая свидетельствует о складывающемся устойчивом правовом механизме, нацеленном на защиту компьютерной информации. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за преступления в сфере компьютерной информации.

Однако в действующем российском законодательстве пока еще нет четкого представления о правовом механизме защиты компьютерной информации как целостной разработанной правовой системе[7].

Изучение зарубежного опыта борьбы с компьютерными преступлениями показало, что наиболее развернутым и проработанным в вопросе правового регулирования борьбы с компьютерной преступностью является законодательство США. Наряду с федеральными законами борьбу с компьютерной преступностью регулирует законодательство 50 штатов. Проведенный анализ законодательства большинства штатов позволяет утверждать, что везде выделяется два характерных преступления в сфере компьютерной информации: 1) несанкционированный доступ и 2) повреждение компьютерных данных. В области применения наказаний треть штатов сгруппировали все санкции в отдельной части кодекса, придерживаясь систематичности классификации преступлений и наказаний. В другой трети штатов виды наказаний указаны в самих законах по компьютерным преступлениям. В остальных случаях санкции привязаны к размеру нанесенного ущерба.

В Нидерландах, ФРГ и Швейцарии основные дополнения, касающиеся рассматриваемых преступлений, были внесены в национальные уголовные кодексы в качестве статей, содержащих составы как преступлений в сфере компьютерной информации, так и преступлений, связанных с компьютерами.

В России уголовная ответственность за преступления в сфере компьютерной информации впервые была предусмотрена в Уголовном кодексе РФ, вступившем в действие с 1 января 1997 г., в гл. 28 УК РФ "Преступления в сфере компьютерной информации". Предусмотренные в ч. 1 ст. 272 и ч. 1 ст. 274 УК РФ деяния отнесены к преступлениям небольшой тяжести, а эти же деяния при отягчающих обстоятельствах — к преступлениям средней тяжести. Только создание, использование и распространение вредоносных программ для ЭВМ (в том числе вирусы), повлекших по неосторожности тяжкие последствия, наказываются лишением свободы на срок до семи лет и относятся к категории тяжких преступлений. В 1996 г. названные выше нормы в самой минимальной степени удовлетворяли потребности правоприменительной практики. За истекший период компьютеризация проникла во все сфе-

ры жизни общества, а неправомерные посягательства на информацию, содержащуюся на электронно-магнитных носителях, причиняют не только огромный экономический ущерб, но и посягают на государственную безопасность, конституционные права человека, его честь и достоинство и т.д. Компьютерная преступность приобрела транснациональный характер. В этой связи возникла необходимость разработки новой системы преступлений в сфере компьютерной информации в России. При разработке этой системы следует учесть опыт зарубежных государств, где компьютерная преступность оказалась более распространенной и нанесла более серьезный ущерб. Успокаиваться относительно небольшим количеством регистрируемых преступлений в сфере компьютерной информации (по сравнению с зарубежными странами) не следует. Компьютерная преступность во всем многообразии ее форм растет, и уголовное право (наряду с другими мерами профилактического характера) должно быть реальным средством по предупреждению этих опасных преступлений.

Анализ отечественного законодательства в сфере компьютерной информации позволяет отметить ряд недостатков, затрудняющих расследование неправомерного доступа к компьютерной информации:

- сложность конструкций правовых норм (ст. 272 УК РФ), наличие в них технических понятий и специальных терминов. (Значительная сложность возникает в уяснении терминологии, назначении составных частей ЭВМ, системы ЭВМ и их сети, понимании общего режима их функционирования в различных технологических процессах);
- обилие и порой противоречивость нормативных актов, определяющих правовой статус и специфику компьютерной информации;
- отсутствие обобщений следственной и судебной практики, которые могли бы быть ориентиром в правильной квалификации преступлений;
- сложности разграничения смежных составов преступлений.

С внедрением новых компьютерных технологий, когда обмен информацией стал быстрым, дешевым и эффективным, преступность в информационной сфере переросла за рамки уголовно-правовых норм, направленных для борьбы с ней. Компьютерная преступность не знает границ, она выходит за пределы российской действительности. Это международное понятие, и бороться с ней надо согласованно и сообща. К числу мер по снижению деятельности субъектов, виновных в совершении преступлений в сфере компьютерной информации, на территории СНГ и стран Балтии можно отнести следующие: необходимо регулярно проводить усовершенствование законодательной базы и повышение уровня компетенций правоохранительных органов, также важным фактором противодействия киберпреступникам является разработка и внедрение инновационных технических средств и решений, которые позволяют реализовать проактивный отклик на выявленные инциденты и практически мгновенную реакцию на угрозы информационной безопасности.

В 2011 году фиксируется значительное расширение "русского" рынка преступлений в сфере компьютерной информации и соответствующий рост доходов хакеров. При сохранении существующих условий можно прогнозировать дальнейшее обострение этой проблемы. Для того чтобы эффективно способствовать снижению современных темпов роста "русского" рынка киберпреступности, необходимо ужесточить наказания, активизировать межгосударственную работу, привлечь к сотрудничеству отраслевые ассоциации, проводить обучение на регулярной основе среди сотрудников государственных структур и популяризировать фундаментальные политики информационной безопасности среди населения.

Проблемы информационной безопасности постоянно усугубляются процессами незаконного, несанкционированного проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего компьютерных вычислительных систем. Не случайно поэтому защита компьютерной информации становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных — защиту от несанкционированных сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;
- конфиденциальность (законность) информации;
- доступность для всех авторизованных зарегистрированных пользователей;

 защиту компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка) [1]

Анализ действующего российского уголовного законодательства в сфере компьютерной информации позволяет говорить о необходимости нескольких правовых проблем, которые могут быть рассмотрены в качестве составных частей правового механизма защиты компьютерной информации:

– установление контроля над несанкционируемым, противоправным доступом к компьютерным информационным данным системы;

– ответственность за выполнение технологических операций, связанных с правовой защитой компьютерной информации.

Ситуация с преступностью в сфере компьютерной информации осложняется существенным обстоятельством – высоким уровнем ее латентности. По усредненным оценкам, 80–90% преступлений в сфере компьютерной информации остаются «невидимыми» для зарубежных правоохранительных органов.

«Невидимость» преступления в сфере компьютерной информации обусловлена во многом отсутствием стремления самих жертв заявлять в правоохранительные органы из-за нежелания публичной огласки, привлечения к уголовной ответственности собственных сотрудников, незнания об уголовном характере правонарушения.

Путями преодоления латентности преступлений в сфере высоких технологий, в том числе и неправомерного доступа к компьютерной информации, можно назвать следующие:

– использование социологических методов и приемов выявления и измерения латентной преступности в сфере компьютерной информации: массовый опрос населения, анкетирование, экспертные оценки, контент-анализ материалов средств массовой информации;

– преодоление правового нигилизма руководителей учреждений, предприятий, организаций и отдельных граждан путем освещения проблем компьютерной преступности в средствах массовой информации;

– повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов.

Литература

1. Амелин Р.В. Информационная безопасность. [Электронный ресурс]/Режим доступа – http://nto.immpu.sgu.ru/system/files/3/__77037.pdf

2. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение [Текст]: автореф. дис. ... канд. юрид. наук. – М., 2003. – 28 с.

3. Крылов В.В. Расследование преступлений в сфере информации [Текст]. – М., 2005. – 168 с.

4. Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть [Текст] / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 2008. – 866 с.

5. Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. [Электронный ресурс] / Режим доступа – http://kurgan.unets.ru/~procur/my_page.htm, 1999

6. Щеголева Н.А.Право на участие в управлении делами государства: понятие и ограничения // Среднерусский вестник общественных наук. – 2011. – № 3. – С. 114–116.

7. Щеголева Н.А., Шашкова А.А.Информационное общество и государство: специфика взаимодействия (правовой анализ) // Среднерусский вестник общественных наук. – 2010. – № 4. – С. 134–140

Solntsev M.N., e-mail: vestnik.gmu@yandex.ru
Student of the Orel branch of FSBEE HPE "Russian Academy of National Economy and Civil Service under the President of the Russian Federation".

CRIMINOLOGICAL DESCRIPTION OF CRIMES IN THE SPHERE OF COMPUTER INFORMATION

The problems of computer crimes prevention are considered in the article, the tendencies of computer crimes abroad are singled out. The analysis of home legislation in the sphere of computer information in Russia is presented.

Key words: security of computer information, information security, computer crimes.