УДК 347.7+334.722

Е. І. НИЗЕНКО

Міжрегіональна Академія управління персоналом, м. Київ

ДЕЯКІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Наукові праці МАУП, 2009, вип. 3(22), с. 208–212

Розглянуто деякі питання, що стосуються захисту інформації у сфері підприємницької діяльності з урахуванням реалій, що склалися в Україні, та появи нових організаційно-правових форм захисту інформаційного ресурсу підприємства. Аналізуються правові норми чинного законодавства у зазначеній сфері, питання і проблеми, пов'язані з практикою організації підприємцем захисту інформації, що обробляється в автоматизованій системі. Визначено структурні елементи системи захисту інформації підприємства. Висвітлено методи технічного захисту інформації, що обробляється в електронному вигляді в автоматизованих інформаційних системах.

Проблема забезпечення захисту прав і законних інтересів суб'єктів підприємницької діяльності нині набула особливої значущості.

У державі в законодавчому порядку прийнятий комплекс заходів, що регулюють відносини у сфері підприємницької діяльності. Проблема забезпечення безпеки підприємництва в Україні висуває на перший план питання ефективності захисту інформаційних ресурсів організацій та установ [2].

Загальні засади державного регулювання підприємницької діяльності законодавчо закріплені у ст. 42 Конституції України. На конституційному рівні вперше закріплено право на підприємницьку діяльність, яка не заборонена законом.

Перед тим, як перейти до розгляду питання про захист інформації у сфері підприємницької діяльності, варто з'ясувати, у чому взагалі полягає суть проведення цілеспрямованих таємних активних операцій, спрямованих на отримання інформації, що захищається.

Забезпечення успіху в роботі із захисту відомостей, що становлять комерційну або банківську таємницю, залежить від глибокого і всебічного знання сучасних можливостей її таємного отримання.

Для дій з незаконного збирання пошукачами важливої інформації про конкурентів характерно використання негласних методів і технологій [1].

Саме про процес пошуку й отримання конфіденційної інформації суб'єкта господарювання і банківської таємниці з використанням заборонених методів, а також про створення підприємствами різних організаційно-правових форм, відповідної системи правового, організаційно-технічного захисту комерційної таємниці і режиму доступу до неї йдеться у нашій статті.

Злочинне збирання комерційної таємниці може здійснюватися із застосуванням наступних дій: підкупу, оплатного придбання корисної конфіденційної інформації, її перехоплення за допомогою приладів електронної апаратури;визначення обсягів послуг, виробництва товарів, виробничих потужностей; розпитування осіб, які мають доступ до таємниці, та підслуховування розмов про такі відомості; викрадання документів; фіксування відомостей, що становлять комерційну таємницю підприємства, використовуючи для цього приховану фото- та відеозйомку; прослуховування телефонів та ін.

Для глибшого осмислення методів негласного отримання інформації варто розглянути деякі серед них.

Аналіз практики застосування розвідувальних методів свідчить про те, що успішне їх використання багато в чому залежить від правильного вибору в кожному конкретному випадку адекватних пристроїв, електронної апаратури, а також

форми поведінки пошукачів важливої інформації про конкурентів.

Відомо, що застосування розвідувальних систем виявлення витоку інформації через канали паразитного випромінення дає можливість установити наявність маскуючого випромінювання в ефірі, що свідчить про те, що в приміщенні встановлені засоби радіопротидії, а тому унеможливлюється застосування закладних пристроїв для підслуховування.

Проте виявлення за допомогою радіоелектронних засобів розвідки спеціального генератора перешкод дозволяє дійти висновку про наявність у даній установі секретів, що приховуються на професійному рівні [6, *19*].

Характеризуючи даний аспект, не можна не вказати на фізичні принципи роботи закладних прослуховуючих пристроїв. Серед наявних нині засобів технічної розвідки розглянемо стетоскоп, який працює на основі принципу вібрування. Зазначимо, що кожному способу обміну інформації притаманне своє середовище. Доречно сказати, що стетоскоп використовують для прослуховування крізь товсті стіни.

Максимальна товщина перегородки з цегли, бетону, сталі може досягати — 50 см. Річ у тім, що одним з досить поширених каналів витоку інформації є акустичний, який утворюється за рахунок впливу на елементи і конструкції будівель, що викликає їх вібрацію. Механічні коливання стін (перекриттів, стелі, підлоги, вікон, коробів вентиляційних систем, труб систем опалення, водопостачання, кондиціювання та ін.), що виникають в одному місці, передаються на значні відстані. Звук, що поширюється у жорстких середовищах, називають структурним.

Вплив звукового тиску на перешкоди, які виникають на шляху звукових хвиль, викликає їх вібрацію в рамках смуги звукових частот (у межах від 100 до 6000 Гц). Під впливом акустичних полів електронна схема стетоскопа перетворює смугу звукових частот на струм звукової частоти. Далі електричні сигнали, промодульовані голосовою інформацією (акустичним полем), надходять з датчика на пристрій передання інформації, який складається з підсилювача і блока обробки сигналів.

До арсеналу заборонених законом протиправних методів злочинного збирання комерційної таємниці належать дії, що здійснюються з метою таємного отримання інформації у процесі спілкування з людьми, які є джерелом комерційних секретів [4, *12*].

Теоретичне поняття "спілкування" — це специфічний вид людської діяльності, об'єктивне явище комунікативної культури, засіб інформаційного обміну. Проблема спілкування із самого початку її виникнення користувалася посиленою увагою психологів, фахівців з розвідки.

За шпигунською термінологією технологія таємного отримання інформації має назву "витягування інформації" за допомогою прийомів соціотехніки [3, *6*].

Застосування технології таємного отримання інформації у процесі спілкування з людьми, які володіють важливими комерційними відомостями, передбачає маскування мети розмови.

Процес спілкування з особами, які мають доступ до таємниці, будується на попередньому встановленні і застосуванні надалі окремих характеристик співрозмовника, у тому числі звичайних схильностей, рівня інтелекту, способу мислення, нездатності повністю і в усіх деталях контролювати свою поведінку та висловлювання під час бесіди, марнославства, хвалькуватості, балакучості та ін. [9, *313*].

Застосування у сфері промислового (комерційного) шпигунства сучасної апаратури для добування протиправними способами засекреченої інформації конкурента (комерційної таємниці), а також здійснення інших незаконних дій стосовно збору інформації негативно впливає на бізнес [8].

Один із шляхів протистояння загрозам інформації — це впровадження організаційно-технічних заходів захисту інформаційної системи підприємств, організацій та установ [7].

Отже, визнання в Україні прав приватної власності, відмова держави від монополії у сфері управління економікою і проголошення свободи підприємницької діяльності спричинили появу великої кількості суб'єктів підприємництва. Підприємці одержали право здійснювати у встановленому законом порядку будь-які види діяльності.

У сучасних умовах господарювання перед підприємцями та іншими учасниками господарської діяльності постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, які можуть бути віднесені до комерційної таємниці підприємства [5].

Комерційна таємниця є одним з найдавніших способів охорони результатів інтелектуальної діяльності.

Цивільний кодекс України у статтях 505–508 визначає перелік майнових прав, пов'язаних з правом інтелектуальної власності щодо комерційної

таємниці, але в ньому, а також у Господарському кодексі України не встановлено правового режиму комерційної таємниці.

Тому за відсутності чітко встановлених правових засад одержання, використання, поширення та зберігання інформації, яка становить комерційну таємницю, а також гарантій захисту такої інформації реалізація норм, що містять санкції за правопорушення в цій сфері, в деяких випадках може призвести до порушень прав особи.

Таким чином, правове регулювання відносин щодо захисту комерційної таємниці є прерогативою спеціального законодавчого акта, якого на сьогодні не існує.

Комерційна таємниця віднесена Цивільним кодексом України (ст. 420) до об'єктів права інтелектуальної власності. До сукупності правомочностей володаря прав на комерційну таємницю входить і право захищати свої права.

Реалізація прав інтелектуальної власності на комерційну таємницю забезпечується виключним правом власника перешкоджати неправомірному її використанню.

Статут підприємства — це основний документ, в якому обов'язково повинно бути зафіксовано положення про те, що підприємство має право на організацію захисту комерційної таємниці. Зафіксовані у Статуті положення надають підприємству можливість створювати структурні підрозділи для захисту своєї комерційної таємниці, а також видавати внутрішні нормативні документи, що стосуються питань охорони комерційної таємниці.

У сфері підприємницької діяльності сьогодні умовно виокремлюють два види охорони інформації, тобто два види інформаційної безпеки: пасивну й активну. При цьому пасивна охорона характеризується тим, що власник інформації надає їй режим відкритості, доступності для всіх зацікавлених осіб.

На практиці організації системи забезпечення безпеки підприємства активна охорона інформації здійснюється для захисту комерційної таємниці від несанкціонованого власником використання.

На відміну від інших видів діяльності тут об'єктом захисту стає інформаційний ресурс, тобто інформація на матеріальних носіях — документи бази даних, технічна документація та ін. Автоматизовані засоби обробки інформації та комп'ютерні мережі передання інформації, інформаційні ресурси підприємства забезпечують спеціалісти-експлуатаційники. Інформаційна інфраструктура не включає безпосередньо інформаційні ресурси, оскільки вони є предметом, що обробляється за допомогою цієї інфраструктури. Призначення компонентів інформаційної інфраструктури (технічні засоби автоматизованої системи і технології, програмне забезпечення, комп'ютерні мережі передання інформації, спеціалісти-експлуатаційники) полягає в тому, що вони є тим, за допомогою чого реалізуються інформаційні процеси. Головна функція інформаційної інфраструктури полягає в реалізації інформаційних процесів. Тому інформаційна інфраструктура повинна забезпечувати збереження державної таємниці, конфіденційності документованої інформації, попередження інших незаконних дій, спрямованих на вторгнення в інформаційні системи.

Основу регулювання правових відносин щодо захисту інформації в автоматизованих інформаційних системах становить Закон України "Про захист інформації в автоматизованих системах" від 5 липня 1994 р. № 80/94-ВР. Дія цього закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах (АС).

Дозвіл на введення АС в експлуатацію надає Держстандарт технічної системи захисту інформації Служби безпеки України за умов, коли придбані підприємцем засоби із захисту інформації в автоматизованій інформаційній системі підприємства відповідають вимогам нормативних документів із технічного захисту інформації.

Таке право затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23 лютого 2002 р. № 9.

Найважливішими структурними елементами системи захисту інформації можна вважати такі засоби захисту:

- фізичні;
- адміністративні;
- апаратні;
- програмні;
- криптографічні;
- атестація системи комп'ютерної безпеки.

Програмні засоби — це системні програми, що входять до складу програмного забезпечення системи обробки інформації для попередження несанкціонованого передавання даних через локальну мережу чи Інтернет, викликаної TEMPEST-атакою, а також протидії перехопленню композиційного сигналу монітора.

TEMPEST-атака здійснюється шляхом "зараження" потрібного комп'ютера спеціальною програмою-закладкою "троянський кінь" чи з використанням технологій побудови комп'ютерних вірусів.

Метод технічного захисту інформації входить до складу програми TEMPEST-захисту і застосовується для виконання функції запобігання відтоку таємної інформації шляхом перехоплення технічними засобами розвідки електромагнітних випромінювань комп'ютера. З цією метою також застосовують пасивний метод попередження відтоку даних, що обробляються в електронному вигляді, через технічні канали.

Пасивний метод — це сполучення екранування корпусу та окремих елементів комп'ютера із застосуванням високочастотних фільтрів, щоб досягти великого затухання в широкому діапазоні частот.

Попередження можливості перехоплення електромагнітних випромінювань в інформаційних системах, базовим елементом яких є комп'ютер, відбувається переважно за допомогою спеціальних широкосмугових джерел шуму, що робить неможливим застосування закладених для підслуховування пристроїв. Інший варіант захисту інформації — екранування джерела випромінювання з комп'ютера для зменшення рівня випромінювання робочої станції.

При цьому можна ще говорити про реалізацію такого технічного рішення, яке базується на використанні криптографічних пристроїв, що часто застосовують для шифрування інформації в банківських комп'ютерних мережах передання даних. Шифрування інформацції — це процес перетворення її в недоступну для стороннього форму криптографічним методом. Перевага криптографічних методів полягає в тому, що навіть після компроментації засобів керування доступом (паролів, прав доступу до мережі та ін.) до інформації остання залишається для зловмисника недосяжною (тобто не читається).

В організації захисту комерційної таємниці підприємства є така особливість: розв'язання певного завдання або його частини доручається конкретному підрозділу чи спеціалісту.

Як правило, вирішення проблеми протидії витоку інформації, що обробляється в АС, покладається на підрозділ захисту інформації служби безпеки підприємства. Координація дій з планування та реалізації внутрішніх і зовнішніх заходів захисту інформації в автоматизованій інформаційній системі підприємства покладається на керівника підрозділу захисту інформації [5, *83*].

На керівників груп закритого діловодства та підрозділу захисту інформації покладаються такі обов'язки:

- організація закритого діловодства;
- вживання заходів щодо запобігання розголошенню комерційної таємниці;
- контроль за своєчасним, правильним визначенням та зміною грифа обмеження з встановленої на підприємстві багатоступеневої системи важливості відомостей, що мають комерційну таємницю;
- організація робіт зі створення і використання комплексної системи захисту інформації;
- фіксація випадків розголошення відомостей, що мають комерційну таємницю;
- жорстке попередження протиправних дій, спрямованих на вторгнення в інформаційні ресурси.

У структуру підрозділу, який має забезпечувати інформаційну безпеку підприємства, можуть входити:

- керівник підрозділу захисту інформації в автоматизованій системі (заступник начальника служби безпеки підприємства);
- юрист;
- фахівці в галузі конкурентної розвідки, промислової контррозвідки;
- фахівці, які вміють застосовувати спеціальну охоронну техніку для захисту приміщень;
- системний адміністратор;
- системний програміст;
- криптограф;
- аудитор;
- спеціаліст експлуатаційних комп'ютерних систем;
- головний спеціаліст із захисту комерційної таємниці.

Зазначимо, що ефективне розв'язання проблеми захисту інформації в умовах підприємницької діяльності вимагає поєднання організаційно-правових заходів із найсучаснішими технічними засобами захисту інформації.

Література

1. *Іваницька Н.* Промислове шпигунство та правові інструменти захисту від нього // Бизнес и безопасность. — 2006. — № 1 — С. 2–4.

2. *Курбет П., Безштанько В., Цуркан В.* Політика інформаційної безпеки як необхідний елемент успішного функціонування організації // Бизнес и безопасность. — 2006. — № 1. — С. 84–85.

3. *Нелін О. І., Низенко Е. І., Панфілов В. М.* Роль недержавних служб безпеки в захисті економічних інтересів підприємництва. — К.: Поліграф-Сервіс, 2001. — 32 с.

4. *Низенко Э. И.* Обеспечение безопасности предпринимательской деятельности: Учеб. пособие. — К.: МАУП, 2003. — 124 с.

5. *Низенко Е. І.* Організаційно-правове забезпечення, формування та реалізація державної політики в сфері безпеки підприємництва // Приватне право і підприємництво: Зб. наук. пр. — Вип. 3. — К.: Наук.-дослід. ін-т приватного права і підприємництва Академії правових наук України, 2003. — С. 79–84.

6. *Низенко Е. І., Каленяк В. П.* Забезпечення інформаційної безпеки підприємства: Навч. посіб. — К.: МАУП, 2006. — 134 с.

7. *Низенко Е. І.* Загальнотеоретичні характеристики окремих напрямів захисту конфіденційної інформації від злочинних посягань // Наукові праці МАУП. — 2007. — Вип. 1 (15). — С. 127–132.

8. *Низенко Е. І.* Система недержавної безпеки підприємництва як невід'ємна складова національної безпеки України // Становлення і розвиток української державності: Матеріали Всеукр. наук.-практ. конф., Київ, МАУП, 27 жовт. 2006 р. — К.: ДП "Вид. дім "Персонал", 2008. — С. 286–289.

9. *Низенко Е. І.* Організаційно-методичні особливості підготовки в юридичних навчальних закладах фахівців з безпеки підприємництва // Наукові праці МАУП. — 2008. — Вип. 2 (18). — С. 312–317.

Захист інформації є одним з найважливіших напрямів у системі забезпечення безпеки діяльності організацій та установ. Теоретичні підходи до з'ясування сутності інформаційної безпеки підприємства доцільно реалізовувати з позиції системного аналізу напрямів комплексного вирішення проблеми забезпечення інформаційної безпеки у сфері підприємницької діяльності. Запропонована структура підрозділу, який має забезпечити інформаційну безпеку підприємства. Це дає змогу характеризувати процес створення служби безпеки організацій та установ в цілому з метою комплексного захисту підприємницької діяльності від реальних або потенційних загроз, які можуть призвести до суттєвих економічних втрат.

Защита информации является одним из важнейших направлений в системе обеспечения безопасности предпринимательской деятельности организаций и учреждений. Теоретические подходы к выяснению сущности информационной безопасности предприятия целесообразно реализовывать с позиции системного анализа направлений, комплексного решения проблемы обеспечения информационной безопасности в сфере предпринимательской деятельности. Предложена структура подразделения, которое должно обеспечить информационную безопасность предприятия. Это дает возможность характеризировать процесс создания службы безопасности организаций и учреждений в общем с целью комплексной защиты предпринимательской деятельности от реальных или потенциальных угроз, которые могут привести к серьезным экономическим потерям.

The defense information is of the most important in securing safety of system organizations. Theoretical methods of approach to ascertainment essence information`s of safety enterprise, exepediency implement on position of system analysis, the directions of complex decision of problem of enterprise` informative safety inbusiness activity sphere. The offer scheme of organization subdivision which intend securing information, safety enterprise an opportunity description process, make the service of safety organizations for objective complex defense the business activity, from feasibility or potential menaces, which it possible cause to economic substantially bereavement.

Надійшла 8 червня 2009 р.