УДК 004.056.5

Інформаційна безпека суспільства: концептуальний аналіз

Муравська (Якубівська) Ю.Є.
кандидат економічних наук, доцент,
доцент кафедри економічної безпеки та фінансових розслідувань
Тернопільського національного економічного університету

Стаття присвячена розгляду питань, пов'язаних з інформаційною безпекою в епоху інформаційного суспільства, і являє собою міждисциплінарні уявлення про ризики, пов'язані з функціонуванням безпеки в сучасному суспільстві, насамперед на основі збору, обробки та захисту інформації. Автором проведено концептуальний аналіз категорій у сфері безпеки. Основна увага зосереджена на сутності поняття «інформаційна безпека», а також відмінностях між розвідувальною діяльністю та промисловим шпигунством.

Ключові слова: економічна безпека, інформаційна безпека, інформаційне суспільство, розвідувальна діяльність, промислове шпигунство.

Муравская (Якубивская) Ю.Е. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЩЕСТВА: КОНЦЕПТУАЛЬНЫЙ АНАЛИЗ

Статья посвящена рассмотрению вопросов, связанных с информационной безопасностью в эпоху информационного общества, и представляет собой междисциплинарные представление о рисках, связанных с функционированием безопасности в современном обществе, прежде всего на основе сбора, обработки и защиты информации. Автором проведен концептуальный анализ категорий в сфере безопасности. Основное внимание сосредоточено на сущности понятия «информационная безопасность», а также различиях между разведывательной деятельностью и промышленным шпионажем.

Ключевые слова: экономическая безопасность, информационная безопасность, информационное общество, разведывательная деятельность, промышленный шпионаж.

Muravska (Yakubivska) Y.Y. INFORMATION SECURITY OF SOCIETY: CONCEPTUAL ANALYSIS

The scientific article is devoted to issues related to information security in the information society, and represents an interdisciplinary understanding of the risks associated with the functioning of security in today's society, primarily based on the collection, processing and data protection. The author made a conceptual analysis of categories of security. The main focus is based on the essence of the concept of "information security" as well as differences between the intelligence activities and industrial espionage.

Keywords: economic security, information security, information society, intelligence activities, industrial espionage.

Постановка проблеми у загальному вигляді. Сучасні реалії функціонування і ведення бізнесу в епоху інформаційного суспільства приносять нові загрози для економічної безпеки. Міждисциплінарні знання в галузі безпекознавства, права, економіки, менеджменту та інформатики дають можливість вивчити ці ризики і прийняти рішення, які зводять до мінімуму загрози для інформаційної безпеки. Субдисципліна економічної безпеки – інформаційна безпека – відіграє важливу роль у визначенні економіко-правових явищ, у тому числі досліджені ризиків, що впливають на сферу безпеки в широкому розумінні. Безпекознавчі теорії підкреслюють функцію інформаційного суспільства як типу суспільства, в якому інформація відіграє ключову роль. Інформація є набагато важливішою і ціннішою, ніж матеріальні ресурси.

Аналіз останніх досліджень і публікацій. У статті основна увага акцентується на взаємозв'язку економічного та юридичного аспектів як елементів загальної системи інформаційної безпеки, що регулює діяльність у сфері розвідувальної діяльності та економічної безпеки загалом. На основі опрацювання наукових досліджень І.В. Зайцевої-Калаур [8], а також попередніх публікацій Ю.Є. Якубівської [9; 10], публікацій закордонних вчених А. Гідденса [1], М. Яблонського М. Мелуса [2], М. Калінського, А. Керковської, Г. Томашевського [3], Н. Полмара і Т. Аллена [4], М. Германа [5], Л. Коженьовського [6], З. Людзієвського [7], а також законодавства України щодо інформаційної безпеки, можна дійти висновку про науково-практичне значення їхніх досліджень.

Виділення невирішених раніше частин загальної проблеми. Актуальність тематики

цієї статті пояснюється необхідністю концептуального осмислення понять «безпека», «інформаційна безпека», а також пошуку меж у розумінні категорій «розвідувальна діяльність» та «промислове шпигунство».

Формулювання цілей статті. Мета статті полягає у концептуальному осмисленні та аналізі категорій у сфері інформаційної безпеки, яка є ефективною в контексті її сприйняття. З метою досягнення вищевказаної мети потрібно вирішити такі завдання:

– проаналізувати інтерпретацію концепції безпеки та подати її характеристику;

– охарактеризувати інформаційну культуру та безпеку інформації;

– дослідити ключові відмінності між розвідувальною діяльністю та промисловим шпигунством;

– запропонувати удосконалене визначення інформаційної безпеки.

Виклад основного матеріалу дослідження. Інформаційне суспільство є одним із типів суспільств, які розвиваються в результаті соціального прогресу. У соціальному просторі інформація стає матеріалізованим результатом комунікації, який базується на знаннях. Завдяки інформації ми передаємо дані або повідомлення, які є частиною процесу подальших дій у суспільстві та унікальними за своєю значущістю.

Варто зазначити, що почуття безпеки стало вагомим фактором для кожного із суспільств. Вже зараз деякі автори пропонують заміну термінів «мир» та «війна» на категорії «безпека» та «загроза». У певному значенні взаємозамінність цих термінів також зумовлена соціально-культурними змінами. Сучасні соціологічні теорії інтерпретують та пояснюють також і безпекознавчі процеси, що відбуваються протягом останніх кількох років. Вони засновані на різних моделях соціальної реальності, вказуючи на відмінність факторів у забезпеченні безпеки на мікро- та макрорівнях.

Безпека є однією з основних людських потреб, тобто дуже важливою для суспільства. Почуття безпеки повинно бути пов'язане зі станом миру, відсутністю страху. Інформаційна безпека у своїх дослідженнях зосереджується на визначенні стану загроз для пристроїв, систем, сегментів руху і заходів інформаційного забезпечення, а також ймовірності виникнення загроз для них. Для кожного суспільства питання безпеки є одним із основних вимірів його способу мислення про соціальну реальність. Безпека є державним завданням, що полягає у відсутності загроз, які суб'єктивно сприймаються окремими особами і групами. Це означає, що безпека складається з двох елементів: об'єктивного і суб'єктивного. Перший з них, що має об'єктивний характер, є зовнішнім щодо особистості, соціальної групи, спільноти. Другий носить суб'єктивний характер і є відчуттям безпеки. З позиції суспільних відносин безпекою можна назвати стан, у якому людина має відчуття впевненості, почуття довіри до іншої особи або правової системи. Протилежністю безпеки є стан загроз.

Згідно з дослідженнями автора безпека розуміється як визначена впевненість біологічних та соціальних істот, яку можна спостерігати через три взаємозалежних виміри, такі як суб'єктивний вимір (як визначеність існування і виживання, що підтверджується відсутністю серйозних загроз для інтересів, що пов'язані з фізичним існуванням), а також об'єктивний і процесуальний вимір (як впевненість у необхідності умов розвитку та активності у цей час і в близькому майбутньому).

Безпека не повинна розглядатися як незалежна змінна, оскільки вона

– динамічна і процесуальна – підлягає постійним змінам під впливом комплексу багатофакторних явищ;

– суб'єктивна й об'єктивна – у разі, коли соціальні відносини безпеки утворюються в результаті впливу цього явища на індивідуумів, соціальні групи, суспільство;

– вирівняна, структурована;

– відносна – залежно від кількості факторів.

Вплив на безпеку мають всі соціальні взаємодії, а також економічні чи політичні. Культура безпеки суспільства вказує на зобов'язальну систему значень, за допомогою яких певна група людей розуміє зміст загроз. Створення сучасної інформаційної культури заснована на процесах комунікації та передачі інформації. До аспектів комунікації звертається А. Гідденс, описуючи їх як потік інформації від однієї особи або групи осіб до іншої особи або групи [1]. Комунікація має важливе значення для суспільної взаємодії. Тому очевидною необхідністю є поєднання безпеки з культурним виміром людини.

Безпека в суспільній системі має очевидне значення. Інформаційна культура дає нам змогу зрозуміти явища, які є інформацією і комунікаціями, а також їх використання в організації. Можна навіть вважати, що інформаційна культура є одним із найбільш важливих елементів потенціалу безпеки, що дуже

близький до поняття культури управління. Обидва елементи зорієнтовані на передачу інформації. Інформація (її зміст, якість, час передачі, важливість завдань) символізує потенціал успіху організації чи бізнесу.

Чужа таємна інформація викликає настільки велику цікавість, що витрачаються значні зусилля та кошти для її отримання. Загроза відсутності інформації або небезпека втратити таємницю завжди супроводжує людину. Інформація може ускладнити життя і розвиток, стати причиною руйнування і розпаду або шансом для несподіваного успіху і фортуни. Причиною цього є розвиток економічних, політичних і військових відносин, основним елементом яких є конкуренція. Вплив на ці сфери має водночас і глобалізація, яка зумовлює значні зміни у підході до джерел сировини, необхідних для виробництва, а також нових ринків та тих, що перебувають у процесі відкриття. Зазначені чинники спричинили переоцінку підходів до поняття безпеки. Ці процеси можна спостерігати у житті окремих фізичних осіб, а також економічних інституцій або навіть державних установ. Розвиток сучасних інформаційних технологій на рівні небачених до сьогодні масштабів зумовив розвиток обміну інформацією та підвищення її значення, особливо інформації про діяльність потенційного конкурента або навіть суперника. Весь зазначений стан справ можна назвати прогресивною інформаційною війною. Зокрема, інформація витісняє традиційні блага і стає одним з основних і необхідних ресурсів.

Почуття безпеки є однією з основних потреб людини – найвищою соціальною цінністю. Безпека характеризує комплексний індекс всіх часткових вартостей, які є найбільш цінними для людини. Тому, зараховуючи безпеку до основних благ, варто підкреслити, що вона повинна бути об'єктом найпильнішої уваги в управлінні кожної господарської одиниці.

Автором запропоновано напрями побудови ситуаційної моделі безпеки, яка є ефективною в контексті її сприйняття. Вона охоплює чотири стани:

– стан відсутності безпеки, в якому є реальна і серйозна зовнішня загроза, про яку є адекватне уявлення;

– стан одержимості, в якому невелика загроза розглядається як велика;

– стан помилкової безпеки, в якому значна загроза розглядається як невелика;

– стан безпеки, де внутрішня загроза є низькою.

Коли переходимо до концепції інформаційної безпеки, то бачимо відмінності у визначенні цього явища окремими авторами. І. Зайцева-Калаур зазначає, що поняття інформаційної безпеки особистості та суспільства є тісно пов'язаними, оскільки інформаційна безпека окремої особистості формує у кінцевому результаті інформаційну безпеку суспільства та держави [8, с. 182]. Інформаційну безпеку можемо визначити охороною інформації, яка полягає в ускладненні отримання даних про фізичну природу наявного або планованого стану речей і явищ у їхньому власному просторі функціонування, а також у перешкоджанні внесення змін до інформаційних комунікацій та фізичного знищення носіїв інформації. Інше визначення інформаційної безпеки, запропоноване М. Яблонським і М. Мелусем [2], передбачає низку заходів, яких необхідно вжити, щоб отримати бажаний стан безпеки (запобігання (профілактика), відлякування, індикація і застереження, виявлення, підготовка до надзвичайної ситуації і реакція на можливі атаки). З розвитком інформаційного суспільства і зростанням значення інформації в економічному житті шляхом комп'ютеризації рівень захисту інформації стає пріоритетним показником. Вдалі визначення області безпеки інформації подали М. Калінські, А. Керковська та Г. Томашевський. Інформаційна безпека є не тільки фізичною безпекою і забезпеченням захисту технічних інформаційних ресурсів. Інформаційна безпека насамперед є прагненням забезпечити і підтримувати конфіденційність, цілісність, доступність, підзвітність, автентичність, безвідмовність і достовірність інформації і систем, в яких вона обробляється [3].

На основі розглянутих у статті визначень можна запропонувати удосконалене ширше визначення інформаційної безпеки як стану, вільного від загроз, що сприймаються в основному як надання інформації стороннім особам; шпигунство; саботаж та диверсійні заходи. Інформаційна безпека являє собою також будь-яку дію, систему або метод, які спрямовані на захист інформаційних ресурсів, що передаються, зберігаються в пам'яті комп'ютерів і телекомунікаційних мереж. Інформаційна безпека – це не тільки захист від несанкціонованого доступу, крадіжки даних або їх знищення. Варто її розуміти набагато ширше. Інформаційна безпека розуміється як компонент фізичної, особисто-організаційної та IT-безпеки господарюючого суб'єкта чи іншої інституції.

Не можна заперечувати той факт, що інформаційні ресурси є найбільш цінним активом кожної компанії. Оцінка цієї інформації привела до усвідомлення менеджерами компаній, що ефективність їхньої діяльності і конкурентоспроможність на ринку залежить від пошуку та отримання інформації. Це привело до зростання значення, а також розвитку бізнес-аналітики та, відповідно, розвідувальної діяльності. Особливий інтерес у конкуруючих компаній викликають результати досліджень і конструкційні плани, а також списки постачальників і клієнтів, заплановані маркетингові кампанії та цінова політика.

Отримання інформації про конкуренцію має довгу історію в економіці, проте термін «економічна розвідка» в контексті організованого збору даних з'явився порівняно нещодавно. Ми можемо прийняти за початок вісімдесяті роки двадцятого століття. Тоді в американських коледжах почали викладати предмет про збір інформації про конкуренцію. Визначення поняття економічної розвідки подали у своїй енциклопедії Н. Полмар і Т. Аллен, які зазначили, що економічна розвідка – це збір інформації економічного характеру в основному з відкритих та вільних джерел [4]. З іншого боку, на думку М. Германа, розвідувальна діяльність включає в себе збір інформації, задавання питань, опис, підготовку відповідних гіпотез і подання доказів для того, щоби провадити найефективнішу політику [5].

Розвідка у звичному розумінні – це отримання інформації від респондента через безпосередній контакт. Звичайно, в епоху інноваційних рішень прямий контакт не завжди означає особистий. Характерною є відмінність між сприйняттям розвідки як чогось позитивного та концепцією шпигунства, що в основному носить негативний відтінок. На цю відмінність також звертає увагу Л. Коженьовська [6]. Основна відмінність між розвідкою і шпигунством стосується методів і джерел отримання інформації. Економічна розвідка використовує в основному правові методи і відкриті джерела інформації, тоді як шпигунство використовує заборонені законом і секретні методи, що охоплюються таємницею або захищеними джерелами інформації. Границя відмінності між так званими економічною розвідкою і промисловим шпигунством є гладкою, і часто те, що одна держава розглядає як економічну розвідку, інші можуть розглядати як промислове шпигунство, спрямоване на отримання прибутку [7].

Сам процес збору цінної інформації через спеціалізовані фірми або зовнішні компанії, які спеціалізуються на цьому, є схематичним і може бути представлений таким чином:

– планування – визначення цілей розвідки, способів отримання інформації та ефективності контролю осіб, які займаються цим збором;

– збір – процес отримання інформації та передачі її для подальшої обробки;

– обробка – це процес перетворення інформації у готові дані розвідки, а також аналіз та інтерпретація;

– передача – розподіл розвідувальних даних між отримувачами.

Не існує єдиної схеми організації роботи людей, що беруть участь в отриманні економічної інформації. У багатьох країнах найбільш поширеною формою є інституціоналізація, створення компаній, які, як правило, називають економічними розвідками і які мають необхідні знання та навички для пошуку та отримання інформації. Вони пропонують іншим підприємствам свої послуги на відкритому ринку. Деякі компанії організовують такі відділи в межах своєї організаційної структури, однак великим недоліком цього рішення є правильний підбір і навчання працівників, а також персоналу, відповідального за координацію їхньої діяльності. Проблемою може бути також надання відповідної технічної та інформаційної підтримки. Незалежно від того, чи процес збору інформації довіряється зовнішній компанії, чи працівникам самого підприємства, вкрай важливо, щоб їхня діяльність була в межах закону, а інформація була отримана за допомогою правових методів. В Україні економічний простір інформаційної безпеки регулюють закони і нормативні акти, такі як Закон України «Про інформацію»; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; Закон України «Про державну таємницю»; Закон України «Про захист персональних даних»; Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»; Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» та інші.

Як зазначалося у попередніх дослідженнях автора, в Україні основний акцент робиться на відповідність міжнародним нор-

мам та стандартам, що відображається на організації установ, що регулюють процес інтелектуалізації та науково-технічного розвитку як на національному, так і на глобальному рівні, а відтак є чинниками формування ефективного інституційного середовища у цій сфері [9]. Фактичний рівень відповідності законодавства України у сфері інтелектуальної власності не повністю враховує положення міжнародних актів, що є важливою передумовою інформаційної безпеки в контексті забезпечення євроінтеграційних процесів [10, с. 38]. Правові міркування вказують на те, що інформаційна безпека є не поодиноким актом, а процесом його безперервного забезпечення.

Висновки з цього дослідження. Розвиток технологій, зокрема телекомунікаційних систем та електроніки, привів до надзвичайно швидкого зростання комунікаційних можливостей. Настала ера інформації, яка стала найважливішим і найбільш бажаним з усіх ресурсів. Більшість зі складників успіху, будь то бізнес, військові або державні справи, ґрунтуються на передачі, придбанні і контролі інформації. Інформаційні системи в сучасному економічному просторі з огляду на широкомасштабне використання цифрових інструментів становлять, з одного боку, безцінне джерело знань про стан господарюючих суб'єктів, а з іншого – є мішенню для несанкціонованого збирання та отримання такої інформації і конкурентної боротьби. Тому все більше усвідомлюється важливість знань для життя людини і функціонування економіки. Це приводить до природного стану, коли ми захищаємо інформацію, розглядаючи її як найбільше благо. Водночас конкуренти хочуть отримати чужі знання за найнижчою ціною. У результаті конфлікту інтересів, а також розвідувальних дій все частіше використовуються ефективні методи отримання інформації і захисту від них. Характер цих заходів майже повністю переведений із соціального ґрунту або частково військового (хоча придбання інформації завжди була невід'ємною частиною військових справ) до рівня економічного і отримання знань про конкурентоспроможність інших компаній. Поширення цього явища значною мірою залежить від рівня комп'ютеризації, індустріалізації і розміру країни, в якій працює підприємство.

Метою захисту інформації є забезпечення безпеки для цінних ресурсів організації, таких як управлінська інформація, інформація про обладнання та інформація про застосування програмного забезпечення. За допомогою вибору відповідних заходів безпеки забезпечується більш ефективне досягнення бізнес-цілей, захист цілей компанії, місії, матеріальних і фінансових ресурсів, репутації та співробітників. Тому дуже важливо дослідити ризики, пов'язані з безпекою інформації, та способи боротьби з такого роду загрозами. У зв'язку з дуже динамічними змінами, які відбуваються з розвитком інформаційних технологій, з'являються нові, раніше невідомі загрози. Особливим полем для маневру є розвиток інформаційних технологій, що дає змогу придбати інформацію віддалено, без фізичної присутності в місці зберігання. Це є викликом не тільки для підприємців, які дбають про свої власні інтереси, але й для держави, яка повинна побудувати ефективну правову систему для захисту від шпигунських дій.

ЛІТЕРАТУРА

1. Giddens A., Griffiths S. Sociology, Cambridge : Polity, 5th ed., 2006. – 1050 p.

2. Jabłoński M., Mielus M., Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej, [w:] Bezpieczeństwo informacji i biznesu Zagadnienia wybrane,pod red. Kwieciński M., Oficyna Wydawnicza AFM, Kraków 2010. – S. 11–14.

3. Kaliski M., Kierkowska A., Tomaszewski G., Ochrona informacji i zasobów relacyjnych przedsiębiorstwa [w:] Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu,pod red. Kaczmarek J., Kwieciński M., Wyd. Dom Organizatora, Toruń 2010. – S. 10–14.

4. Polmar N., Allen T.B., Księga szpiegów, Encyklopedia, Wyd.Magnum, Warszawa, 2000. – 702 s.

5. Herman M., Potęga wywiadu, Wyd. Bellona, Warszawa, 2002. – 112 s.

6. Korzeniowska H., Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji, Wyd. EAS, Kraków, 2004.– 68 s.

7. Ludziejewski Z. Bezpieczeństwo informacyjne w instytucjach gospodarczych. Zeszyty naukowe WSOWL, Nr 4 (170), 2013. – S. 5–15.

8. Зайцева-Калаур І.В. Інформаційне право : [Навчальний посібник] / І.В. Зайцева-Калаур. – Тернопіль: ФО-П Шпак В.Б., 2014. – 185 с.

9. Якубівська Ю.Є. Імплементація міжнародних норм у сфері інтелектуальної власності в національну практику в контексті підвищення ефективності інституційного середовища / Ю.Є. Якубівська // Ефективна економіка [Електронне наукове фахове видання]. – № 10. – Дніпропетровськ : ДДАТУ, 2015. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4430

10. Якубівська Ю.Є. Колізії норм права та компетенції органів управління у сфері інтелектуальної власності як загроза інформаційній безпеці / Ю.Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Юридичні науки. – К. : УДУФМТ, 2015. – № 4 (81). – С. 37–42.