УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ

УДК 343.45

И.Р. БЕГИШЕВ,
соискатель

Институт экономики, управления и права (г. Казань)

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРИОБРЕТЕНИЕ ИЛИ СБЫТ ЦИФРОВОЙ И ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ, ЗАВЕДОМО ДОБЫТОЙ ПРЕСТУПНЫМ ПУТЕМ

Статья посвящена анализу преступных деяний в сфере обращения цифровой и документированной информации. Рассматривается вопрос о признании информации имуществом. Выявляется пробельность в вопросе об установлении уголовной ответственности за приобретение или сбыт цифровой информации, заведомо добытой преступным путем. Предлагается авторский вариант решения данной проблемы.

Современный век высоких технологий немыслим без оперативного обмена информацией. Цифровая информация окружает нас повсюду: в работе за компьютером, при передаче данных в системах мобильной связи, при работе с использованием беспроводных технологий передачи данных, в сети интернет и т.д. Порой цифровая информация является не только объектом преступных посягательств, но и объектом экономической деятельности.

По данным аналитического отчета компании "InfoWatch", специализирующейся на защите конфиденциальной информации, в первом полугодии 2009 г. было установлено 413 инцидентов утечки информации из организаций: из них 64,2% из коммерческих организаций, 21,3% из государственных организаций, 10,4% из некоммерческих и образовательных организаций, 4,1% из неустановленных организаций. По видам этих утечек информации к умышленным утечкам отнесены 55,9%, к случайным 39,0%, к неустановленным – 5,1% всех утечек информации. По типу информации все утечки делятся на следующие: персональных данных – 87,2%, коммерческой тайны, ноу-хау – 2,9%, государственной и военной тайны – 2,2 %, другой конфиденциальной информации – 6,8%, неустановленного вида – 1,0% от числа всех зафиксированных утечек. Необходимо отметить, что данные о вышеназванных утечках включают все инциденты во всех странах мира, информация о которых была опубликована в СМИ, а также блогах, веб-форумах и других сетевых ресурсах [1].

Ограничение оборота цифровой информации, заведомо добытой преступным путем, является ключевым фактором противодействия преступлениям в сфере высоких технологий и, несомненно, нуждается в уголовно-правовой защите.

Часто цифровая информация, циркулирующая в компьютерных и телекоммуникационных системах и их сетях, становится объектом преступных посягательств. Похищенная циф-

ровая информация передается, например, заказчику за вознаграждение. Примерами соответствующих правонарушений могут служить следующие деяния:

1) перехват, запись на технический носитель информации или сбыт полученной информации из систем мобильной и спутниковой связи;

2) кража и вымогательство цифровой информации об абонентах и клиентах различных организаций с последующей реализацией данной информации;

3) кража персональных данных и кредитных историй граждан с целью их последующей реализации или использования в незаконных целях.

Постоянные предложения приобрести различные (в большинстве своем ведомственные) базы данных свидетельствуют о том, что продажа конфиденциальных сведений о гражданах и юридических лицах стала отдельным видом бизнеса. Если появление очередной опубликованной базы для граждан является просто еще одним малоприятным фактом обнародования сведений об их частной жизни, то на некоторых предприятиях это может отрицательно повлиять на бизнес. Например, для оператора сотовой связи распространение базы биллинга может обернуться существенным оттоком абонентов к более "надежному" оператору-конкуренту. Поэтому оператору подчас экономически более выгодно найти "производителя", подготовившего украденную базу к продаже, и выкупить весь тираж. Но проблема перекрытия возможных утечек при этом остается весьма актуальной [2].

Существенным пробелом в УК РФ является отсутствие нормы, устанавливающей ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем. Под признаки ст. 175 УК РФ "Приобретение или сбыт имущества, заведомо добытого преступным путем" не подпадают приобретение и сбыт заведомо добытой преступным путем цифровой информации.

Предметом состава преступления, предусмотренного ст. 175 УК РФ, выступает имущество, заведомо добытое преступным путем. К имуществу относят ценные бумаги, движимые и недвижимые вещи (строения, например дачи, коттеджи, автотранспорт, товары, сырье, материалы и т.д.). Понятием имущества охватываются и деньги, например валюта, похищенная из обменного пункта или из квартиры [3, с. 156].

Законодатель указывает, что имущество, выступающее в качестве предмета преступления, должно быть добыто преступным путем. Способами такой добычи являются, прежде всего, различные виды хищений, вымогательство, получение взятки, коммерческий подкуп, незаконное получение кредита, подкуп участников и организаторов профессиональных спортивных соревнований и зрелищных коммерческих конкурсов, браконьерство.

Кроме того, предметами преступления, предусмотренного ст. 175 УК РФ, не могут быть драгоценные металлы, природные драгоценные камни, ядерные материалы или радиоактивные вещества, оружие или его основные части, боеприпасы, взрывчатые вещества и взрывные устройства, наркотические средства или психотропные вещества, сильнодействующие или ядовитые вещества. Их незаконное приобретение наказывается, соответственно, по ст. ст. 191, 220, 222, 228, 234 УК РФ.

Информацию обычно не признают имуществом, и поэтому манипуляции с ней не подлежат ответственности по ст. 175 УК РФ именно по той причине, что под имуществом там понимают совокупности вещей и материальных ценностей, состоящих во владении какого-либо лица. Думается, что цифровая информация имеет некоторую схожесть с другими вещами и материальными ценностями. Однако между ними имеется принципиальное различие: цифровую информацию, по сравнению, например, с драгоценным металлом или ценной бумагой, являющимися материальными ценностями, невозможно потрогать и ощутить, хотя носитель информации (например, компьютер), на котором находится цифровая информация, является материальной ценностью. Компьютер, таким образом, может являться предметом преступления, предусмотренного ст. 175 УК РФ.

Как считает О.Н. Крапивина, имущество, по смыслу ст. 175 УК РФ, состоит из вещей, инди-

видуально определенных и определенных родовыми признаками, потребляемых и непотребляемых; одушевленных и неодушевленных. Имущественные права и нематериальные блага не могут выступать в качестве предмета преступления, предусмотренного ст. 175 УК РФ. В силу нематериального происхождения к предмету преступного приобретения (сбыта) по уголовному закону РФ также не могут быть отнесены идеи, взгляды, информация, компьютерная информация, электрическая и тепловая энергия [4, с. 12].

Цифровая информация, выступающая в качестве предмета преступления, должна быть добыта преступным способом.

Что же это за преступные способы добычи цифровой информации?

Предполагается, что преступными являются способы добычи цифровой информации, предусмотренные в ст. ст. 272 "Неправомерный доступ к компьютерной информации" и 273 "Создание, использование и распространение вредоносных программ для ЭВМ" УК РФ. Так, например, неправомерный доступ к охраняемой законом компьютерной информации может повлечь за собой копирование информации, а распространенная в информационно-телекоммуникационной сети вредоносная программа может найти, скопировать и переслать ценную информацию в "чужие руки".

Существует и иной способ добычи цифровой информации, не предусмотренный УК РФ, – это перехват цифровой информации, распространяющейся посредством радиоволн в эфире. К ней можно отнести все правонарушения, посягающие на сведения, циркулирующие в современных сетях передачи данных Wi-Fi, Bluetooth и подобных.

Простая радиостанция стоимостью в пару сотен долларов позволит перехватывать многие секретные передачи. Обычно "говорят" морзянкой, но также используют и человеческий голос, а в последнее время много информации передают в "компьютерном" варианте. Конечно, радиоперехват не имеет никакого отношения к локальным сетям, но от этого его популярность не уменьшается. В эфире можно услышать много такого, что не найдешь ни на одном из серверов [5, с. 75].

Цифровую информацию, добытую тем или иным преступным путем, можно успешно сбыть или приобрести.

На практике к такой информации относят следующие виды:

– конфиденциальную и служебную информацию;

– персональные данные;

– сведения в цифровой форме, составляющие коммерческую, налоговую или банковскую тайну;

– сведения, составляющие государственную тайну.

Незаконное копирование такой информации наносит ущерб ее собственнику или владельцу.

Следует отметить, что в ст. ст. 138, 183, 283 УК РФ указаны виды тайн, которые защищены законом, однако уголовная ответственность за приобретение и сбыт таких сведений, заведомо добытых преступным путем, в них не установлена.

Представляется необходимым ограничить преступные действия, связанные с приобретением и сбытом цифровой информации, добытой заведомо преступным путем от деяний, предусмотренных ст. ст. 146 и 147 УК РФ.

В России "рыночного образца" можно купить почти все. В том числе, полное досье на ближнего и дальнего своего, в котором будут указаны подробности из жизни нужной персоны: от банковского счета до номера «квартиры, где деньги лежат». Информационные пираты спокойно берут на абордаж всех, кого угодно, даже крупнейшие частные и государственные организации.

Совершенно очевидно, что на распространение и тиражирование скопированных данных у "пирата" нет никаких официальных прав. А установить нелегалов бывает очень легко: по тому же контактному телефону с продавцами конфиденциальной информации могут связаться и сотрудники правоохранительных органов. Резонно спросить: куда же смотрит, к примеру, УБЭП?

– Туда, куда надо, – отвечает пресс-секретарь УБЭП ГУВД г. Москвы Филипп Золотниц-

кий. – Наблюдение за деятельностью этих мошенников ведется постоянно. Но задержать их не так легко, как кажется. Торговец базами данных ответственности за утечку информации из той или иной организации не несет. Его можно только оштрафовать за реализацию нелицензированного товара и конфисковать этот самый товар. Но чтобы аналогичная продукция снова не появилась в продаже, надо раскрыть всю цепочку аферистов. Это долгий процесс: продавец зачастую плохо знает даже хозяина торговой точки, не говоря уже о личности человека, через которого непосредственно происходит утечка информации из фирмы. А поиск "высокотехнологичных" преступников не совсем наш профиль [6].

Следует отметить, что помимо цифровой информации незаконные действия с документированной информацией также могут нанести гражданам и организация непоправимый ущерб. Например, кража ценных бумаг, платежных документов, бизнес-планов и иных документов, содержащих сведения конфиденциального характера может отрицательно повлиять на репутацию организации. Ярким примером этого является следующее событие: конфиденциальная медицинская информация пациентов одного из дорогих частных госпиталей Великобритании была продана сыщикам, работавшим под прикрытием. Сотни документов, содержащих личную информацию о состоянии здоровья пациентов, домашние адреса и даты рождения, предлагались по £4 за каждый [7].

Учитывая, что ст. 175 УК РФ не содержит указания на такой предмет, как цифровая и документированная информация, и в связи с вышесказанным, предлагаем установить ответственность за сбыт и приобретение цифровой и документированной информации, заведомо добытой преступным путем, и ввести соответствующую норму в УК РФ в следующей редакции:

Статья 272.1 Приобретение или сбыт охраняемой законом цифровой и документированной информации, заведомо добытой преступным путем, –

наказывается ...

Квалифицирующим признаком приобретения и сбыта цифровой и документированной информации, заведомо добытой преступным путем, может быть совершение его организованной группой или лицом с использованием своего служебного положения, что довольно часто встречается на практике.

Список литературы

1. Аналитический отчет "Глобальное исследование утечек. Первое полугодие 2009". – URL: http://www.infowatch.ru/threats_and_risks/analytical_reports/2811

2. Безопасность баз данных. Что, от кого и как надо защищать. – URL: http://www.aladdin.ru/press-center/publications/publication5219.php?print=Y&ID=5219

3. Лебедева В.М. Комментарий к Уголовному кодексу Российской Федерации. – М.: Норма, 2007. – С. 156.

4. Крапивина О.Н. Приобретение или сбыт имущества, заведомо добытого преступным путем: сравнительно-правовое, уголовно-политическое и криминологическое исследование: автореф. дис. … канд. юрид. наук. – М., 2008. – С. 12.

5. Касперски К. Взлом Пентагона. Как взломать закрытую сеть // Спецхакер. – 2005. – № 10. – С. 75.

6. Ермакова М. Секретные материалы по доступной цене // Российская газета. – 2004. – 22 июня (Фед. вып. № 3507).

7. Великобритания: данные пациентов продаются на чёрном рынке. – URL: http://www.dailymail.co.uk/news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input--end-black-market.html

В редакцию материал поступил 05.02.10.

Ключевые слова: информация; преступления, посягающие на информацию.