УДК 004.056.5:061.5 (045)

А. Ю. Нашинець-Наумова,
кандидат юридичних наук

ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглядаються проблемні питання забезпечення інформаційної безпеки підприємства як суб'єкта інформаційного права та інформаційних правовідносин.

Ключові слова: інформація, інформаційна безпека підприємства, забезпечення безпеки, правопорушення у сфері обігу інформації на підприємстві, інформаційні системи, технічний захист інформаційних систем.

Значення інформації в житті людини сьогодні складно переоцінити. Діяльність щодо отримання та обробки інформації займає досить багато часу. Підсвідомо людина стикається з величезним числом джерел інформації і являється, відповідно, частиною глобального інформаційного обміну. В той же час, в умовах розвитку інформаційних технологій процес пошуку і обробки інформації істотно прискорюється, що робить доступними практично будь-які джерела інформації в умовах реального часу. В нашій країні, як і у всьому світі, відбувається поступове становлення інформаційного суспільства, економічною основою якого є створення та вдосконалення технічних і технологічних способів і засобів виробництва, отримання та поширення інформації на основі створення та використання інформаційно-комунікаційних технологій, які можуть розглядатися в якості найважливішої ознаки сучасної інформаційної епохи. Підвищення економічної складової інформаційно-комунікаційних технологій вимагає створення і відповідної правової основи їх виробництва та використання [1, с. 5].

Розуміючи важливість інформаційного розвитку української держави та входження до світового інформаційного простору, Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» було задекларовано, що розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя визначається одним із пріоритетних напрямів державної політики [2].

В цілому інформація пронизує усі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму [3, с. 11]. Важливо також підкреслити зв'язок процесів інформатизації суспільства з його історичним розвитком. Як відмічають фахівці в галузі інформаційних проблем, інформатизація життя сприяє зародженню і зміцненню основ прогресивного сучасного етапу громадського розвитку – громадянського суспільства. У літературі відбивається позиція, що визначає інформаційне суспільство «як новий історичний етап розвитку громадянського суспільства» [4, с. 2].

Аналіз структури економіки і виробництва дозволяє відмітити в умовах інформаційних процесів послідовне зростання значення і ролі юридичних осіб, що є суб'єктами малого і середнього підприємництва, яке за оцінками економістів вносить в усіх країнах помітний вклад в загальний обсяг громадського виробництва.

Саме з розвитком правового регулювання процесів інформаційного обміну набагато простіше встановлювати партнерські стосунки, шукати контрагентів, реалізовувати і закуповувати продукцію, стали доступніші нові «види бізнесу» – нові форми здійснення підприємницької діяльності. В цілому інформація настільки тісно пов'язана з бізнесом, що цей зв'язок виводить на перший план проблеми, значення яких складно переоцінити. До їх числа відноситься і проблема забезпечення інформаційної безпеки підприємства. Тема інформаційної безпеки є відносно добре розробленою в літературі. Необхідно відмітити роботи таких авторів як О. Баранова, К. Бєлякова, В. Брижка, В. Гавловського, І. Гаврилова, О. Гладківської, М. Гуцалюка М. Жулинського, Л. Задорожньої, О. Зінченка, Г. Лазарєва, А. Марущака, А. Новицького, Б. Раціборинського, В. Хахановського, В. Цимбалюка, М. Швеця та ін. Останнім часом підготовлений ряд дисертаційних досліджень, присвячених питан-

ням інформаційної безпеки, при цьому треба відмітити, що більшість робіт пов'язана з питанням інформаційної безпеки держави, або з забезпечення безпеки інформаційних систем. Проте, проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано, зокрема, з тим, що автори більшу увагу приділяють забезпеченню інформаційної безпеки держави, а також відсутністю цілеспрямованого підходу до проблеми в цілому у тих учених, які зачіпали роль інформації в діяльності підприємства. Тому автор в даній роботі намагається проаналізувати питання забезпечення інформаційної безпеки підприємства як суб'єкта інформаційного права та інформаційних правовідносин. **Основною метою** даної статті є вивчення основних вимог щодо забезпечення інформаційної безпеки підприємства.

У системі забезпечення безпеки все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим об'ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі та обробки. Переклад значної частини інформації в електронну форму, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації.

Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства».

Так, В. Цимбалюк характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [5, с. 3]. В. Фурашев вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [6, с. 48]. С. Гуцу пропонує розглядати інформаційну безпеку 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 [7, с. 35]. О. Литвиненко, під інформаційної безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [8, с. 9]. Цікавим та водночас дискусійним є визначення Б. Кормича, який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [9, с. 241]. Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [10, с. 32].

Таким чином, інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різноманітних засобів, що є в її розпорядженні.

Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

О. Сороківська визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [11]. М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації; доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [12, с. 452].

Враховуючи дані визначення, ми погоджуємося з А. Марущаком, що інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що

забезпечує її нормальне функціонування і динамічний розвиток [13, с. 94].

Отже, підсумовуючи вищезазначене, вважаємо за необхідне наголосити, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

Досвід свідчить, що для боротьби з правопорушеннями у сфері обігу інформації на підприємстві необхідна цілеспрямована організація процесу захисту інформаційних ресурсів.

Джерело цього виду загроз може бути внутрішнім (власні працівники), зовнішнім (наприклад, конкуренти) та змішаним (замовники – зовнішні, а виконавець – працівник фірми). Як показує практика, переважна більшість таких правопорушень здійснюються самими працівниками підприємства.

Що ж є безпосереднім об'єктом правопорушень у сфері обігу інформації? Насамперед – це інформація (дані). Правопорушник дістає доступ до інформації, що охороняється, без дозволу її власника, або з порушенням встановленого порядку доступу. Способи такого неправомірного доступу до комп'ютерної інформації можуть бути різними – крадіжка носія інформації, порушення засобів захисту інформації, використання чужого імені, зміна коду або адреси технічного пристрою, представлення фіктивних документів на право доступу до інформації, установка апаратури запису, що підключається до каналів передачі даних. Причому доступ може бути здійснений в приміщеннях підприємства, де зберігаються носії, з комп'ютера на робочому місці, з локальної мережі, з глобальної мережі. Усі загрози на об'єкти інформаційної безпеки за способом впливу можуть бути об'єднані в п'ять груп [14, с. 172]: власне інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні.

Наслідки досконалих протиправних дій можуть бути різними:

- ✓ копіювання інформації (оригінал при цьому зберігається);
- ✓ зміна змісту інформації в порівнянні з тією, яка була раніше;
- ✓ блокування інформації – неможливість її використання при збереженні інформації;
- ✓ знищення інформації без можливості її відновлення;
- ✓ порушення роботи ЕОМ, системи ЕОМ або їх мережі.

Правове регулювання обігу інформації на підприємстві та відповідальності за правопорушення у зазначеній сфері ґрунтується на тому, що за українським законодавством захисту підлягає будь-яка документована інформація, неправомірне звернення до якої може завдати збитку її власникові, користувачеві. Захист здійснюється в цілях витоку, розкрадання, втрати, спотворення, підробки інформації, а також відвертання несанкціонованих дій зі знищення, модифікації, спотворення, копіювання, блокування інформації; відвертання інших форм незаконного втручання в інформаційні ресурси і інформаційні системи, забезпечення правового режиму документованої інформації як об'єкту власності [15]. Крім того, за перелічені вище протиправні дії передбачена як адміністративна, так і кримінальна відповідальність. І це не випадково, оскільки загрози інформаційним системам можуть привести не лише до значних фінансових втрат, але і до безповоротних наслідків – ліквідації самого суб'єкта підприємництва.

Також необхідно враховувати, що загроза інформаційним системам може настати з боку наступних суб'єктів:

- ✓ працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);
- ✓ працівники підприємства, що не мають права в силу своїх службових обов'язків, але здійснили несанкціонований доступ до конфіденційної інформації;
- ✓ особи, які не пов'язані з підприємством трудовою угодою (контрактом).

Аналіз стану справ у сфері інформаційної безпеки свідчить, що на сьогодні в процесі своєї діяльності підприємства, що неодноразово випробовують неправомірні дії інших суб'єктів, не завжди звертаються в правоохоронні органи, або взагалі намагаються не розголошувати випадки посягань на їх інформаційні системи. Це пов'язано з тим, що підприємства, комерційні банки не хочуть «відлякувати» клієнтів, споживачів тим фактом, що їх інформаційні системи (а також і вся інформація, що міститься в них) недостатньо добре захищені. Латентні за

своїм характером проступки приносять найбільшу шкоду, оскільки безвідповідальність правопорушників дозволяє їм продовжувати і розширювати свою незаконну діяльність.

Забезпечення безпеки підприємств з боку інформаційних систем є однією з блоків проблеми безпеки взагалі. Захист від правопорушень у сфері обігу інформації повинен розпочинатися з розробки концепції інформаційної безпеки підприємства.

Способи захисту підприємства від правопорушень у сфері обігу інформації можна розділити на дві групи – організаційні і технічні. Організаційні способи захисту пов'язані з обмеженням можливого несанкціонованого фізичного доступу до інформаційних систем. Технічні способи захисту припускають використання засобів програмно-технічного характеру, спрямованих, передусім, на обмеження доступу користувача, який працює з інформаційними системами підприємства, до тієї інформації, звертатися до якої він не має права [16, с. 46-47].

Фахівці-практики виділяють, наприклад, такі основні напрями технічного захисту інформаційних систем [17, с. 54]:

✓ захист інформаційних ресурсів від несанкціонованого доступу і використання – використовуються засоби контролю включення живлення і завантаження програмного забезпечення, а також методи парольного захисту при вході в систему;

✓ захист від витоку по вторинних каналах електромагнітних випромінювань і наведень – за допомогою екранування апаратури, приміщень, застосуванням маскуючих генераторів шумів, додатковою перевіркою апаратури на наявність компрометуючих випромінювань;

✓ захист інформації в каналах зв'язку і вузлах комутації – використовуються процедури аутентифікації абонентів і повідомлень, шифрування і спеціальні протоколи зв'язку;

✓ захист юридичної значущості електронних документів – при довірчих стосунках двох суб'єктів підприємницької діяльності і коли виникає необхідність передачі документів (платіжних доручень, контрактів) по комп'ютерних мережах – для визначення істинності адресата документ доповнюється «цифровим підписом» – спеціальною міткою, нерозривно логічно пов'язаною з текстом і формованою за допомогою секретного криптографічного ключа;

✓ захист автоматизованих систем від комп'ютерних вірусів і незаконної модифікації – застосовуються імуностійкі програми і механізми модифікації фактів програмного забезпечення.

Отже, на підставі проведеного дослідження, як узагальнення можна зазначити, що підприємства розглядаються як суб'єкти інформаційного права, а тому повинні вивчати інформаційні правовідносини, в які вони практично вступають, реалізовуючи повноваження регульовані нормами різних галузей права, повинні також досліджуватися їх статус як суб'єктів вказаної галузі.

При цьому одним з принципових аспектів, на якому має бути зосереджена увага, є питання забезпечення інформаційної безпеки підприємства. Якщо процедури створення, отримання спеціальних статусів і дозволів, припинення діяльності і нагляд за такою діяльністю більшою мірою відносяться до предмета інших галузей права, то забезпечення інформаційної безпеки, потреба в якому, як автор намагався показати, проявляється впродовж усього часу існування підприємства і його взаємодії з іншими суб'єктами, практично цілком відноситься до предмета інформаційного права. В той же час, як неможливо повною мірою виділити інформаційну складову в діяльності підприємства, так дуже складно розмежувати правове регулювання цієї сфери різними галузями права.

Література

1. *Журавлев Ю. А*. Правовые основы обеспечения информационной безопасности юридических лиц: автореф. дисс. на соискание ученой степени канд. юрид. наук: спец. 12.00.14. «Административное право, финансовое право, информационное право» / Ю.А. Журавлев. – Москва, 2009. – 26 с.

2. *Про* основні засади інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. // Офіційний вісник України. – 2007. – № 8. – Ст. 273.

3. *Бачило И.Л.* Гражданское общество и право / И.Л. Бачило // Информационные ресурсы России. – 2005. – № 3. – С. 10-15.

4. *Сергиенко Л. А*. Культура и гражданское общество / Л.А. Сергиенко // Информационные Ресурсы России. – 2007. – №6. – С.1-6.

5. *Цимбалюк В.С.* Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №8. – С.30-33.

6. *Фурашев В.М.* Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46–56.

7. *Гуцу С.Ф.* Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.

8. *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. / О.В. Литвиненко. – К., 1997. – 18 с.

9. *Кормич Б.А.* Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

10. *Харченко Л.С.* Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2004. – 136 с.

11. *Сороківська О.А.* Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс] / Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

12. *Тацюра М.Ю.* Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23-24 вересня 2010 р. м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра. – Сімферополь: Фенікс, 2010. – С. 451–453.

13. *Марущак А. І.* Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України / А.І. Марущак. – 2011. – № 21. – С. 92–95.

14. *Курушин В. Д.* Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М.: Новый юрист. – 2012. – 256 с.

15. *Про* захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 р. // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 286.

16. *Казакевич О. Ю.* Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов / О.Ю. Казакевич, Н.В. Конев. – М.: Юрфак МГУ, 2011. – 152 с.

17. *Степанов Е. М.* «Кроты» на фирме (персонал и конфиденциальная информация) // Предпринимательское право / Е.М. Степанов. – 1999. – №4. – С. 53-56.

А. Ю. Нашинець-Наумова

Вопросы обеспечения информационной безопасности предприятия

В статье рассматриваются проблемные вопросы обеспечения информационной безопасности предприятия как субъекта информационного права и информационных правоотношений.

A. U. Nashynets-Naumova

Questions of providing of informative safety of enterprise

In the article the problem questions of providing of informative safety of enterprise are examined as an informative legal and informative legal relationships subject.