

УДК 343.102(477):656.13

ФУРМАНЧУК Є., кандидат юридичних наук

## ОКРЕМІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ПРОВАДЖЕННЯ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ

*Анотація.* У статті досліджуються теоретичні та практичні проблеми інформаційної безпеки у сфері провадження господарської діяльності в Україні та шляхи удосконалення захисту інформації в даній сфері.

*Ключові слова:* інформація, інформаційна безпека, інформаційна безпека у сфері провадження господарської діяльності, захист інформації.

*Аннотация.* В статье исследуются теоретические и практические проблемы информационной безопасности в сфере осуществления хозяйственной деятельности в Украине и пути совершенствования защиты информации в данной сфере.

*Ключевые слова:* информация, информационная безопасность, информационная безопасность в сфере осуществления хозяйственной деятельности, защита информации.

*Summary.* The article deals with the research on theoretical and practical problems of information security in the sphere of economic activity implementation in Ukraine and the ways of information protection improvement in this sphere.

*Keywords:* information, information security, information security in the sphere of economic activity implementation, information protection.

**Постановка проблеми.** В умовах побудови в Україні незалежної, демократичної, правової держави з економікою, заснованою на ринкових засадах, надзвичайно важливу роль відіграє забезпечення інформаційної безпеки у сфері господарської діяльності. Держава, здійснюючи свою повсякденну діяльність через призму своїх органів та посадових осіб, забезпечує недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; забезпечує ефективну взаємодію органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; забезпечує побудову та розвиток інформаційного суспільства; забезпечує економічний та науково-технологічний розвиток України; формує позитивний імідж України; інтеграцію України у світовий інформаційний простір [1]. Проте, недосконале нормативно-правове забезпечення інформаційної діяльності у сфері економіки в цілому, зокрема, щодо провадження господарської діяльності в Україні, не задовольняє інформаційно-економічних потреб різних соціальних груп, що є прямою загрозою інформаційній безпеці держави та суспільства.

Проблемам упорядкування інформаційних відносин та інформаційної безпеки були присвячені роботи таких вчених як: Баранов О.А., Бачила І.Л., Брижка В.М., Гаврилова О.О., Копилова В.О., Фурашева В.М. та багато інших. Однак сьогодні питання інформаційної безпеки у сфері господарської діяльності залишається відкритим і потребує подальших досліджень.

**Метою статі** є визначення шляхів удосконалення інформаційної безпеки у сфері провадження господарської діяльності.

**Виклад основного матеріалу.** Відповідно до статті 17 Конституції України інформаційна безпека є однією з найважливіших функцій держави, справою всього Українського народу [2].

Інформаційна безпека являє собою стан захищеності життєво важливих інтересів людини та держави, за якого забезпечується їхнє нормальне функціонування і розвиток та зводиться до мінімуму заподіяння збитків через несвоєчасність і недостовірність інформації, через внутрішні та зовнішні інформаційні загрози [3, с. 38; 4, с. 160-161; 5, с. 134].

Інформаційна безпека створює систему протидії впливу зовнішніх та внутрішніх загроз і захисту власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави [6, с. 42].

Сьогодні поняття “інформаційна безпека” на законодавчому рівні не визначено, хоча робилися спроби щодо такого закріплення. Так, в статті 3 проекту Закону України “Про інформаційний суверенітет та інформаційну безпеку України” від 07.07.98 р. № 1207 визначено, що інформаційна безпека України – це захищеність життєво важливих інтересів суспільства, держави та особи, за якої виключається заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України [7].

У статті 2 проекту Закону України “Про інформаційну безпеку” від 22.09.04 р. № 5732 зазначено, що інформаційна безпека України являє собою комплекс системних превентивних заходів із надання гарантій захисту життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз [8].

Враховуючи те, що інформаційна безпека є частиною національної безпеки, та виходячи з поняття “національна безпека”, закріпленого в Законі України “Про основи національної безпеки”, інформаційну безпеку у сфері провадження господарської діяльності необхідно розглядати як захищеність життєвих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері господарської діяльності при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [9].

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці у сфері провадження господарської діяльності є:

1) недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;

2) несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;

3) використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації, недостатній рівень розвитку національної інформаційної інфраструктури;

4) прояви обмеження свободи слова та доступу громадян до інформації;

5) комп'ютерна злочинність та комп'ютерний тероризм;

6) розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

7) намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [1; 9].

Інформація відіграє важливу роль у сфері провадження господарської діяльності в Україні, дозволяє орієнтуватися в ситуації, планувати свої дії, відстежувати результативність заходів, що проводяться, ухилятися від несподіванок, маніпулювати окремими людьми і організаціями людей (угрупованнями) [10, с. 28-29]. Без інформації органи державної влади не матимуть можливості ефективно виконувати визначенні завдання та функції у сфері провадження господарської діяльності, здійснювати аналітичну роботу, планувати, надавати практичну допомогу, контролювати та охороняти. Тому інформація, що надходить до органів державної влади у сфері провадження господарської діяльності, переробляється з використанням технічних і програмних засобів та накопичується в автоматизованих інформаційних системах. Автоматизовані інформаційні системи у сфері провадження господарської діяльності об'єднують в собі сукупність даних, обладнання, програмних засобів, персоналу, стандартних процедур, які призначені для автоматичного збору, обробки, розподілу, зберігання, представлення інформації згідно з вимогами пошуку і видачі інформації.

Такі автоматизовані інформаційні системи складаються із взаємопов'язаних функціональних підсистем, що забезпечують простоту роботи з отриманою інформацією, постійне поповнення оперативною і достовірною інформацією, оперативний пошук інформації та надають можливість працювати і приймати управлінські рішення у сфері провадження господарської діяльності.

Сьогодні в Україні існують різноманітні автоматизовані інформаційні системи, бази даних щодо провадження господарської діяльності та суб'єктів господарювання, які займаються певними видами господарської діяльності. Так, інформація щодо реєстрації юридичних осіб та фізичних осіб-підприємців збирається, накопичується та зберігається в Єдиному державному реєстрі юридичних осіб та фізичних осіб-підприємців; інформація щодо обліку суб'єктів господарювання – ліцензіатів, а також виданих, переоформлених, визнаних недійсними, анульованих ліцензій та їх копій або дублікатів міститься в Єдиному ліцензійному реєстрі; інформація щодо надання суб'єкту господарювання дозволу, висновку, рішення, погодження, свідоцтва, іншого документу, який дозвільний орган зобов'язаний видати суб'єкту господарювання на провадження певних дій щодо здійснення господарської діяльності або видів господарської діяльності – в реєстрі документів дозвільного характеру; інформація щодо об'єднань громадян та благодійних організацій – в Єдиному державному реєстрі об'єднань громадян та благодійних організацій тощо [11 – 13].

Кожен суб'єкт господарської діяльності вправі вимагати від органів державної влади забезпечення зберігання та захисту інформації, яку було надано, вимагати усунення будь-яких порушень його права на інформацію, захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію.

Говорячи про інформаційну безпеку у сфері провадження господарської діяльності в Україні, необхідно виділити такі основні проблеми:

- 1) організації доступу до інформації;
- 2) організації забезпечення цілісності інформації щодо загроз її порушення;
- 3) організації комплексного контролю за інформаційними ресурсами та їх функціонуванням;
- 4) організації сумісності систем захисту інформації в автоматизованих (комп'ютерних) системах з іншими системами безпеки відповідної організаційної структури;
- 5) організації виявлення можливих каналів несанкціонованого витоку інформації;
- 6) організації блокування (протидії) несанкціонованого витоку інформації;
- 7) організації виявлення, кваліфікації, документування порушення інформаційної безпеки;
- 8) формування відповідальності і правового визначення санкцій та організації притягнення винних осіб до відповідальності (дисциплінарної, цивільної, адміністративної, кримінальної) [14, с. 169].

Інформація, що надходить до таких інформаційних ресурсів, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації та полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки.

Відповідно до Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” захист інформації являє собою діяльність, спрямовану на запобігання несанкціонованим діям щодо інформації в системі. Істотна частина проблем забезпечення захисту інформації може бути вирішена організаційними заходами, проте з розвитком інформаційних технологій зростає і потреба в застосуванні технічного захисту та вжитті технічних заходів [15].

Технічний захист інформації являє собою вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Технічний захист інформації полягає в захисті інформації від несанкціонованого доступу та витоку технічними каналами.

Власник системи, в якій обробляється інформація, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Захист інформації повинен забезпечуватись на всіх технологічних етапах обробки інформації і в усіх режимах функціонування.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган [15].

Для захисту інформації в органах, що здійснюють державний контроль (нагляд) у сфері провадження господарської діяльності, встановлюється спеціальне програмне забезпечення для захисту інформації, запроваджуються система розмежування доступу до інформації, система ідентифікації та автентифікації, система аудиту та моніторингу та система антивірусного захисту.

Як показує практика, одним з основних способів захисту інформації органами, що здійснюють контроль та нагляд у сфері провадження господарської діяльності, є

запровадження системи ідентифікації та автентифікації. Орган державної влади, який отримав інформацію від суб'єктів господарської діяльності, повинен вжити всіх заходів щодо її зберігання, розподілу між структурними підрозділами та їхніми працівниками, підготовки до переробки, переробки, надання такої інформації в переробленому вигляді, аналізі, забезпечення прямих і зворотних зв'язків у її циркуляції.

Ця мета досягається шляхом надання кожному працівнику певного виду доступу до інформації на основі попередньої ідентифікації, тобто введення реєстраційного ім'я користувача в системі (логін) та паролю (певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом у мережі). Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі значенням, яке зберігається в спеціальній захищеній базі даних, і в разі успішної автентифікації проводить авторизацію з подальшим допуском користувача до роботи в системі.

Забезпечення інформаційної безпеки у сфері провадження господарської діяльності має базуватися на таких принципах, як: свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів; запобігання правопорушенням в інформаційній сфері; економічна доцільність; гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції. А для цього необхідна державна підтримка вітчизняного виробника інформаційної продукції та телекомунікаційного обладнання, національних операторів телекомунікацій, зокрема, шляхом створення нормативно-правових, фінансових, фіскальних та інших передумов для підвищення їх конкурентоспроможності на світовому та національному ринках інформаційних та телекомунікаційних послуг.

### ***Висновки.***

Не зважаючи на досить розгалужену систему забезпечення безпеки інформації та її захисту, Україні необхідно і надалі вживати заходів щодо підвищення безпеки інформаційних систем, включаючи мережі зв'язку, насамперед безпеку первинних мереж зв'язку та інформаційних систем органів державної влади у сфері провадження господарської діяльності, оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації, створення організаційної структури системи забезпечення інформаційної безпеки.

Проблема інформаційної безпеки у сфері провадження господарської діяльності не може бути вирішена без впровадження нових ідей до політики у сфері інформатизації. Для забезпечення інформаційної безпеки України у сфері провадження господарської діяльності держава має здійснювати підтримку вітчизняних виробників, формувати вітчизняну індустрію інформаційних послуг, підвищувати ефективність використання державних, корпоративних і приватних інформаційних ресурсів; здійснити гармонізацію законодавства України з питань інформаційної безпеки в економічній сфері з міжнародними нормами і стандартами; розробити та вдосконалити методи і засоби захисту інформації; забезпечити сталий розвиток національного медіа-ринку під час впровадження в Україні цифрового телерадіомовлення; посилити державний контроль за додержанням вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації; здійснити комплексну інформатизацію процесів формування, розподілення і контролю за використанням бюджетних коштів; удосконалити систему статистичної звітності з метою підвищення оперативності, достовірності і релевантності звітної інформації.

### Використана література

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009. – Режим доступу : [//www.rada.gov.ua](http://www.rada.gov.ua)
2. Конституція України // Відомості Верховної Ради (ВВР). – 1996. – № 30. – Ст. 141.
3. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 “Адміністративне право і процес; фінансове право; інформаційне право” // Ю.П. Бурило. – К., 2008. – 19 с.
4. Щодо визначення інформаційної безпеки та її різновидів / В. Петрик : з матеріалів міжнар. наук-практ. конф. [“Форми та методи забезпечення інформаційної безпеки держави”], (Київ, 13 березня 2008 р.). – К. : Видавець Захаренко В.О., 2008. – 216 с.
5. Баранов О.А. Інформаційне право України : стан, проблеми, перспективи / О.А. Баранов. – К. : ВД “СофтПрес”, 2005. – 316 с.
6. Боровський О.О. Безпека національна [соціол. енцикл.] / О.О. Боровський ; укл. В.Г. Городяненко. – К. : Академвидав., 2008. – 456 с.
7. Про інформаційний суверенітет та інформаційну безпеку України : проект Закону України від 07.07.98 р. № 1207. – Режим доступу : [//www.rada.gov.ua](http://www.rada.gov.ua)
8. Про інформаційну безпеку України : проект Закону України від 22.09.04 р. № 5732. – Режим доступу : [//www.rada.gov.ua](http://www.rada.gov.ua)
9. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Відомості Верховної Ради (ВВР). – 2003. – № 39. – Ст. 351.
10. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко та ін. – К. : НДЦПІ АПрН України, 2007 р. – 234 с.
11. Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців : Закон України від 15.05.03 р. № 755-IV // Відомості Верховної Ради (ВВР). – 2003. – № 31-32. – Ст. 263.
12. Про ліцензування певних видів господарської діяльності : Закон України від 01.06.00 р. № 1775-III // Відомості Верховної Ради (ВВР). – 2000. – № 36. – Ст. 299.
13. Про державне підприємство “Інформаційний центр” Міністерства юстиції України : Постанова Кабінету Міністрів України від 14.07.99 р. № 1272.
14. Вступ до інформаційної культури та інформаційного права ; за заг. ред. М.Я. Швеця, Р.А. Калюжного. – Ужгород : ІВА, 2003. – 240 с.
15. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. № 80/94-ВР // Відомості Верховної Ради України (ВВР). – 1994. – № 31. – Ст. 286.

~~~~~ \* \* \* ~~~~~