DIRECTIONS OF LEGAL POLICY IN THE SPHERE OF PUBLIC BANKING LIABILITY

V.V. Stepanova, senior lecturer of chair "Theory of state and law"
Togliatti State University, Togliatti (Russia)

Abstract: The article analyzes common offences in the field of banking relationships and suggest possible directions of legal policy in the sphere of public banking liability.

Keywords: legal responsibility, financial responsibility, violation, offense, banking violation, banking offense, bank.

УДК 343.7

КОММЕРЧЕСКИЙ ШПИОНАЖ

В.В. Хилюта, кандидат юридических наук,
заведующий кафедрой «Уголовное право и криминология»
Гродненский государственный университет имени Янки Купалы,
Гродно (Республика Беларусь)
В.В. Гладышев, магистр юридических наук,
старший преподаватель кафедры «Хозяйственное право»
Гомельский государственный технический университет имени П.О. Сухого,
Гомель (Республика Беларусь)

Аннотация: В статье отражена актуальность проблемы защиты информационной безопасности в современный период развития информационного общества. Авторами исследуются вопросы надлежащей защиты информационной безопасности субъектов экономической деятельности уголовно-правовыми средствами, в частности уголовно-правовая охрана коммерческой и банковской тайны. Проведен анализ авторефератов кандидатских диссертаций по исследуемому вопросу, судебно-правовой практики в Республике Беларусь по коммерческому шпионажу. Впервые предложены подходы дальнейшего совершенствования уголовно-правового закона этой проблемы.

Ключевые слова: информационная безопасность, коммерческая тайна, банковская тайна, компьютерная информация, уголовно-правовая охрана, коммерческий шпионаж.

Современный период развития цивилизации характеризуется переходом к новому типу общества – обществу информационному. Внедрение и развитие информационных технологий создает предпосылки для качественно нового витка цивилизации и предоставляет уникальные возможности для экономико-политических систем, общества, государства и граждан. Информация становится наиболее ценным товаром, уже превышающим по стоимости природные, финансовые, трудовые и иные ресурсы. Естественно, что в таких условиях резко возрастает значимость защиты информации, прежде всего той, доступ к которой ограничен ее конфиденциальным характером [1].

Коммерческая и банковская тайна неразрывно связаны с понятием «конкуренция», т. к. именно конкуренция является одним из важнейших факторов эффективного развития рыночной экономики. Конкурентная борьба неизбежно предполагает сохранение в тайне сведений, обладание которыми посторонними лицами могло бы ослабить экономические позиции субъектов хозяйствования и нанести им невосполнимый ущерб.

Главный принцип для производителей товаров, действующих в рамках маркетинговой концепции рыночных отношений, – производить то, что продается, а не продавать то, на основании чего производится. Спрос на продукцию регулирует предложение, определяющее количество, качество и стоимость производимых товаров [2]. Таким образом, использование своих сильных сторон и укрепление (или сокрытие) слабых – основа маркетинговой стратегии производителя и защиты коммерческой (промышленной) тайны.

Тем не менее положительные результаты в конкурентной борьбе могут быть и не достигнуты, если информация (коммерческая тайна) о товаре, работах и услугах, их качестве, ассортименте, сроках введения на рынок и т. д. станет известна конкурентам. Следовательно, обеспечение надлежащей сохранности и защиты коммерческой или банковской тайны является одной из центральных задач субъекта хозяйствования в деле занятия экономической деятельностью.

Дело в том, что неправомерное получение и использование в своей деятельности чужих научных достижений, технологий, управленческих решений и схем, другой информации, составляющей коммерческую или банковскую тайны, имеет своим следствием приобретение безосновательных преимуществ конкурентом, овладевшим этой информацией, что в конечном счете ведет к исчезновению стимулов для развития и совершенствования форм и способов экономической деятельности и, как следствие, наносит прямой ущерб владельцам коммерческой или банковской тайны.

Введение уголовной ответственности за коммерческий шпионаж было обусловлено значительной общественной опасностью этих действий, связанных с незаконным похищением и собиранием закрытой информации, что и потребовало надлежащей защиты информационной безопасности субъектов экономической деятельности уголовно-правовыми средствами [3; 4]. В этом отношении становление отечественного уголовного законодательства об ответственности за коммерческий шпионаж приходится на период перехода к более прогрессивному экономическому укладу, при котором возникновение и развитие новых экономических отношений, основанных на использовании определенных познаний, требует их надлежащей уголовно-правовой охраны от преступных посягательств конкурентов.

В настоящее время в ст. 254 УК предусмотрена ответственность за *«похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования (коммерческий шпионаж)»*.

Итак, коммерческий шпионаж может быть совершен при наличии следующих условий: а) действия по похищению или собиранию конфиденциальной информации должны быть активными; б) они должны целенаправленно совершаться в отношении информации, к которой отсутствует свободный доступ и которая защищена особым режимом обеспечения ее конфиденциальности;

в) незаконные действия должны быть совершены умышленно и иметь определенную цель: разглашение или незаконного использование коммерческой или банковской тайны.

Являясь одним из видов недобросовестной конкуренции, коммерческий шпионаж представляет собой незаконное получение предпринимателем или иным лицом конфиденциальной информации противоправным путем с целью овладения ею для достижения технического, технологического или коммерческого преимущества, создания экономического превосходства, банкротства конкурента. Экономическая сущность коммерческого шпионажа – это экономия средств субъекта на разработку новых идей, продукции и т. д. за счет похищения или незаконного собирания сведений, составляющих конфиденциальную информацию, у конкурента. Фактически можно говорить о том, что с одной стороны, злоумышленник незаконным образом завладевает чужой информацией, а с другой – экономит свои средства на создание нового продукта за счет противоправного использования информации своего конкурента.

Важным аспектом правоприменения ст. 254 УК является определение способа совершения преступления. Похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, представляет собой акт завладения указанной информацией либо процесс ее поиска, обнаружения или накопления у лица, не допущенного к обладанию такой информацией, незаконными способами.

Собирание сведений, составляющих коммерческую или банковскую тайну, представляет собой деяние, выраженное в процессе поиска, обнаружения, фиксации, накопления, хранения таких сведений, совершенных незаконным способом. Фактически можно говорить о том, что собирание незаконным способом сведений представляет собой получение информации через преодоление принятых ее обладателем правовых, организационных, технических и иных мер по охране конфиденциальности этой информации. Эти сведения могут находиться в форме материальной вещи, магнитного носителя, в виде чертежа, модели, формулы, символов, технологии и т. д. При этом результат такого собирания, т. е. факт получения виновным таких сведений, не имеет никакого юридического значения и на квалификацию содеянного по ст. 254 УК не влияет [5]. Тем не менее данное действие является всего лишь этапом для дальнейшего разглашения или использования сведений, составляющих коммерческую или банковскую тайну.

Страховой агент В., покидая прежнее место работы – страховую компанию ООО, забрала распечатку клиентской базы по договорам КАСКО за последние три месяца. Списки содержали анкетные данные клиентов, их адреса и сроки окончания договоров и составляли коммерческую тайну ООО. Устроившись на работу в другую страховую компанию, В. стала переманивать автовладельцев, пользовавшихся услугами ООО, предлагая им более выгодные условия страхования. При этом В. разгласила данные клиентской базы ООО своей коллеге по новому месту работы – Х. Получив тревожные сигналы от страхователей, руководство ООО обратилось в правоохранительные органы с заявлением о возбуждении в отношении бывшей работницы В. уголовного дела по ст. 254 УК. Впоследствии В. было предъявлено обвинение по ч. 1 ст. 254 УК в совершении коммерческого шпионажа.

В уголовно-правовой литературе отмечается, что в целом собирание сведений, составляющих коммерческую или банковскую тайну, является некой деятельностью, складывающейся из нескольких действий, объединенных в систему единой целью, которую преследует виновный, но это не есть разовое действие. Незаконное получение сведений, образующих коммерческую или банковскую тайну, может быть результатом собирания этих сведений, а может быть просто их получением. Как отмечает по этому поводу Н.А. Лопашенко, «собирание» и «получение» – это понятия, не совпадающие ни по объему, ни по содержанию [6]. Мы же полагаем, что все-таки термин «собирание» будет включать в себя и понятие получения сведений, т. к. собирание представляет собой сам процесс, и он может быть не всегда завершенным.

Похищение сведений, составляющих коммерческую или банковскую тайну, – это совершение действий, непосредственно направленных на завладение этими сведениями любым незаконным способом (путем кражи, грабежа, присвоения, обмана, злоупотребления доверием, вымогательства и т. д.), в результате которых такие сведения становятся известны лицу, не имеющему право на ознакомление с данной конфиденциальной информацией.

Способы коммерческого шпионажа, как правило, весьма разнообразны, и во многом такая преступная деятельность осуществляется на профессиональной основе с использованием традиционного набора шпионских методов и средств получения сведений, составляющих коммерческую или банковскую тайну. Чаще всего при совершении коммерческого шпионажа применяются следующие способы:

- подкуп работников организации, имеющих доступ к документам, содержащим коммерческую или банковскую тайну (получение вознаграждения или взятки лицом, обладающим такой информацией; «переманивание» сотрудника организации с целью использования его знаний о конфиденциальных источниках информации);

-склонение к разглашению коммерческой или банковской тайны сотрудников организации, имеющих доступ к конфиденциальным сведениям, а также лиц, сменивших прежнее место работы, или пенсионеров, имевших доступ к закрытой информации (с использованием подкупа, различных угроз, принуждения, вербовки и т. д.);

- внедрение агентов на должности, позволяющие получить непосредственный доступ к сведениям и документам, содержащим коммерческую или банковскую тайну, либо скрытно собирать информацию в процессе служебной (производственной) деятельности;

- использование источников информации в финансовых и налоговых органах, государственных структурах, правоохранительных органах с целью получения закрытой (конфиденциальной) информации субъекта хозяйствования;

- подкуп посредников в торговых переговорах;

- проведение разведывательного опроса (замаскированное выведывание сведений у осведомленных лиц, которые разглашают конфиденциальную информацию, не осознавая этого, с использованием специальных анкет и вопросников, рассылаемых организациями по почте, факсу и другими способами);

- перехват информации, циркулирующей в технических средствах и помещениях (служебных, жилых, производственных);

- прямое завладение документами, содержащими коммерческую или банковскую тайну (копирование такой информации, ее кража, подмена другими сведениями, похищение различных изделий, микросхем, агрегатов, технических документов, ноутбуков с конфиденциальной информацией и т. д.);

- собирание сведений, составляющих коммерческую или банковскую тайну, должностными лицами тех органов, которые имеют право такие сведения получать с нарушением порядка их получения, без надлежащих оснований, прямого похищения информации;

- использование специальных технических средств, предназначенных для негласного получения информации (акустический контроль помещения, автомобиля, непосредственного поведения человека и его переговоров; контроль и прослушивание телефонных перегово-

ров, факсовой и модемной связи; фото и видеосъемка, применение специальных оптических приборов для распознавания информации и т. д.);

- несанкционированный доступ к сведениям, содержащимся в средствах вычислительной техники и электронных банках данных (электромагнитный перехват; несанкционированный доступ в компьютерную сеть; непосредственный перехват компьютерной информации, который осуществляется через внешние коммуникационные каналы системы либо путем непосредственного подключения к линиям периферийных устройств; использование специальных аппаратных и программных программ перехвата информации) [7–11].

Так, следственным отделом управления КГБ по Могилевской области в отношении одного из работников ОАО «Белшина» было возбуждено уголовное дело. Б. обвинялся в коммерческом шпионаже и коммерческом подкупе. В частности, сотрудник ОАО «Белшина», занимавший должность экономиста отдела по работе со странами дальнего зарубежья с октября 2005 г., незаконно собирал сведения о финансовых операциях своего предприятия с иностранными компаниями. Чтобы получить данные о других организациях (объемах поставок, финансовых операциях и т. п.), экономист начал тайно копировать рабочие документы коллег, используя в этих целях сетевой сервер. Собранная на электронные носители информация за вознаграждение передавалась по Интернету с электронного адреса ОАО «Белшина» представителям компаний из США, Литвы, Англии и Австралии. В частности, Б. удалось заполучить документы, раскрывающие рыночную стратегию концерна «Белнефтехим» и входящих в него предприятий, данные о производственных мощностях шинного комбината, информацию о предполагаемых операциях по закупке и продаже товаров, тактике переговоров, круге лиц и фирм, с которыми предполагается их вести. Все эти сведения составляли коммерческую тайну предприятия.

В конце февраля 2007 г. из ООО «С», где был установлен режим коммерческой тайны, уволились два менеджера по продажам А. и Б.. После их увольнения выяснилось, что из офиса компании пропала клиентская база на бумажных носителях, которая составляла коммерческую тайну организации. Руководство ООО «С» обратилось в правоохранительные органы, и в последующем было установлено, что в январе 2007 г. А. и Б. учредили собственное юридическое лицо – ООО «В» с аналогичной сферой деятельности. Продолжая работать в ООО «С», они значительно завышали цены на продукцию для контрагентов данной организации и взамен предлагали товар по более низким ценам от имени ООО «В». При заключении договоров с контрагентами в интересах ООО «В» использовались сведения, относящиеся к учетной политике организации (клиентская база, цены на товар, планы поставок товара, условия заключения договоров, информация о ценообразовании и предполагаемых скидках, акциях, расчетах и т. п.). Указанные сведения составляли коммерческую тайну ООО «С» и использовались А. и Б. в деятельности ООО «В» в ущерб интересам ее обладателя, что отрицательно влияло на нормальную работу ООО «С». Правоохранительными органами в действиях А. и Б. были усмотрены признаки коммерческого шпионажа [12].

Следует также обратить внимание, что в ч. 2 ст. 254 УК почему-то не указан такой квалифицирующий признак, как «совершение преступления группой лиц по предварительному сговору». Повышенная общественная опасность подобных противоправных деяний очевидна, как и то обстоятельство, что коммерческий шпионаж не всегда совершается одиночками, а во многом благодаря согласованным действиям нескольких лиц, действующих в соучастии.

Так, Б., Д., К. примерно в августе 2010 г., при не установленных следствием обстоятельствах, вступили в предварительный сговор с неустановленными лицами на несанкционированный доступ к охраняемой законом компьютерной информации о персональных идентификационных номерах-кодах (далее по тексту ПИН-кодах) и реквизитах банковских карт путем незаконного тайного копирования перечисленной компьютерной информации с банковских карт при помощи специальных устройств, устанавливаемых на картоприемники банкоматов. Для совершения преступления неустановленные лица при неустановленных обстоятельствах, действуя согласно достигнутой договоренности, изготовили два специальных устройства в виде накладок на картоприемники банкоматов модели для тайного несанкционированного считывания информации с банковских карт, представляющих из себя радиоэлектронные сборки, смонтированные на двусторонних печатных платах. Среди радиоэлектронных компонентов на платах имелись микросхемы энергонезависимой памяти и видеоконтроллер. Также к плате на разъемном соединении был прикреплен модуль видеокамеры. Группа контактных площадок, к которым был припаян разъем, характерна для места монтажа разъема типа USB. По имеющимся характерным конструктивным признакам (номенклатура электронных компонентов, их взаимное расположение, наличие органов управления) радиоэлектронные сборки, которые закреплены на обоих устройствах, являлись видеорекордерами – устройствами видеонаблюдения, снабженными собственными средствами регистрации получаемой видеоинформации (на микросхему энергонезависимой памяти). К микрофонному входу, вместо микрофона, который в обоих устройствах удален, с помощью отрезков монтажного электрического провода были присоединены магнитные головки, закрепленные на вставках из полимерного прозрачного материала. После этого К., действуя согласно достигнутой договоренности, при неустановленных обстоятельствах получил от неустановленного лица указанные выше устройства и передал их Д. для последующей установки на банкоматы. Далее, Б. совместно с Д., действуя в соответствии с отведенными им ролями в совершении преступления, с целью неправомерного доступа к охраняемой законом компьютерной информации с помощью использования полученных от К. устройств, прибыли в кассовый зал, где подошли к банкомату, принадлежащему ОАО и, действуя тайно от окружающих, при помощи двустороннего скотча установили одно из указанных выше устройств на щель картоприемника банкомата, включив при этом внутреннее питание устройства для его запуска. В результате скрытно установленного на банкомат указанного технического средства Б., Д., К., действуя совместно с единым умыслом, незаконным способом скопировали информацию о реквизитах 59 банковских карт и ПИН-кодах к ним. При таких обстоятельствах Б., Д., К., действуя совместно и по предварительному сговору, не обладая правами на доступ к информации и работу с ней, осуществили неправомерный доступ к компьютерной информации, вводимой в электронно-вычислительную машину банкомата законным держателем банковской карты при наборе на клавиатуре ПИН-кода для доступа к своему банковскому счету, что повлекло несанкционированное копирование информации, выразившееся в переносе в память устройства, установленного Б. и Д. на картоприемник банкомата, информации о номерах и ПИН-кодах банковских карт, необходимых для проведения операций в банкомате, их обработки в процессинговом центре банка-эквайрера, серверах платежной системы, процессинговом центре банка-эмитента через систему дистанционного банковского обслуживания, в результате чего обладателю указанной конфиденциальной клиентской информации ОАО был причинен ущерб. Кроме того, Д., Б. и К. совершили собирание сведений, составляющих банковскую тайну, незаконным способом.

Указанный пример свидетельствует о том, что если лицо завладевает коммерческой или банковской тайной, которая одновременно является компьютерной информацией, и при этом нарушает доступ к компьютерной информации, то подобного рода действия должны квалифицироваться по совокупности преступлений. В данном примере – по ч. 1 ст. 254 УК и ч. 2 ст. 349 УК.

В принципе, коммерческий шпионаж имеет довольно широкое распространение на территории нашей страны, однако мизерные данные официальной статистики по такого рода делам объясняются достаточно высокой латентностью таких преступлений, хотя многие руководители субъектов хозяйствования в различной степени, но встречаются в своей профессиональной деятельности с похищением или незаконным собиранием сведений, составляющих коммерческую или банковскую тайну. Это и неудивительно, поскольку по своей социальной природе коммерческий шпионаж представляет собой профессиональные или любительские действия разведывательного характера, направленные на похищение или собирание информации с целью подавления конкурента или улучшения своих позиций перед контрагентом.

СПИСОК ЛИТЕРАТУРЫ

1. Клебанов Л.Р. Уголовная ответственность за незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну : автореф. дис. … канд. юрид. наук. М., 2001. 28 с.
2. Зубик В.Б., Зубик Д.В. Экономическая безопасность предприятия (фирмы). Минск: Вышэйшая школа, 1998. 391 с.
3. Лукашов А.И. Преступления против порядка осуществления экономической деятельности: уголовно-правовая характеристика и вопросы квалификации. Минск: Тесей, 2002. 256 с.
4. Артемов В.В. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, в уголовном праве России : автореф. дис. … канд. юрид. наук. М., 2011. 26 с.
5. Масленников А.В. Уголовная ответственность за незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну : автореф. дис. … канд. юрид. наук. Ставрополь, 2000. 31 с.
6. Лопашенко Н.А. Преступления в сфере экономики: авторский комментарий к уголовному закону. М.: Волтерс Клувер, 2006. 720 с.
7. Гамза В.А., Ткачук И.Б. Безопасность коммерческого банка. М.: Изд. Шумилова И.И., 2000. 216 с.
8. Клебанов Л.Р. Уголовно-правовая охрана коммерческой, налоговой и банковской тайны. М.: Юрлитинформ, 2006. 192 с.
9. Якоби С. Уголовно-правовые и криминологические проблемы предупреждения преступлений в сфере коммерческой банковской деятельности. М.: Камерон, 2004. 208 с.
10. Лукашов А.И., Мухин Г.Н. Конфиденциальная информация и коммерческая тайна: правовое регулирование и организация защиты. Минск: Тесей, 1998. 128 с.
11. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М.: Инфра-М, 2001. 301 с.
12. Овчаренко П. Уголовная ответственность за незаконное использование коммерческих секретов // Экономические преступления. 2009. № 7.

COMMERCIAL ESPIONAGE

V.V. Hilyuta, candidate of legal sciences, head of chair “Criminal law and criminology”
Yanka Kupala State University of Grodno, Grodno (Republic of Belarus)
V.V. Gladyshev, master of Law, senior lecturer of chair “Business Law”
P.O. Sukhoi State Technical University of Gomel, Gomel (Republic of Belarus)

Abstract: The article reflects the urgency of the problem of protection of information security in the modern period of development of the information society. The author investigates the question of adequate protection of information security subjects of economic activity by means of criminal law, in particular criminal and legal protection of commercial and banking secrecy. The analysis of the abstracts of master’s theses on the subject under investigation, the judicial practice of the Republic of Belarus for commercial spying. First proposed approaches to further improve the criminal-legal law this problem.

Keywords: information security, commercial secrecy, banking secrecy, computer information, data-criminal legal protection, industrial espionage.