К., 2003. 14. Комісарчук Ю.А. Організована злочинність у ринкових умовах// http//www.naiau.kiev.ua/visnik/n2000–4.

Надійшла до редколегії 15.01.04

М.В. Куркін

ДЕЯКІ ПОНЯТТЯ КАТЕГОРІАЛЬНОГО БАЗИСУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із основних завдань, що мають найважливіше значення для підприємств, котрі функціонують у сучасних умовах перебудови економіки України на ринкові відносини, є завдання забезпечення їх економічної безпеки. Інформатизація суспільства, глобалізація економічних відносин, розширення сфер взаємодії суб'єктів цих відносин, включаючи інформаційно-комунікаційні, – усі ці чинники визначають основні напрямки наукових досліджень, пов'язаних з економічною безпекою, зокрема, її інформаційним аспектом. Питання забезпечення інформаційної безпеки є актуальними для всіх груп суб'єктів, що господарюють на ринку, і пов'язані з проблемами збереження державної та комерційної таємниці, інформації фінансово-кредитних установ, що становить інтерес для конкуруючих ринкових суб'єктів, і вимагає свого вирішення на різних рівнях інституціональної побудови суспільства.

У зв'язку з цим важливого значення набувають методичні питання, пов'язані з визначенням понять, котрі відносяться до категоріального базису інформаційної безпеки. Метою даної роботи є визначення й уточнення деяких понять інформаційної безпеки. Саме вони дозволять сформулювати сутність і формалізувати такі проблеми, як безпека інформаційної системи, економічного об'єкта, персоналу підприємства.

Розглянемо наступні аспекти, що визначають проблему забезпечення інформаційної безпеки.

1. Політика забезпечення інформаційної безпеки суспільства і його інститутів є однієї з чільних державних політик. У першу чергу, вона спрямована на забезпечення безпеки інформації в урядових, військових установах і відомствах, в яких інформація містить державну та військову таємницю (із різними грифами таємності), а також у фінансово-кредитних установах і суб'єктах господарської діяльності, які активно працюють у сфері розробки і реалізації стратегічно важливих інноваційних напрямків. Іншим, не менш важливим напрямком, є забезпечення безпеки інформації на підприємствах, що активно виходять на ринок, досить стабільно функціонують на ньому й у відношенні яких можуть порушуватися різні зобов'язання по збереженню їхніх комерційних таємниць (впровадження інновацій, нових технологій, виробничих процесів) [1].

Таким чином, можна зробити висновок про те, що існує три основних компоненти ринкових контрагентів, для яких забезпечення інформаційної безпеки має різне значення і зміст.

Теоретичне і практичне використання цього положення приводить до формулювання наступної базової передумови – визначення інваріантних

стосовно зазначених об'єктів понять «інформація», «безпека» і «інформаційна інфраструктура».

Стосовно поняття «інформація» пропонується в якості такої детермінанти визначити властивості інформації, до яких варто віднести: адекватність, вірогідність, повноту, оперативність, цінність, точність і корисність.

Аналіз сучасних підходів до оцінки таких властивостей, як цінність і важливість інформації, показує, що для об'єктів, які належать до вище описаних груп, ці поняття, а точніше їхня пріоритетність, відрізняються. Так, наприклад, для електронного платіжного документа важливим є забезпечення цілісності, коректності інформації, у порівнянні з її важливістю і цінністю, що визначає легітимність інформації для прийняття різних управлінських рішень [2]. Крім цього, необхідно відзначити, що самий тип документа, що циркулює в стандартизованих схемах документообігу на різних підприємствах, визначає деяку сукупну характеристику (параметр) властивостей інформації. Як приклад, можна навести документи урядових і стратегічно важливих державних об'єктів, у відношенні яких можна зробити висновок, що будь-яке порушення їхніх властивостей, як інформаційного продукту, може привести до важких, а найчастіше непередбачуваних наслідків. Урахування самого характеру інформації приводить до необхідності класифікації (концепцій) у відношенні економічних об'єктів та їхньої інформаційної захищеності і безпеки [3].

У зв'язку з цим визначимо перший аспект, котрий представляє теоретичний напрямок у сфері інформаційної безпеки, що характеризується складом і функціями інститутів суспільства, і назвемо його категоріальним.

2. Розвиток і глобалізація світових суспільних і економічних процесів приводять до того, що поняття «відкритість суспільства» вимагає розвитку супутніх цим процесам явищ – різкого підвищення інтенсивності інформаційно-комунікаційних процесів. Вони, у свою чергу, супроводжуються впровадженням і широким використанням інформаційних технологій, що прискорюють ці процеси і роблять їх доступними для їхніх учасників [4]. Водночас, відкритість суспільства, залучення в глобальні процеси великої кількості людей, ресурсів, цілих країн супроводжується низкою негативних явищ, що безпосередньо пов'язані з інформацією, інформаційними продуктами й інформаційними послугами.

До них варто віднести:

– численні порушення у фінансово-кредитній сфері (шахрайство, обман, неправомірні дії з документацією у сфері електронного документообігу) [5];

– несанкціонований доступ до конфіденційної інформації;

– неправомірні зміни, модифікації, що спотворюють зміст інформації, внаслідок чого вона втрачає свою юридичну значимість;

– численні явища, що призводять до негативних результатів у масштабах країни, які в даний час об'єднуються під загальною назвою «інформаційна війна» [6].

У зв'язку з цим, світовим співтовариством було поставлене завдання розробки універсальних стандартів стосовно забезпечення безпеки інфор-

маційних технологій, до яких відносяться «Загальні критерії оцінки безпеки інформаційних технологій». Вони задовольняють потреби всіх учасників інформаційних процесів: споживача інформації, оцінювача захищеності інформаційного об'єкта і розроблювача оцінки захищеності інформаційного об'єкта. Принципово важливим елементом, що вводиться в систему інформаційної безпеки, є профіль захисту. Він являє собою сукупність типових вимог безпеки до визначеного класу об'єктів, для котрих необхідно зробити оцінку необхідного рівня інформаційної безпеки.

Цей аспект, що представляє прикладний напрямок у сфері інформаційної безпеки, котрий характеризується складом і функціями об'єктів інформаційної безпеки, назвемо нормативним.

3. Наступний аспект інформаційної безпеки визначимо як здатність підприємницької структури самій визначати свій рівень інформаційної захищеності. Її змістовний сенс зводиться до того, що самий суб'єкт господарської діяльності формулює, реґламентує, реалізує рішення наступних завдань із забезпечення інформаційної безпеки:

– визначення найімовірніших погроз для суб'єкта, що господарює;

– визначення найуразливіших місць в інформаційній системі суб'єкта;

– оцінку можливого збитку;

– оцінку ризиків, пов'язаних з імовірністю виникнення й імовірністю реалізації погроз;

– розробку заходів щодо запобігання і пом'якшення наслідків у виді збитку, котрий завдається у сфері інформаційної інфраструктури суб'єкта, його інформаційній системі.

Цей аспект, який представляє прикладний напрямок у сфері інформаційної безпеки, що характеризується індивідуальним вибором безлічі погроз, оцінки ризиків і обробки наслідків, назвемо евристичним.

Таким чином, дослідження й аналіз існуючих підходів і концепцій до визначення інформаційної безпеки дозволили виділити теоретичний і прикладний напрямки у сфері забезпечення інформаційної безпеки. Евристичний підхід характеризується врахуванням індивідуальних особливостей ринкового агента в процесах його взаємодії з елементами ринкового середовища, таких як: рівень конкурентноздатності виробленої продукції; рівень і ступінь впровадження інноваційних розробок; розмір ніші, що займається на ринку; характер корпоративних відносин, в яких він бере участь; робота з контрагентами на основі використання Internet-технологій; обсяг угод, що укладаються із використанням засобів електронної комерції стосовно загального обсягу угод; обсяг реалізованої продукції E-commerce.

Структурний аналіз поняття «інформаційна безпека» проведемо на основі аналізу понять «безпека» і «інформація».

Виділимо такі аспекти, в яких вони диференціюються:

– психологічний: відчуття, переживання, потреба в захисті життєво важливих потреб та інтересів людей;

– філософський: стан, тенденції розвитку, умови життєдіяльності соціуму, його структур та інститутів, при яких забезпечується їхня якісна визначеність;

– юридичний: система встановлених законами гарантій захищеності особистості і суспільства, що забезпечує нормальну життєдіяльність, права і свободу.

Визначимо наступні детермінанти розглянутих аспектів: система, захищеність індивіда і суспільства, інтереси і потреба, здатність підтримувати нормальну, життєво необхідну діяльність, можливість розвивати цю здатність у процесі розвитку й удосконалювання структур та інститутів суспільства.

З іншого боку, «безпека» визначається як відсутність небезпеки, або стан, при якому існує захист від небезпеки і результатом дії якої є неможливість нанесення збитку об'єкту загрози. І, нарешті, «безпека» визначається як «відбивання» загроз та існуючих небезпек або ж їхня відсутність. Дане визначення вказує на той факт, що повинні існувати засоби, котрі прогнозують і запобігають потенційним загрозам і небезпекам, які наносять збиток особі або суспільству.

Узагальнюючи результати аналізу, одержимо наступну структуру поняття «безпека» (Рис. 1).

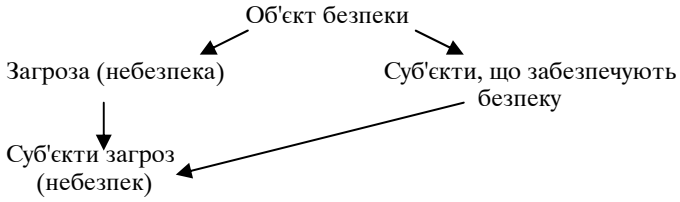


Рис. 1. Структура поняття «безпека»

Змістовий склад приведеної на рис. 1 структури дозволяє виявити наступну характеристику, що раніше не відзначалася авторами при визначенні поняття «безпека», а саме, – наявність зв'язку «суб'єкти загроз – суб'єкти забезпечення безпеки». На практиці вона визначає необхідність превентивних цілеспрямованих дій (заходів) із боку суб'єктів, що забезпечують безпеку, стосовно суб'єктів загроз (небезпек). Методологічний висновок стосовно введення цього зв'язку зводиться до необхідності розробки схем взаємодії, що дозволяють зменшувати рівень загроз за рахунок навмисного впливу на можливих суб'єктів загроз (створювати контр загрози).

Перейдемо до поняття «інформація» як об'єкта впливу загроз, що визначають характер внутрішніх і зовнішніх взаємодій об'єкта. Аналіз показав, що під інформацією варто розуміти деякий «інформаційний вимір», що характеризує особистість, індивіда, соціум, суспільство, націю, культуру.

Інша інтерпретація, корені якої лежать в основі соціальних і технічних систем, характеризується як інформаційне поле, в якому функціонують вище визначені суб'єкти. Це поле має свої характеристики і параметри, що можуть бути змінені і модифіковані відповідно до механізмів, що визначаються взаємодією суб'єктів і об'єктів загроз і суб'єктів загроз і суб'єктів забезпечення безпеки. Такий підхід дозволяє включити в розгляд нові ідеї, відповідно до котрих усталеність інформаційного поля економічного об'єкта характеризується усталеністю області, що містить у собі локальне поле взаємодії зазначених суб'єктів (мал. 2), а саме, рівновагою сил взаємного впливу полів 1 і 2, в якості яких виступають інформаційне поле загроз (суб'єктів погроз) і інформаційне поле суб'єкта, що забезпечує безпеку, відповідно.

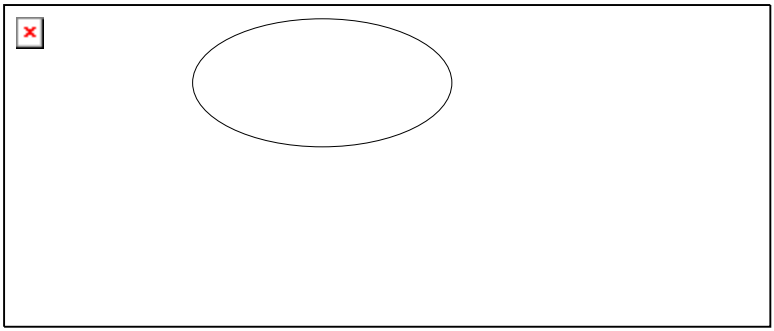
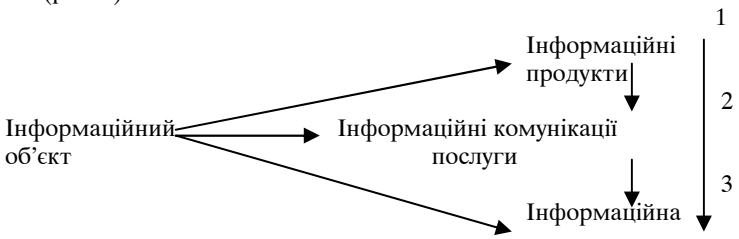


Рис. 2. Схема взаємодії інформаційних полів загроз, суб'єктів, що забезпечують безпеку інформаційних об'єктів

Ця схема включає прямий вплив засобів, що забезпечують захист, на ті засоби, за допомогою котрих «проектуються» і реалізуються потенційні загрози і небезпеки.

Введемо поняття «інформаційний об'єкт» як об'єкт, характер функціонування якого визначається інформаційними властивостями об'єкта, інформаційним продуктом, що є результатом діяльності індивіда, суспільства, соціуму, складом і характером інформаційних послуг та інформаційної інфраструктури, що підтримує ці об'єкти.

Таким чином, одержимо наступну структуру поняття «інформаційний об'єкт» (рис. 3).



інфраструктура

Рис. 3. Структура поняття «інформаційний об'єкт»

Інформаційна структура, у свою чергу, містить у собі засоби забезпечення виробництва і реалізації інформаційних продуктів і інформаційних послуг індивідом і суспільством у цілому, а також їхнього ефективного функціонування в процесах виробництва, відтворення і комунікацій (передачі).

Використання розглянутих підходів до визначення понять дозволяє одержати наступну структуру поняття «інформаційна безпека» (рис. 4).

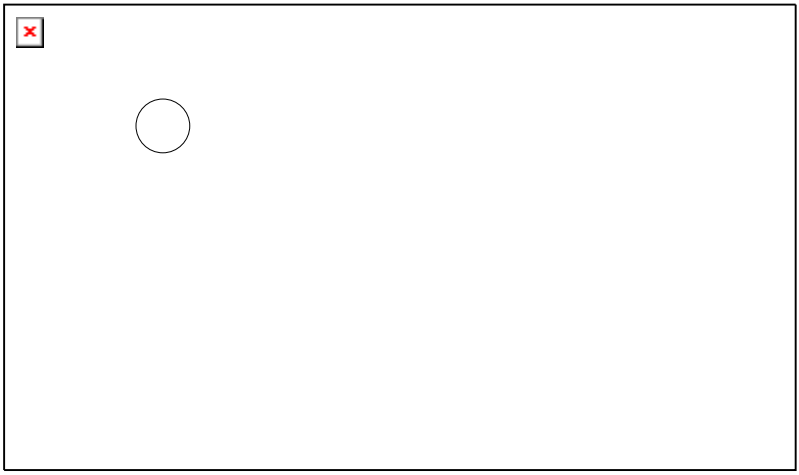


Рис. 4. Структура поняття «інформаційна безпека»

На мал. 4 показано, що суб'єкти, які забезпечують інформаційну безпеку, повинні прогнозувати і реалізовувати заходи щодо забезпечення безпеки в двох напрямках: стосовно інформаційних об'єктів, що піддаються загрозам, і стосовно суб'єктів, що самі є джерелами загроз або мають потенціал створення загрози (небезпеки).

Суб'єкти – джерела погроз можуть опосередковано впливати на інформаційні об'єкти винятково за рахунок факту своєї наявності («загроза сильніше нападу»). Самі ж загрози безпосередньо (прямо) впливають на інформаційні об'єкти і створюють тим самим небезпеку одержання збитку, що може бути оцінене із використанням теорії ризиків. Імовірність виникнення і реалізації загрози створює передумови розрахунку можливих ризиків при нанесенні збитку і розміри самого збитку.

Таким чином, запропоновані структури понять «інформаційний об'єкт», «безпека», «інформаційна безпека», що визначають категорії економічної безпеки, дозволяють відбити нові підходи до рішення проблем забезпечен-

ня інформаційної безпеки економічних об'єктів, а саме, підвищення усталеності інформаційних систем підприємств на основі забезпечення усталеності процесів взаємодії інформаційних полів суб'єктів загроз і інформаційних інфраструктур економічних об'єктів, нейтралізація впливу суб'єктів загроз або зниження їхнього рівня в результаті навмисних превентивних дій тощо.

Подальший розвиток понятійного апарату пов'язаний з уточненням таких понять як «інформаційна війна», «інформаційна зброя», а також розробкою стратегії і механізмів протидії їм на його основі.

Список літератури: 1. Петренко С.А., Возможная методика построения системи информационной безопасности предприятия // Прогноз финансовых рисков/ www.bre.ru. 2. Лазарєва С.Ф. Економіка та організація інформаційного бізнесу. К., 2002. 3. Петренко С.А., Попов Ю.И. Оценка затрат на информационную безопасность. S.petrenko@confident.spb.ru. 4. Алексеева И.Ю., Авчаров И.В., Вотрин Д.С., Стрельцов А.А. и др. Информационные вызовы национальной и международной безопасности/ Под общ. ред. А.В. Федорова и В.Н. Цыгичко. М., 2001. 5. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів // Український центр інформаційної безпеки / www.bezpeka.com/library/lib_aspect.html. 6. Почепцов Г.Г. Информационные войны. М., 2000.

Надійшла до редколегії 12.02.04

О.О. Теличкін

Суб'єкти правоохоронної діяльності міжнародних місій на користь миру

Досвід діяльності з розв'язання конфліктів в Афганістані, Іраку, Палестині свідчить, що підтримання міжнародного миру і безпеки значною мірою залежить від можливостей світової спільноти підтримувати правопорядок у зоні відповідальності міжнародної місії. В операціях на користь миру правоохоронні функції можуть виконувати різноманітні структури: військова поліція збройних сил ООН, інших міжнародних/регіональних організацій, коаліцій держав або окремих держав; цивільна поліція ООН, інших міжнародних/регіональних організацій, коаліцій держав або окремих держав; підрозділи з реформування судових та правоохоронних органів; підрозділи з контролю за дотриманням прав людини; служби безпеки ООН та інших міжнародних/регіональних організацій; підрозділи моніторингу політичного становища; міжнародні судові органи тощо.

У перших, монофункційних операціях із розв'язання інтердержавних конфліктів завдання щодо забезпечення правопорядку в зоні відповідальності місії покладалися на особовий склад збройних сил ООН. Наприклад, під час проведення операції з підтримання миру «Перші надзвичайні збройні сили ООН» з 6073 військовослужбовців, дислокованих у зоні Суецького каналу з метою роз'єднання єгипетських та ізраїльських військ, лише менш ніж 60 % особового складу було задіяно за прямим призначенням, у той час як решта застосовувалася для інших, у тому числі поліцейських, функцій. Зокрема, в завдання військовослужбовців входило затримання осіб, які