РОЗДІЛ 8. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

ІНФОРМАЦІЙНА БЕЗПЕКА ДІЯЛЬНОСТІ ПІДПРИЄМСТВ
INFORMATION SAFETY OF ENTERPRISES

УДК 004.056

Убийвовк І.І.
старший викладач кафедри економіки та математичних дисциплін
Полтавський інститут економіки і права

У статті розглянуто організацію інформаційної безпеки діяльності підприємств, яка відіграє важливу роль під час реалізації загальної стратегії та тактики безпеки підприємства. Від вдалої реалізації прийнятої політики в області інформаційної безпеки залежать конфіденційність особистої інформації та ступень її захисту для забезпечення комерційних інтересів підприємства. Запропоновано результати аналізу проблем інформаційної безпеки в умовах ринкової економіки. Наведено приклади організації управління інформаційною безпекою діяльності підприємства.
Ключові слова: *інформаційна безпека, економічна безпека, захист інформації, несанкціонований доступ, безпека інформації.*

В статье рассмотрена организация информационной безопасности деятельности предприятий, которая играет важную роль при реализации общей стратегии и тактики безопасности предприятия. От успешной реализации принятой политики в области информационной безопасности зависят конфиденциальность личной информации и степень ее защиты для обеспечения коммерческих интересов предприятия. Предложены результаты анализа проблем информационной безопасности в условиях рыночной экономики. Приведены примеры организации управления информационной безопасностью деятельности предприятия.
Ключевые слова: *информационная безопасность, экономическая безопасность, защита информации, несанкционированный доступ, безопасность информации.*

In article the organization of information security of activities of the entities is considered. Organization of information security has an important role in the implementation of the overall strategy and tactics of security. The successful implementation of adopted policies on information security depends on the confidentiality of personal data and the degree of protection for the commercial interests of the company. In the article the analysis of information security problems in a market economy are offered. Examples of the organization's information security management activities of the enterprise are performed.
Key words: *information security, economic security, information protection, unauthorized access, information security.*

Постановка проблеми. У наші дні інформація має надзвичайну цінність, яка може визначатися не тільки обсягами праці, витраченої на її створення, але й розміром прибутку, отриманого від її можливої реалізації. Проблема сучасності – захист інформації, надійне забезпечення збереження та встановлення статусу використання.

Становлення інформаційного суспільства має як позитивні, так і негативні наслідки: пришвидшилася передача інформації значного обсягу, прискорилась її обробка та впровадження, але занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю.

Перехід суспільства до інформаційного змінив статус інформації – може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. Одним із головних пріоритетів є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя. Саме цим зумовлена актуальність забезпечення інформаційної безпеки інтересів людини (громадянина), суспільства та держави в цілому.

Тривалий час розуміння інформаційної безпеки в наукових та нормативно-правових джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому з низки питань, присвячених розгляду проблеми забезпечення інформаційної безпеки, найбільш вивченими та дослідженими її аспектами є безпека інформації (інформаційно-технічна безпека).

Аналіз останніх досліджень і публікацій. Різні аспекти забезпечення інформаційної безпеки підприємства та вдосконалення управління нею досліджено у працях багатьох вітчизняних і зарубіжних учених, зокрема визначення змісту інформаційної безпеки діяльності підприємства, аналіз загроз та індикаторів інформаційної безпеки висвітлено в працях О.Ф. Бєлова, О.І. Барановського, М.А. Бендикова, М.М. Єрмошенка, Я.А. Жаліла, Т.Т. Ковальчука, Г.В. Козаченка, Н.О. Лоханова, О.М. Ляшенко, В.І. Мунтіяна, Є.А. Олейнікова, С.К. Реверчука та ін.

Постановка завдання. Метою даної статті є дослідження проблем інформаційної безпеки діяльності підприємств в умовах ринкової економіки.

Виклад основного матеріалу дослідження. Одна з основних внутрішньовиробничих функціональних складників безпеки підприємства – інформаційна. Вона полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Належні служби підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційного складника безпеки підприємства. До таких належать: збирання всіх видів інформації щодо діяльності того чи іншого суб'єкта господарювання;аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів; прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів; оцінка рівня економічної безпеки за всіма складниками та в цілому; розробка рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання; інші види діяльності з розробки інформаційного складника економічної безпеки.

На підприємство постійно надходять потоки інформації, що розрізняються за джерелами їхнього формування. Заведено відокремлювати: 1) відкриту офіційну інформацію; 2) вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації; 3) вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації.

Оперативна реалізація заходів із розробки та охорони інформаційного складника економічної безпеки здійснюється послідовним виконанням певного комплексу робіт. Виділяють п’ять напрямів: 1) збирання різних видів необхідної інформації; 2) обробку та систематизацію одержаної інформації; 3) аналіз одержаної інформації; 4) захист інформаційного середовища підприємства, що охоплює: заходи для захисту суб'єкта господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб; технічний захист приміщень, транспорту, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації; збирання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій із метою припинення таких спроб; 5) зовнішню інформаційну діяльність [5, с. 223].

Серед сучасних підприємців панує думка, що використовуючи основні правила безпеки, можна добитися значних успіхів у бізнесі. До них належать: розвідка; професіоналізм у встановленні контактів (мінімальні витрати часу і сил для пошуку інформації, необхідної для налагодження контакту); кваліфікація менеджера (витрати часу тільки на потрібних людей); уміння долати перешкоди, пошук варіантів і обхідних шляхів для дозволу виникаючих проблем; уміння завершувати операцію навіть з негативним результатом (усе ж краще, ніж відсутність якого-небудь результату). Інформація – це засіб, за допомогою якого розвідка робить вплив на проведення і розробку політики будь-якої фірми і забезпечення її безпеки, що представляється своєчасно в усній або письмовій формі керівництву фірми.

Сьогодні всі комерційні структури розвинених держав мають у своєму штаті підрозділи, які займаються інформаційною діяльністю. В одних фірмах це інформаційно-аналітичний відділ, в інших – відділ маркетингу, на який керівництво фірми разом з іншими покладає й інформаційно-аналітичні завдання, або відділ комерційної розвідки. Часто все залежить від рівня розуміння керівництвом фірми ступеня важливості інформаційно-аналітичної роботи для безпеки всіх сторін діяльності будь-якої комерційної структури.

Основне завдання – збір інформації: 1) про економічний стан фірми, регіону, своєї країни, країн, в яких є партнери, і т. д.; про політичну ситуацію в регіоні і країні; про морально-психологічний клімат у колективі; 2) про конкурентів і методи конкуренції (кримінальні структури і можливі терористичні погрози); про постановку завдань щодо перевірки потенційних партнерів, клієнтів, конкурентів; 3) розробка програм протидії промисловому шпигунству, терористичним погрозам та іншим методам недобросовісної конкуренції; 4) розробка програм дезінформації конкурентів через засоби масової інформації, інформаційно-телекомунікаційні канали, постачальників, суміжників, партнерів, клієнтів шляхом організації псевдопросочування конфіденційної інформації; розробка програм захисту конфіденційної інформації.

На рис. 1 показано зразок структури інформаційно-аналітичного підрозділу [1, с. 38], завданням якого є обробка інформації.

Першою важливою операцією є аналіз, який служить додатковим фільтром, що відкидає непотрібне і що є захистом від шуму без підстави. Ця операція полягає у визначенні важливості, точності і значущості інформації. Інформація є важливою, якщо вона зв'язана, тобто має зв'язок з елементами бази, і якщо вона здатна внести внесок до організації. Коли внесок значимий і безпосередній, інформація вимагає термінових дій. Інформація, що не має значення, повинна бути виключена, щоб уникнути втрати часу й енергії. Не завжди легко встановити, є інформація достовірною або помилковою, особливо якщо вона містить відомості про події, які ще не відбулися.

Допускається два критерії, по яких можна судити про точність інформації, надійність дже-

рела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження за іншими джерелами, якщо можливо – за незалежним.

Інформація може бути важливою і точною і водночас даремною, оскільки вона недостатня для розуміння і дії. Розвідка в бізнесі належить до даних про навколишнє середовище і конкурентів, аналізованим із метою використовувати їх в конкретній ситуації. Ні окрема особа, ні організація не можуть ефективно діяти в умовах конкуренції без глибокого розуміння цього середовища або не маючи у своєму розпорядженні новітньої інформації про те, що в ній відбувається.

Вид потрібної інформації залежить від виду компанії (фірми), її конкурентного середовища і багатьох інших характеристик самої фірми та її оточення. Сьогодні практично весь український бізнес у тому або іншому ступені має тіньові сторони: ухилення від податків, подвійну бухгалтерію, захування дійсного об'єму постачань, безготівкові операції через фірми-однодневки та ін. У такій ситуації фірма може стати заручником кримінальної структури, яка бере фірму під свій контроль і може використовувати її для відмивання власних нелегально отриманих коштів. Отже, необхідно постійно володіти інформацією про співвідношення сил і розділення сфер впливу в регіоні, в яких знаходиться фірма, в ніші ринку, яку займає фірма [2, с. 137].

Потреба в інформації варіюється залежно від здійснюваної або планованої діяльності. Компанія може мати довгострокові (стратегічні) плани, тактичні або короткострокові, плани і поточні операції, всі вони вимагають добре вивіреної інформації. Сьогодні переважна маса ділової інформації може бути отримана з відкритих джерел без порушення етичних норм. Система безпеки кожного підприємства цілком індивідуальна. Її повнота та дієвість залежать від наявної в державі законодавчої бази, від обсягу матеріально-технічних та фінансових ресурсів, виділених керівниками підприємств, від розуміння працівників важливості забезпечення безпеки бізнесу.

Надійний захист інформаційної безпеки підприємства можливий лише за комплексного та системного підходу до її організації, тому має місце таке поняття, як «система інформаційної безпеки діяльності підприємства».

Система інформаційної безпеки підприємства – це комплекс організаційно-управлінських, технічних, профілактичних заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.

Для керівників будь-якого підприємства піклування про його безпеку є найголовнішим обов'язком, тому що у разі його розпаду керувати буде нічим. Уважно наглядати потрібно не тільки за процесами, які відбуваються у навколишньому середовищі, а й не меншу увагу необхідно приділяти аналізу власне самої системи. Обов'язковим є оперативна оцінка якості роботи, постійна перевірка достовірності вхідної інформації, надійності всіх елементів системи. Будь-яке підприємство, маючи цілі розвитку, виконує функції забезпечення відносно споживачів його послуг або продукції. Інформаційна безпека – це характеристика, що будується на стосунках системи і середовища, як зовнішнього, так і внутрішнього [4, с. 68].

Інформаційна безпека підприємства повинна оцінюватись з урахуванням умов, обмежень і критеріїв усіх основних учасників його виробничо-економічної діяльності, а саме: держави, підприємств-конкурентів, споживачів. З усього вищезазначеного можна зробити висновок, що для українських підприємств самими значимими проблемами сучасного етапу реформ є: відсутність засобів на технічне переоснащення; неритмічність роботи; відсутність контрактів, замовлення; безробіття; велика дебіторська заборгованість. На шляху зміцнення інформаційної безпеки українських підприємств можна запропонувати такі кроки: зміну системи оплати праці кадрів; ство-

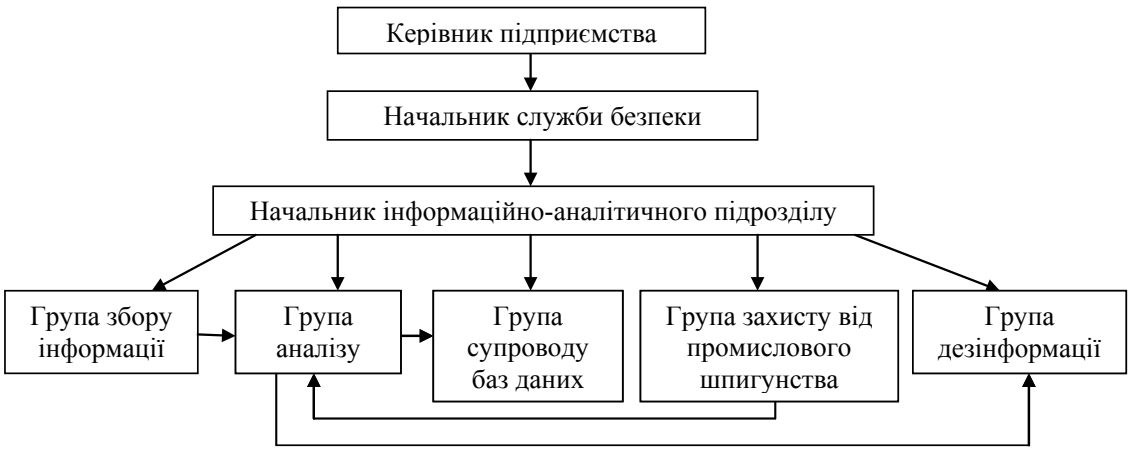

Рис. 1. Зразок структури інформаційно-аналітичного підрозділу

рення нових організаційно-виробничих структур; активну участь у міжнародних виставках, семінарах; у рамках ресурсної безпеки – вдосконалювання системи розрахунків; підвищення продуктивності праці; збільшення капіталовкладень у ресурсозбереження; стимулювання «ресурсного» напряму; у рамках економічної безпеки – застосування принципу дотримання критичних термінів кредитування; створення інформаційного центру, щоб постійно мати відомості про борги підприємства і перекрити канали витоку інформації: створення в структурі інформаційного центру спеціальної групи фінансових робітників, що перевіряла би податкові та інші обов'язкові платежі для виявлення можливої переплати і надавала зведення про маловикористовувані основні виробничі фонди з метою їхнього можливого продажу; використання нових форм партнерських зв'язків; у рамках соціальної безпеки – наближення рівня оплати праці до показників розвитих країн, притягнення робітників до управлінських функцій; підвищення кваліфікації робітників; зацікавленість адміністрації підприємства у працевлаштуванні безробітних; розвиток соціальної інфраструктури підприємства; підвищення матеріальної відповідальності робітників за результати своєї праці [3, с. 90].

Серед наявних засобів забезпечення безпеки підприємства можна виокремити такі:

– технічні засоби (охоронно-пожежні системи, відео- та радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо);

– організаційні засоби (створення спеціалізованих формувань, що забезпечують безпеку підприємства);

– інформаційні засоби (друкована і відеопродукція з питань збереження конфіденційної інформації);

– фінансові засоби (без достатніх фінансових коштів неможливе функціонування системи економічної безпеки підприємства);

– правові засоби (підприємство повинне у своїй діяльності керуватися не лише виданими вищестоящими органами влади законами та підзаконними актами, але й розробляти власні локальні правові акти з питань забезпечення економічної безпеки підприємства);

– кадрові засоби (підприємство повинне бути забезпечене кадрами, що займаються питаннями економічної безпеки);

– інтелектуальні засоби (залучення до роботи кваліфікованих спеціалістів, наукових робітників, що дає змогу модернізувати систему безпеки підприємства).

Одночасне впровадження всіх цих засобів неможливе. Воно проходить в кілька етапів: виділення фінансових коштів; формування кадрових і організаційних засобів; розробка системи правових засобів; залучення технічних, інформаційних та інтелектуальних засобів.

Переведені зі статичного в динамічний стан вищевказані засоби перетворюються в методи забезпечення економічної безпеки підприємства. Відповідно, можна виділити технічні, інформаційні, фінансові, правові, інтелектуальні методи. Наведемо стислий перелік цих методів:

– технічні (спостереження, контроль, ідентифікація);

– інформаційні (складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо);

– фінансові (матеріальне стимулювання працівників, що мають досягнення в забезпеченні економічної безпеки підприємства);

– правові (судовий захист законних прав і інтересів, сприяння діям правоохоронних органів);

– кадрові (підбір, навчання кадрів, що забезпечують безпеку підприємства);

– інтелектуальні (патентування, ноу-хау тощо).

Під інформаційною безпекою треба розуміти і такий стан соціально-технічної системи підприємства, який дає змогу уникнути зовнішніх загроз і протистояти внутрішнім чинникам дезорганізації за допомогою наявних ресурсів, підприємницьких здібностей менеджерів, а також структурної організації [1, с. 37].

Головна мета управління інформаційною безпекою – забезпечення найефективнішого функціонування, найпродуктивнішої роботи операційної системи та економічного використання ресурсів, забезпечення певного рівня трудового життя персоналу та якості господарських процесів підприємства, а також постійного стимулювати нарощування наявного потенціалу та його стабільного розвитку [4, с. 67].

На основі аналізу накопиченого емпіричного матеріалу можна здійснити узагальнення на рівні теоретичних засад організації інформаційної безпеки як функції.

Організацію безпеки умовно поділено на три рівня. В основу поділу покладено такий метод, як зрізи середовища, в якому знаходиться інформація: 1) соціальне (окрема людина, спільноти людей, держава, міжнародне співтовариство); 2) інженерно-технічно-логічне (машинне, апаратно-програмне, автоматичне); 3) соціотехнічне (людино-машинне).

Кожен зазначений рівень щодо середовища об'єктивно доповнює і взаємообумовлює інші рівні, утворюючи в основі триєдину гіперсистему – організацію інформаційної безпеки конкретного суб'єкта суспільних відносин.

Важливим елементом організації інформаційної безпеки є поділ заходів на групи. У теорії та практиці виділяють такі три групи: активні засоби

захисту (розвідка, дезінформація тощо); пасивні засоби (встановлення екранів проти несанкціонованого витоку інформації тощо); комплекс засобів підтримки – органічне поєднання попередньо вказаних груп щодо моделювання потенційних (невідомих раніше практиці) загроз.

Інформаційна безпека в сучасному світі, в якому основним товаром є інформація, в якому саме та чи інша інформація впливає на прийняття державою тактичних та стратегічних рішень, є основою національної безпеки. Для України, яка прагне до Європейського Співтовариства, особливо важливим є приведення чинного законодавства до європейських стандартів, що передбачає прийняття нових законів, удосконалення та доопрацювання чинних. Існує також необхідність у створенні координаційної комісії з питань нормативно-правового забезпечення інформаційної безпеки України, яка б стала акумулятором пропозицій різних органів державної влади та громадських організацій у справі вироблення інформаційної політики для України. Варто наголосити, що Україна потребує закону «Про інформаційну безпеку», який би врегульовував суспільні відносини у сфері інформаційної безпеки, враховуючи те, що інформація організовується спонтанно, не через упорядкування з боку держави, те, що обмеження на поширення інформації, навіть для забезпечення національної безпеки, зумовлює сповільнення розвитку суспільства. Цей закон мав би давати визначення методів та засобів захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері, окреслив би засади для формування державної політики інформаційної безпеки, розвитку інформаційного простору країни.

Висновки з проведеного дослідження. Інформаційна безпека – це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємств. Підтримка інформаційної безпеки – це комплекс організаційних, правових та інженерно-технологічних заходів щодо збереження, охорони та захисту життєво важливих інтересів суб'єктів інформаційної діяльності. Особливість безпеки інформаційної діяльності полягає у запобіганні, протидії та подоланні природних, техногенних і соціогенних загроз, здатних порушити життєдіяльність конкретного суб'єкта (людини, суспільства, держави, світового співтовариства), у тому числі підприємництва.

Поняття та сутність інформаційної безпеки в умовах інформатизації України як соціального явища можна визначити так: інформаційна безпека в умовах інформатизації України – це суспільні відносини щодо створення та підтримання на належному рівні функціонування відповідної автоматизованої інформаційної системи (у тому числі систем телекомунікації); комплекс організаційних, правових та інженерно-технологічних заходів щодо підтримки (охорони, захисту зберігання), запобігання та подолання природних, техногенних і соціогенних загроз, здатних порушити життєдіяльність конкретної соціотехнічної інформаційної системи.

Відповідно, зазначені формулювання можуть адаптуватися до конкретної (спеціальної) сфери суспільних відносин, у тому числі підприємницької діяльності.

Рис. 2. Організація управління інформаційною безпекою підприємства

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Братель О. Поняття та зміст доктрини інформаційної безпеки / О. Братель // Право України. – 2006. – № 5. – С. 36–40.

2. Остроухов В. До проблеми забезпечення інформаційної безпеки України / В. Остроухов // Політичний менеджмент. – 2008. – № 4. – С. 135–141.

3. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства / В. Цимбалюк // Підприємництво, господарство і право. – 2008. – № 3. – С. 88–91.

4. Чубарук Т. Проблеми законодавчого забезпечення інформаційної безпеки в Україні / Т. Чубарук // Право України. – 2007 . – № 9. – С. 67–69.

5. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки. – 2009. – № 10. – С. 220–225.