Незаконное получение сведений, составляющих коммерческую тайну, и преступления в сфере компьютерной информации: проблемы соотношения.

Паршуков М. И.
Начальник исследовательского отдела Исследовательского центра правовых проблем информационной безопасности УрГЮА, к.ю.н.

В условиях жесткой конкуренции успех в бизнесе и получение прибыли в предпринимательской деятельности во многом зависят от сохранности в тайне секретов производства, интеллектуального потенциала и технологий.

В сложившейся ситуации предприниматель старается всеми возможными способами обеспечить неизвестность третьим лицам ценной его бизнесу информации. Такая информация, как правило, и составляет коммерческую тайну, т.е. она имеет действительную или потенциальную коммерческую ценность в силу неизвестности, к ней нет свободного доступа на законном основании и в отношении нее введен режим коммерческой тайны.

Однако обеспечить сохранность коммерчески ценных сведений не всегда удается. Встает необходимость привлечения виновных лиц к ответственности.

Нормы, устанавливающие ответственность за незаконное разглашение коммерческой тайны, содержатся в Федеральном законе «О коммерческой тайне», Гражданском кодексе РФ, Трудовом кодексе РФ, Кодексе об административных правонарушениях РФ, Уголовном кодексе РФ.

Однако возможность привлечения к ответственности лица незаконно получившего сведения, составляющие коммерческую тайну, предпринимателя предусматривается лишь Уголовным кодексом РФ.[1]

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996. № 25. ст. 2954.

Так ч.1 ст. 183 УК РФ определяет незаконное получение сведений, составляющих коммерческую тайну, как собирание сведений, составляющих коммерческую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом. Здесь же устанавливаются виды наказания и пределы ответственности за это преступное деяние.

Под похищением в данной статье понимается как изъятие подлинников документов, так и временное завладение этими документами в целях их фотографирования снятия копий или описания.[2] Похищение может носить тайный или открытый характер, осуществляться путем обмана или с применением насилия.

Под подкупом следует понимать передачу лицу, обладающему рассматриваемой информацией, денег, ценных бумаг, иного имущества, а равно оказание ему услуг имущественного характера за выдачу этой информации. Иногда в юридической науке понятие подкупа включается также и обещание предоставить имущество или услуги.[3]

Угроза - это психическое насилие, которое может применяться как в отношении самих лиц, владеющих информацией, составляющей коммерческую тайну, так и в отношении их близких.

К иным незаконным способам относятся, например, беседы о найме на работу со служащими конкурирующих фирм при отсутствии намерения принимать данного служащего на работу, подслушивание разговоров или скрытое наблюдение с использованием различных специальных технических устройств.

Все перечисленные способы обладают таким признаком, как незаконность.

---

[2] Анашкин Г. З. Ответственность за измену Родине и шпионаж. М., 1964. С. 134; Клягин В. С. Ответственность за особо опасные государственные преступления. Минск, 1973. С. 142 - 143. Цит. по Хакулов М. Х. О составе преступления, предусмотренного ст. 183 УК РФ // Российский следователь, 2006, N 6

[3] Уголовное право России. Особенная часть: Учебник / Под ред. А.И. Рарога. М., 1998. С. 174.

Повсеместное распространение ЭВМ сделало ее основным средством формирования, обработки, использования и хранения информации. В связи с этим появились особые конфиденциальные (доверительные) общественные отношения между операторами ЭВМ в информационных системах предпринимательской деятельности, возникающие по поводу коммерческой тайны, которые сразу стали объектами преступных посягательств.

Уголовный кодекс РФ предусматривает 3 вида преступлений в сфере компьютерной информации. Это неправомерный доступ к компьютерной информации (ст.272); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В ч.1 ст. 272 УК РФ речь идет о неправомерном доступе к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; в ч.1 ст. 273 УК РФ – о создании программ для ЭВМ или внесении изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Каким же образом соотносятся преступления, направленные на незаконное получение сведений, составляющих коммерческую тайну, и преступления в сфере компьютерной информации, если речь идет о конфиденциальной коммерческой информации, содержащейся на электронных носителях?

Представляется целесообразным выделить две модели их соотношения:

1. Преступное деяние квалифицируется либо как преступление, направленные на незаконное получение сведений, составляющих

коммерческую тайну, либо как преступление в сфере компьютерной информации.

В данном случае определяющим разграничивающим критерием будет субъективная сторона составов названных преступлений.

Так, например, в составе, предусмотренном ч.1 ст.183 УК РФ, обязательным признаком субъективной стороны является цель преступления – незаконное получение сведений, составляющих коммерческую тайну. В силу этого не является преступлением в сфере компьютерной информации хищение CD-диска со сведениями, составляющими коммерческую тайну.

Неправомерный доступ к информации, составляющей коммерческую тайну, содержащейся на машинном носителе, в ЭВМ, системе ЭВМ или их сети, совершенный без цели получения доступа к именно такой конфиденциальной информации, без цели ее дальнейшего использования или разглашения, а равно без корысти или иной личной заинтересованности, влечет ответственность по ст. 272 УК РФ. Признаки состава преступления, предусмотренного ст. 183 УК РФ в этом случае отсутствуют.

2. Преступление в сфере компьютерной информации является способом совершения преступлений, направленных на незаконное получение сведений, составляющих коммерческую тайну. В таких случаях имеет место идеальная совокупность преступлений, что, прежде всего, определяется различием объектов посягательства. Так, например, незаконное получение сведений, составляющих коммерческую тайну, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности преступлений, предусмотренных ст. 183 и ст. 272 УК РФ.

Хорошим примером может послужить уголовное дело, рассмотренное Тагилстроевским районным судом города Нижнего Тагила Свердловской области по обвинению Р. по ст. 159, 183, 272, 273 УК. В октябре-ноябре 1998 года Р., пользуясь своим служебным положением, совершил изменение ведомости начисления заработной платы на предприятии так, что у

работников, которым начислялось более ста рублей, списывалось по одному рублю, эти средства поступали на счет, откуда их впоследствии снял Р. Изменения в программе были квалифицированы по статье 273, сбор сведений о счетах лиц, данные о которых были внесены в базу предприятия, - по статье 183, модификация этих данных - по статье 272, а получение начисленных денежных средств – по статье 159 УК РФ. Р. был приговорен к 5 годам лишения свободы условно с лишением права заниматься профессиональной деятельностью программиста и оператора ЭВМ сроком на 2 года.

С принятием в 2004 г. Федерального закона «О коммерческой тайне» [4]ситуация несколько поменялась.

Законодатель определил необходимый набор мероприятий по охране конфиденциальности информации, который в обязательном порядке должен включать в себя следующее:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных

[4] Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» // Российская газета. 05.08.2004. № 166.

предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Стоит отметить, что данное положение ориентировано исключительно на традиционные бумажные формы делопроизводства и не учитывает современных, цифровых способов создания, хранения и передачи информации, а также ее защиты.

Непринятие перечисленных выше мер лишает предпринимателя права на защиту ценой информации в режиме коммерческой тайны.

Таким образом, в силу существующих пробелов в действующем законодательстве в правоприменительной практике складывается ситуация, когда преступное деяние, совершенное с целью незаконного получения информации, составляющей коммерческую тайну, содержащейся на машинном носителе, в ЭВМ, системе ЭВМ или их сети не может быть квалифицировано должным образом. Возможно, оно будет квалифицировано следователем, прокурором, судьей лишь как неправомерный доступ к компьютерной информации, что не отражает суть совершенного преступления.

В сложившейся ситуации представляется необходимым внести соответствующие изменения в Федеральный закон «О коммерческой тайне», определив тем самым статус коммерчески ценной конфиденциальной информации на электронном носителе.