УДК 65.012.8

Л.В. ПЕРЕВАЛОВА, канд. філос. наук, проф., НТУ «ХПІ», Харків
С.В. КВАША, студент, НТУ «ХПІ», Харків

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ

У статті аналізуються поняття конфіденційної інформації, комп'ютерної безпеки. Розглядаються проблеми, пов'язані із захистом прав суб'єктів господарювання на конфіденційну інформацію, пропонуються шляхи вдосконалення механізму захисту конфіденційної інформації від неправомірних посягань.

В статье анализируются понятия конфиденциальной информации, компьютерной безопасности. Рассматриваются проблемы связанные с защитой прав субъектов хозяйствования на конфиденциальную информацию, предлагаются пути усовершенствования механизма защиты конфиденциальной информации от неправомерных посягательств.

The concepts of confidential information are analysed in the article, to computer safety. Problems are examined related to securing of rights for management subjects for confidential information, the ways of improvement of mechanism of defence of confidential information are offered from illegal encroachments.

На сучасному етапі розвитку економіки і суспільства в цілому інформація, як об'єкт інтелектуальної власності компанії, стає все більш значущим інструментом на її шляху до комерційного успіху. Науково-технічні розробки, економічні та організаційні рішення, які невідомі третім особам, можуть надавати компанії конкурентні переваги і служити основним або додатковим джерелом прибутку. Останнім часом все частіше власники такої інформації почали усвідомлювати необхідність її захисту. У системі забезпечення безпеки підприємницької діяльності все більшого значення набуває комп'ютерна безпека. Це пов'язано із зростаючим об'ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі і обробки. Перевід значної частини інформації в електронну форму, використовування локальних та глобальних мереж створює якісно нові загрози конфіденційної інформації.

Проблема забезпечення інформаційної безпеки є на сьогодні однією з найгостріших не лише в Україні, але і в розвинених країнах світу. Досвід експлуатації інформаційних систем і ресурсів в різних сферах життєдіяльності показує, що існують різні і вельми реальні погрози втрати інформації, що приводять до матеріальних і інших збитків. При цьому забезпечити на 100 % безпеку інформації практично неможливо.

Ще у 1981 р. Рада Європи схвалила Конвенцію про захист даних. У Великобританії аналогічний закон був ухвалений у 1984 р. Питання інформаційної безпеки Російської Федерації обговорюються в «Концепції національної безпеки Російської Федерації», що прийнята відповідно до Указу Президента РФ від 17.12.1997 р. Аналогічні законодавчі акти були

прийняті у США, Німеччині та інших країнах світу. Вказані закони встановлюють норми, регулюючі стосунки в області формування і використання інформаційних ресурсів, створення і вживання інформаційних систем, інформаційних технологій і засобів їх забезпечення, захисту інформації і захисту прав громадян в умовах інформатизації суспільства.

В Україні питання захисту інформації регулюються Цивільним, Господарським кодексами України, Законами «Про інформацію», «Про захист від недобросовісної конкуренції» та іншими нормативними актами.

Закон України «Про інформацію» ввів поняття « інформація із обмеженим доступом». Ця інформація відповідно до закону поділяється на конфіденційну та таємну [1].

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб та розповсюджуються за їх бажанням відповідно з передбаченими ними умовами (ч. 2 ст. 30 Закону України «Про інформацію»).

До таємної інформації закон відносить інформацію, котра містить відомості, що складають державну або іншу передбачену законом таємницю, розголошення якої заподіює збиток особі, суспільству і державі. І хоча в нормах закону чітко не вказано, що до таємної інформації належить комерційна таємниця, на нашу думку, в поняття «Інша передбачена законом таємниця» законодавець вклав саме цей сенс.

Цивільний кодекс України не дає визначення конфіденційній інформації, але стаття 505 визначає, що комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [2].

Згідно ч. 1 ст. 36 Господарського кодексу України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою і іншою діяльністю суб'єкта господарювання, які не є державною таємницею, розголошування яких може заподіяти збиток інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад та об'єм відомостей, які складають комерційну таємницю, засоби її захисту визначаються суб'єктом господарювання відповідно до закону [3].

Вищий господарський суд України у своєму листі «Про деякі питання практики застосування господарськими судами законодавства про інформацію» (інформаційний лист ВГСУ від 28.03.2007 р. № 01-8/184) відніс до кола конфіденційної інформації комерційну таємницю, «ноу-хау» та іншу інформацію, що визначається законом. На думку суду особи, які володіють

конфіденційною інформацією, повинні самостійно визначати режим доступу до неї, включаючи її належність до категорії конфіденційній, та встановлювати для неї систему захисту.

Таким чином поряд з терміном «конфіденційна інформація» законодавство широко використовує такий термін як «комерційна таємниця». Тому важливим є не те, яку назву має інформація, що охороняється законом від несанкціонованого доступу третіх осіб, а те, яким вимогам вона повинна відповідати. В зв'язку з цим при передачі за договором технологічних знань і досвіду роботи необхідно включати умову про «конфіденційність» [4, с. 680].

В умовах розвитку ринкової економіки інформація стає найціннішим товаром, тому головним завданням для суб'єктів господарської діяльності є захист конфіденційної інформації, що дозволяє забезпечити компанії економічну безпеку, уникнути банкрутства, захистити себе від недобросовісної конкуренції та комерційного шпигунства, попередити рейдерські атаки. Ось чому так важливо сьогодні визначити, яка ж інформація є конфіденційною, і як саме можна захистити дану інформацію. Саме внаслідок витоку комерційної інформації національні компанії дуже часто страждають від зниження можливості продажу ліцензій на власні наукові розробки, від втрати пріоритету в освоєних областях науково-технічного прогресу, від зростання витрат на переорієнтацію діяльності дослідницьких підрозділів, від зростання витрат підприємства на створення нової ринкової стратегії і багатьох інших.

Одним з видів противоправних посягань на економічну 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 по зрівнянню з тою, що була раніше, блокуванню інформації, знищенню інформації без можливості її відновлення, порушення роботи комп'ютерів та комп'ютерних мереж.

Зарубіжні фахівці розробили різні класифікації засобів здійснення комп'ютерних злочинів. Так, кодифікатор Генерального Секретаріату Інтерполу містить спеціальні коди, які характеризують комп'ютерні злочини, вони мають ідентифікатор, що починається з букви Q. Для характеристики злочину може використовуватися до п'яти кодів, які розташовуються у порядку зменшення значущості злочину. Так, несанкціонований доступ та перехват інформації (QA) містить в себе такі види комп'ютерних злочинів:

– «комп'ютерний абордаж» – доступ до комп'ютеру або до мережі без права на це. Цей вид злочину використовується для проникнення в чужі

інформаційні мережі;

– перехват – перехват інформації за допомогою технічних засобів, без права на це. Він здійснюється або шляхом підключення до зовнішніх комунікаційних каналів, або шляхом підключення до периферійних пристроїв.

Ще одним видом комп'ютерних злочинів є внесення змін до комп'ютерних даних (QDL/QDT):

– логічна бомба – полягає в таємному вбудовуванні в програму набору команд, який повинен спрацювати лише одного дня, але за певних умов.

– троянський кінь – це таємне введення в чужу програму таких команд, які дозволяють здійснювати інші функції, що не планувалися власником програми, але одночасно зберігати і колишню працездатність.

Велику небезпеку представляють комп'ютерні віруси (QDV). Комп'ютерний вірус – це спеціальна програма, яка дозволяє приписати себе до інших програм, розмножується та роджає нові віруси для виконання різних небажаних дій на комп'ютері. Зрозуміло, що позбавитися комп'ютерного вірусу значно складніше ніж забезпечити дійсні міри по його профілактиці [5, с. 189-238].

Забезпечення безпеки підприємницької діяльності з боку комп'ютерних систем представляє один із блоків проблеми захисту конфіденційної інформації. Захист повинний починатися з розробки концепції інформаційної безпеки компанії. 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 [6, с. 128-134]. Фахівці пропонують такі напрямки технічного захисту: використання засобів контролю за включенням живлення і завантаження програмного забезпечення; встановлення паролів; шифрування та спеціальні протоколи зв'язку; додаткова перевірка апаратури; «цифрова підпис» та інші.

Як правило, власник інформації обмежується встановленням в посадових інструкціях, договорах застереження про конфіденційність і про відповідальність за порушення або підписанням окремих угод про нерозголошення конфіденційної інформації. Суб'єкт господарської діяльності повинний мати затверджений перелік конфіденційної інформації, положення про режим конфіденційності, з передбаченими детальними заходами щодо збереження конфіденційної інформації, адекватними існуючим обставинам (ст. 505 ЦКУ), з якими повинна бути ознайомлена особа, яка отримує конфіденційну інформацію. Якщо власник конфіденційної інформації не дотримується таких заходів або відсутній контроль з його боку за дотриманням таких заходів, всі застереження і

укладені угоди про нерозголошення не породжують у сторін прав і обов'язків у сфері дотримання режиму конфіденційності. Крім того, при розробці переліку конфіденційної інформації слід пам'ятати, що є ряд відомостей, які в силу закону не можуть бути віднесені до комерційної таємниці.

За порушення режиму конфіденційності законодавством встановлена цивільно-правова, адміністративна та кримінальна відповідальність. Цивільно-правова відповідальність передбачає зобов'язання відшкодувати власнику конфіденційної інформації заподіяний збиток і сплатити інші фінансові санкції, встановлені договором. Адміністративна відповідальність передбачена ст. 164-3 Кодексу України про адміністративні правопорушення (недобросовісна конкуренція), яка передбачає санкції у вигляді штрафу за поширення, використання, розголошення комерційної, конфіденційної інформації з метою спричинення збитків діловій репутації або майну підприємця. Окремо слід зупинитися на кримінальній відповідальності. Кримінальний кодекс України містить окремий розділ XVI – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – повністю присвячений класифікації та встановленню відповідальності за вчинення комп'ютерних злочинів. Так, наприклад, несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Заслуговує на увагу формулювання ст. 176 ККУ «Порушення авторського права і суміжних прав», в якій прямо згадуються комп'ютерні програми та бази даних, а одним із засобів незаконного тиражування визначено дискети та інші носії інформації (тобто, носії комп'ютерної інформації).

Однак, не можна не помітити, що на сьогоднішній день загальна частка звернень до суду щодо захисту конфіденційної інформації дуже мала. Підприємці, які у процесі свої діяльності неодноразово піддаються неправомірним діям інших суб'єктів, прагнуть не розголошувати випадки посягань на їх комп'ютерні системи. Це пов'язано з тим, що фірми, банки не бажають «лякати» своїх клієнтів, споживачів тим фактом, що їх комп'ютерні мережі, а значить і вся інформація, що міститься в них, недостатньо захищена.

Недосконаліть діючого законодавства, відсутність судової практики по спорах, пов'язаних із захистом конфіденційної інформації призвели до того, що на сьогоднішній день захистити від несанкціонованих порушень

корпоративні ідеї, ноу-хау законодавчим шляхом практично не можливо. Тому у справах збереження власної інформації компаніям слід покладатися тільки на себе. Компанія, яка бажає дійсно захистити свою інформацію повинна мати комплекс діючих мір, якій необхідно постійно вдосконалювати. Тільки таким чином вона може забезпечити надійний захист конфіденційної інформації.

Список літератури: 1. Закон України «Про інформацію» № 2657-ХП від 02.10.1992 р. // Відомості ВР України. – 1992. – № 48. – Ст. 650. **2.** Цивільний кодекс України // Офіційний вісник України. – 2003. – № 11. – Ст. 461. **3.** Господарський кодекс України // Офіційний вісник України. – 2003. – №11. – Ст. 462. **4.** *Сергеев А.П.* Право интеллектуальной собственности в Российской Федерации: учеб. 2-е изд., перераб. и доп. – М.: ТК Велби, Изд-во Проспект. – 752 с. **5.** Тагинцев А.Н. Информационные компьютерные преступления в современном обществе // Вестник Воронежского института МВД России. – Воронеж: Изд-во Воронеж. ин-та МВД России, 2002, № 2 (11). – С. 128-134.
6. *Курушин В.Д., Минаев В.А.* Компьютерные преступления и информационная безопасность. Справочник. – М.: Новый Юрист, 1998. – 256 с.

Надійшла до редколегії 05.05.2011.