УДК 346.21:004

ДО ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Черненко О. А.,
кандидат юридичних наук, старший науковий співробітник Науково-дослідного інституту приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України
(Київ)

У статті розглядаються проблемні питання пов'язані з інформаційною безпекою суб'єктів господарювання.

Ключові слова: безпека, інформація, конкуренція, комерційна таємниця.

В умовах розвитку ринкової економіки інформація стає найціннішим товаром, оскільки саме володіння інформацією, її використання забезпечує ефективне функціонування суб'єктів господарювання. Тому, головним завданням для суб'єктів господарювання є захист конфіденційної інформації, що дозволяє забезпечити економічну безпеку, уникнути банкрутства, захистити себе від недобросовісної конкуренції та комерційного шпигунства.

Проблема забезпечення інформаційної безпеки є на сьогодні актуальною як для України, так і для розвинених країнах світу. В Україні питання захисту інформації регулюються ЦК України, ГК України, Законами України «Про інформацію», «Про доступ до публічної інформації», «Про захист від недобросовісної конкуренції» та іншими нормативними актами.

Окремі питання пов'язані із проблемами забезпечення інформаційної безпеки розглядались у працях таких вчених як О. Качан, О. Литвиненко, О. Сороківська, В. Цимбалюк тощо.

В науковій літературі існують різні погляди на зміст поняття «інформаційна безпека». Інформаційну безпеку характеризують як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [1; с. 30]. Визначають інформаційну безпеку і як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [2; с. 35]. Під інформаційної безпекою розуміється єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [3; с. 9]. Крім того, визначають інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [4].

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Відповідно до Закону України «Про доступ до публічної інформації» інформація з обмеженим доступом поділяється на:

1) конфіденційну інформацію;

2) таємну інформацію;

3) службову інформацію.

Стаття 21 Закону України «Про інформацію» передбачає, що конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

При веденні своєї діяльності суб'єкт господарювання обов'язково наштовхується на необхідність отримання, обробки, зберігання, перетворення, передачі інформації. Цінність інформації визначається через ряд параметрів, до яких належать корисність, достовірність, своєчасність тощо [5].

Найбільш поширеними загрозами інформаційній безпеці суб'єктів господарювання є: розголошення таємної та конфіденційної інформації, її викрадення, модифікація чи знищення, незаконне використання інформації, особливо тієї її частини, що становить інтелектуальну власність суб'єктів господарювання і обумовлює переваги на ринку, несанкціонований доступ до інформації, що охороняється суб'єктом.

Отже, під час конкурентної боротьби постійно існує загроза неправомірних посягань на інформацію конкуруючих суб'єктів:

•маніпулювання інформацією (дезінформація, викривлення інформації, надання неповної або неправдивої інформації);

•несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів;

• протиправне збирання і використання інформації;

•руйнування та використання з протиправною метою чужих інформаційних ресурсів;

•інформаційний тероризм (поширення комп'ютерних «вірусів», установлення програмних та апаратних закладних пристроїв, упровадження радіоелектронних приладів перехвату інформації).

Необхідно наголосити, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки будь-якого суб'єкта господарювання є збереження в таємниці комерційної важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

За загальним правилом, до комерційної таємниці відноситься така інформація: рівень прибутку і цінова політика; фінансові та адміністративні плани розвитку компанії (бізнес–плани); відомості про укладені або заплановані контракти; дані про контрагентів, власні винаходи та раціоналізаторські пропозиції, які ще не захищені авторським або патентним правом; власні аналітичні огляди ринку, маркетингові дослідження [6].

В літературі зустрічається думка, що комерційну таємницю суб'єктів господарювання мають становити і такі відомості, як: перспективні методи керівництва виробництвом; організаційна структура підприємства; організація праці на підприємстві; відомості про виробничі можливості підприємства; характеристика виробництва в цілому і його структурних одиниць: дані про резерви сировини на підприємстві, відомості про фонди окремих матеріалів, у тому числі тих, що випускаються для власних потреб; плани розвитку підприємства та по розширенню виробництва; інвестиційні програми, техніко-економічні обґрунтування і плани інвестицій; планово-аналітичні матеріали за поточний період; обсяг майбутніх закупівель по термінах, асортименту, цінах, країнах, фірмах; відомості, що розкривають планові та фактичні показники фінансового плану; майновий стан; вартість

основних засобів і запасів матеріалів та сировини; банківські операції; відомості про фінансові операції; об'єми виручки; рівень доходів; боргові зобов'язання; відомості про представників, посередників, дилерів і партнерів; відомості про постачальників, покупців і споживачів, оптових і роздрібних; комерційні зв'язки; місця закупівлі сировини та матеріалів; відомості про іноземних комерційних партнерів; відомості і характеристика підприємств – торгових партнерів (основні виробничі фонди, кредити, товарообіг); відомості про клієнтів у торгівлі й рекламі [7]. Також складовою комерційної таємниці суб'єктів господарювання можуть бути і умови договорів (контрактів): терміни, обсяги, умови постачання, знижки, доплати, розстрочки платежів тощо [8].

Загрози інформаційної безпеки поділяються на внутрішні та зовнішні. Зовнішні зловмисні дії можуть бути такими: копіюванні цінних документів, або викрадення файлів; викрадення флеш-карт; викрадення інформації у процесі її передавання по мережі Інтернет; пошкодження носіїв з інформацією; донесення інформації до підприємств-конкурентів, або взагалі до іншої країни; викрадення інформації за допомогою інсайдерів. До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження інформації вірусами, або пошкодження файлів працівниками підприємства [5].

Організовуючи інформаційну безпеку суб'єкту господарювання слід мати на увазі, що переважна частина загроз формується саме через його працівників. Факторами, які можуть вплинути на розголошення інформації можуть бути недоліки професійної підготовки працівників, особливо щодо роботи з документами та інформацією обмеженого доступу, а також такі якості, як безвідповідальність, недисциплінованість, незадоволення рівнем заробітної плати, недобрі відносини між працівником та керівництвом тощо. Психологи стверджують, що біля 25 % всіх співробітників підприємств розголошують інформацію, продають або передають її конкуруючим підприємствам задля додаткового заробітку. Захист інформації на підприємстві є дуже важливою річчю і цей аспект повинен бути обов'язково врахований при укладанні контракту з працівником. Саме тому, контракт, що підписується співробітником, при працевлаштуванні повинен неодмінно містити пункт про нерозголошення комерційної таємниці [5].

Одним з видів противоправних посягань на безпеку підприємства є комп'ютерні злочини. Безпосереднім об'єктом комп'ютерних злочинів є як інформація, так і самі комп'ютерні програми. Посягання на інформацію, що охороняється, можуть бути різними: крадіжка носія інформації, порушення засобів захисту інформації, використання чужого імені, зміна коду або адреси технічного пристрою, надання фіктивних документів на право доступу до інформації, встановлення апаратури, що веде несанкціонований запис тощо. Наслідки протиправних посягань на конфіденційну інформацію підприємства можуть привести до зміни змісту інформації, блокуванню інформації, знищенню інформації без можливості її відновлення, порушення роботи комп'ютерів та комп'ютерних мереж[9]. Велику небезпеку представляють комп'ютерні віруси. Зрозуміло, що позбавитися комп'ютерного вірусу значно складніше ніж забезпечити дійсні міри по його профілактиці.

Механізм захисту конфіденційної інформації передбачає як організаційні, так і технічні засоби. Організаційні засоби захисту спрямовані на обмеження можливого несанкціонованого фізичного доступу до документів, які містять конфіденційну інформацію, у тому числі до комп'ютерних мереж. Технічні засоби передбачають використання засобів програмно-технічного характеру,

перш за все, на обмеження доступу співробітників компанії, особливо тих, що працюють з комп'ютерними системами, до інформації, звертатися до якої вони не мають права [10, с. 128-134].

Враховуючи вищенаведене, можна зробити висновок, що суб'єкт господарювання має використовувати всі можливі заходи щодо захисту інформації, в тому числі ідентифікація користувачів, встановлення паролів, шифрування інформації, міжмережні екрани, віртуальні приватні мережі та контроль за включенням живлення і завантаження програмного забезпечення. Забезпечення інформаційної безпеки на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки буде невід'ємним елементом процесу управління суб'єктом господарювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. *Цимбалюк В. С.* Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2004. № 8. С. 30–33.
2. *Гуцу С. Ф.* Правові основи інформаційної діяльності: навчальний посібник. Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. 48 с.
3. *Литвиненко О. В.* Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. К., 1997. 18 с.
4. *Сороківська О. А.* Інформаційна безпека підприємства: нові загрози та перспективи. Режим доступу: http:///nbuv.gov.ua/portal/Soc_Gum/Vchnu_/032-035.pdf. (дата звернення 20.09.2017).
5. *Качан О. І.* Інформаційна безпека підприємства в умовах глобалізації. Режим доступу: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf. (дата звернення 12.09.2017).
6. *Захист* комерційної таємниці в трудових відносинах // http://www.krapka.org.ua (дата звернення: 28.10.2016).
7. *Яфонкін А. О., Климко В. С.* Окремі проблеми комерційної таємниці суб'єктів господарювання у договірних відносинах в Україні. Режим доступу: https://C:/Users/%D0%9B%D0%B5%D0%BD%D0%B0/Downloads/11147-28932-1-SM%20(2).pdf. (дата звернення: 18.07.2017).
8. *Про комерційну* таємницю: наказ № 35. – Київ, 2011 [Електронний ресурс]: URL: http://pravnik.at.ua/news/2011-01-15-214 (дата звернення: 28.10.2016).
9. *Перевалова Л. В.* Захист конфіденційної інформації:проблеми та шляхи вирішення. Режим доступу: http://www.kpi.kharkov.ua/archive/% pravo5.pdf (дата звернення: 03.09.2017).
10. *Курушин В. Д., Минаев В. А.* Компьютерные преступления и информационная безопасность. Справочник. М.: Новый Юрист, 1998. 256 с.

THE QUESTION OF INFORMATIONAL SECURITY OF BUSINESS ENTITIES

Chernenko O. A., Candidate of Legal Sciences, Senior Researcher of the department of legal support of a market economy of the Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of NALS of Ukraine (Kyiv)

Keywords: safety, information, competition, trade secrets.

Information is the most valuable product, since the very possession of it, its usage ensures the effective functioning of the entity. The most common threats to the business entities' information security are: disclosure of secret and confidential information, its abduction, destruction and illegal usage. There are two types of security threats for information: internal and external. External malicious actions include copying valuable documents (also called as hijacking files) and reporting information to rival companies, while the most common internal threats are theft, virus infections, or corrupted files by company employees.

Computer crime is one of the most dangerous invasions on enterprise security. The direct object of this type of invasion can be both information and computer programs themselves. Computer viruses represent a great danger.

Provision of information security at the appropriate level is possible only when the information component of economic security is an integral part of the management process of the entity.