УДК 343.98:343.534

О. В. КУРМАН,
канд. юрид. наук,
доцент кафедри криміналістики,
Національний університет
«Юридична академія України
імені Ярослава Мудрого»,
м. Харків

ОБСТАНОВКА ВЧИНЕННЯ ЗЛОЧИННИХ ПОСЯГАНЬ НА ВІДОМОСТІ, ЩО СТАНОВЛЯТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ

Розглянуто деякі особливості обстановки злочинів, пов'язаних із посяганнями на відомості, що становлять комерційну таємницю, визначено чинники, що сприяють вчиненню незаконних дій.

Ключові слова: обстановка злочину, комерційна таємниця, незаконне збирання відомостей, незаконне використання відомостей.

В умовах формування ринкової економіки в Україні за останнє десятиріччя відбулися корінні зміни у багатьох сферах діяльності держави. Однак ці зміни не завжди мають позитивний характер. Найжорсткіша конкурентна боротьба за ринки збуту, сфери вкладення капіталів та прагнення до отримання максимальних прибутків примушувала підприємців усіх рівнів уважно слідкувати за діяльністю своїх конкурентів. Для досягнення своїх цілей вони використовували як законні, так і незаконні способи отримання комерційно важливої інформації.

Інформація про результати чужих прикладних і фундаментальних досліджень дозволяє заощадити власні сили й кошти і зосередити всю увагу на виробництві та маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкуренції як «війни всіх проти всіх» роблять викрадення чужих таємниць особливо прибутковою, і тому дуже перспективною справою [5]. Економічним підґрунтям існування такої незаконної діяльності виступає конкуренція. Важливою умовою ефективності конкурентної боротьби є збереження у таємниці відомостей, заволодіння якими сторонніми особами може послабити економічні позиції підприємства та завдати йому шкоду. Дані відомості охоплюються поняттям комерційна таємниця.

Сьогодні з’явилися нові, раніше невідомі способи злочинів у сфері підприємництва та конкурентних відносин, що викликає необхідність розробки ефективних методик виявлення та розслідування цих злочинних деліктів. Основою методики розслідування будь-якого виду злочину є криміналістична характеристика. Дослідженню зазначеної криміналістичної категорії в науці приділялася значна увага. Так, даній проблематиці присвятили свої роботи такі вчені, як Р. С. Белкін [1, с. 731–739], В. А. Журавель [2, с. 138–156], Г. Г. Зуйков [4], О. Н. Колесніченко, В. О. Коновалова [6], В. Ю. Шепітько [10, с. 11–19; 12, с. 445–461] та ін. У той же час дослідження елементів криміналістичної характеристики злочинів, пов’язаних з незаконним отриманням комерційно значущої інформації, не знайшло належного відображення у спеціальній літературі. Певне місце в ієрархії елементів посідає обстановка злочину і, зокрема, причини та умови його вчинення. Між тим знання цих аспектів має велике значення для ефективної протидії з боку правоохоронних органів, розробки методики розслідування та рекомендацій заходів профілактики.

Говорячи про причини та умови вчинення злочинних посягань на відомості, що становлять комерційну таємницю, мають на увазі як об’єктивні (економічні, соціальні, законодавчі), так і суб’єктивні фактори. Так, до об’єктивних можна віднести умови, які складаються в результаті прийняття певних нормативно-правових актів, що регулюють конкурентні та інші відносини, що впливає на діяльність підприємства. Суб’єктивними чинниками є і неналежне виконання співробітниками підприємств своїх обов’язків, недбале ставлення до роботи, і пряма участь у злочинній діяльності.

Незаконному виходу інформації за межі підприємства можуть сприяти такі обставини.

1. Неналежна організація роботи системи конфіденційного документообігу:

– недостатній рівень оснащеності засобами технічного захисту конфіденційних матеріалів – сейфами, сховищами, пристроями для знищення документів;

– неналежний технічний стан зазначених засобів;

– використання сейфів, які частково втратили свої захисні властивості через втрату екземплярів ключів, розповсюдження інформації серед працівників щодо комбінації коду замка.

2. Неналежній рівень організації відбору претендентів на посади, пов'язані із доступом до конфіденційної інформації, а також контролем за діяльністю персоналу:

– низький рівень виробничої та службової дисципліни, несприятлива психологічна обстановка у колективі;

– залучення до роботи із секретними документами осіб, які не володіють достатніми вольовими якостями, непридатні до такої роботи за станом здоров'я та психологічними властивостями;

– часта зміна співробітників, які мають доступ до такої інформації.

3. Відсутність належного контролю за дотриманням режиму збереження комерційної та банківської таємниці, правил документообігу [11, с. 104].

Незаконному збиранню та використанню комерційної інформації сприяє те, що на підприємствах, де використовуються такі відомості, у багатьох випадках відсутні внутрішні документи, інструкції, що регламентують доступ співробітників до документів із конфіденційною інформацією. У таких інструкціях обов'язково повинно бути відображено:

1) функції керівництва у сфері захисту інформації;

2) механізм обліку інформації;

3) механізм забезпечення збереження інформації;

4) механізм доступу до відомостей представників правоохоронних та контролюючих органів[1];

[1] У зв'зку з прийняттям нового КПК України змінився і порядок доступу до документів із комерційною таємницею. Так, у ст. 162 введено нове поняття – «документи, які містять охоронювану законом таємницю». До охоронюваної законом таємниці відноситься конфіденційна інформація, в тому числі така, що містить комерційну таємницю. Згідно зі ст. 160 тимчасовий доступ до таких документів здійснюється на підставі ухвали слідчого судді, суду. Тепер для отримання судового дозволу для ознайомлення з такими документами представникам правоохоронних

5) порядок розповсюдження комерційної таємниці;

6) види відповідальності за розголошення відомостей;

7) термін, протягом якого інформація відноситься до комерційної таємниці. Відсутність типових внутрішніх правил щодо комерційної таємниці на підприємстві, які б містили основні вимоги до збереження документів, отримання доступу до них, роботи з конфіденційною інформацією сприяє вчиненню цього виду злочинів.

На сьогодні одним із розповсюджених методів незаконного збирання відомостей, що становлять комерційну таємницю, є використання комп'ютерної техніки та мережі Інтернет. Для цього злочинці застосовують спеціальні комп'ютерні програми, що дозволяють виконувати пошук необхідних даних та копіювати їх.

Програмні засоби, які використовуються для несанкціонованого доступу, поділяються на декілька видів [3, с. 56–58]:

– експлоіти (сканери) – програми, які використовують певні недоліки в програмному забезпеченні ЕОМ чи мережі, що призводить до настання бажаних для злочинця результатів;

– сніффери – дозволяють перехоплювати дані, що передаються по мережах електрозв'язку;

– «троянський кінь» – програми цієї групи приховано встановлюються будь-яким способом у комп'ютері, що цікавить злочинців, як правило шляхом вбудовування в іншу легальну програму. При цьому програма-носій, виконуючи свої прямі функції, здійснює й додаткові, закладені в неї розробником (наприклад, збирання і передача конфіденційної інформації)[2];

органів потрібно у своєму клопотанні обгрунтувати необхідність отримання саме таких документів, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих документів. У старій редакції КПК така інформація отримувалась за постановою слідчого про проведення виїмки.

[2] У травні 2005 р. за підозрою у вчиненні промислового шпигунства в Ізраїлі та Великобританії було заарештовано 18 осіб, які входили до складу керівництва декількох великих фірм Ізраїлю. Підозрювані використовували спеціальну програму «троянський кінь», яка пересилала дані із заражених комп'ютерів. Шпигунство здійснювалося за діяльністю компаній, що надавали послуги стільникового зв'язку, кабельного та ефірного телебачення,

– руткіти – набір програм, який дозволяє злочинцю внести певні зміни в програмне середовище комп'ютера-жертви для здійснення контролю та отримання у подальшому легкого доступу до нього.

За допомогою спеціальної техніки здійснюється прослуховування приміщень або зняття інформації з каналів зв'язку. Для цього застосовуються радіозакладки, мікрофони спрямованої дії, пристрої для зняття інформації з вікон за допомогою лазерних промінів[3], апаратура для виявлення та розшифровування електромагнітного випромінювання від офісної техніки, міні фото- та відеокамери. Таку техніку можуть встановлювати або використовувати як спеціально підготовлені особи, так і завербовані співробітники підприємства

Вчиненню вказаних незаконних дій нерідко сприяє недбале ставлення співробітників до своїх службових обов'язків, корумпованість, співучасть у злочині. Так, окрім сторонніх осіб ззовні можна виділити декілька груп осіб-співробітників, які займаються незаконним збиранням та використанням інформації, що становить комерційну таємницю:

1) працівники, які займаються збиранням інформації на замовлення, знаходячись із власником комерційної таємниці (уповноваженим органом) у трудових відносинах;

2) працівники, які займаються збиранням інформації для себе (про всяк випадок)[4].

Незаконному збиранню інформації через такі способи сприяють системні порушення співробітниками, зокрема:

займалися імпортуванням автомобілів [8].

[3] Існують спеціальні пристрої, які дозволяють за допомогою лазерного променя з відстані 500 м отримувати мовну інформацію через вібрацію віконного скла. У відповідь на такий спосіб компанія Сименс почала виробляти спеціальні віконні рами, які послаблюють проникнення електромагнітних променів на 110 дБ у певних діапазонах [7].

[4] Так, компанія Cyber-Ark зробила опитування IT-спеціалістів із різних європейських країн. Було встановлено, що 56 % респондентів (із 600 осіб) розглядають конфіденційну інформацію як свого роду страховку від можливого звільнення або як бонус при працевлаштуванні у майбутньому, і вже зробили копії баз даних. Найбільшу цінність представляють відомості щодо клієнтів, інформація про продукцію, що виготовляється, паролі доступу. Для зберігання інформації вони використовують flash-носії, CD чи DVD диски, онлайн сховища в мережі Internet [9].

1) правил організації технічного захисту території приміщень, що охороняється, мереж та систем, що забезпечують функціонування систем життєдіяльності;

2) порядку експлуатації систем обробки та передачі інформації;

3) порядку ведення службової інформації стосовно генерації електронних ключів та паролів доступу;

4) порядку оперативного контролю за функціонуванням системи захисту інформації;

5) порядку реєстрації та аналізу дій користувачів;

6) порядку обліку, зберігання та видачі користувачам носіїв конфіденційної інформації;

7) порядку допуску до приміщень, де здійснюється автоматична обробка даних [11, с. 105].

Таким чином, недоліки в організації роботи підприємств, установ та організацій є одними із основними чинників вчинення злочинних посягань на відомості, що становлять комерційну таємницю. Посилення контролю за діяльністю підлеглих з боку керівництва, більш ретельний відбір кадрів, удосконалення механізмів взаємодії між різними підрозділами, чітко визначені правила поведінки – все це певною мірою сприятиме зменшенню випадків вчинення цього виду злочинів.

Список літератури:

1. *Белкин Р. С.* Курс криминалистики / Р. С. Белкин. – [3-е изд., доп.]. – М. : ЮНИТИ-ДАНА ; Закон и право, 2001. – 837 с.

2. *Журавель В. А.* Криміналістичні методики: сучасні наукові концепції : монографія / В. А. Журавель. – Х. : Апостіль, 2012. – 304 с.

3. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та високих технологій / Л. П. Скалозуб [та ін.] ; за ред. О. М. Джужі. – К., 2009. – 192 с.

4. *Зуйков Г. Г.* Поиск преступников по признакам способов совершения преступлений : учеб. пособие / Г. Г. Зуйков. – М. : ВШ МВД СССР, 1970. – 191 с.

5. *Івченко О.* Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка [Електрон. ресурс]. – Режим доступу : (//www.justinian.com.ua/article.php?id=707).

6. *Колесниченко А. Н.* Криминалистическая характеристика преступлений : учеб. пособ. / А. Н. Колесниченко, В. Е. Коновалова. – Х. : Юрид. ин-т, 1985. – 92 с.

7. Коммерческий шпионаж [Електрон. ресурс]. – Режим доступу : http://www.seur.ru

8. Коммерческий шпионаж: самые известные скандалы последних лет [Електрон. ресурс]. – Режим доступу : http://www.rb.ru/inform/44717.html.

9. Половина ИТ-специалистов готовы на коммерческий шпионаж [Електрон. ресурс]. – Режим доступу : http://soft.mail.ru.

10. Розслідування злочинів у сфері господарської діяльності: окремі криміналістичні методики : монографія / В. Ю. Шепітько [та ін.] ; за ред. В. Ю. Шепітька. – Х. : Право, 2006. – 624 с.

11. *Сербин И. С.* Криминалистическое обеспечение защиты коммерческой тайны / И. С. Сербин. – М. : «Юрлитинформ», 2008. – 152 с.

12. *Шепітько В. Ю.* Вибрані твори // Избр. тр. / В. Ю. Шепітько. – Х. : Апостіль, 2010. – 574 с.

Курман А. В. **Обстановка совершения преступных посягательств на сведения, содержащих коммерческую тайну.**

Рассмотрены некоторые особенности обстановки преступлений, связанных из посягательствами на сведения, содержащие коммерческую тайну, определены факторы, способствующие совершению незаконных действий.

Ключевые слова: обстановка преступления, коммерческая тайна, незаконное собирание сведений, незаконное использование сведений.

Kurman A. V. **The situation of perpetration of a criminal encroachments on the information containing trade secrets.**

There were considered some special features of crime situations connected with an encroachment on the information containing trade secrets; the factors that contribute to the perpetration of the illegal acts were determined.

Key words: crime situation, trade secret, illegal collection of information, illegal use of information.