УДК 62.50:658.21

І.С. Колесник, А.В. Дудатьєв, О.П. Войтович

Вінницький національний технічний університет, Вінниця

ОЦІНКА ВПЛИВУ ВИТОКУ ІНФОРМАЦІЇ НА СТАН ПІДПРИЄМСТВА

Поставлена і вирішена задача побудови моделі для комплексної оцінки безпеки інформаційної діяльності організацій в умовах глобалізованих «недружніх» ринків, де одним із засобів конкурентної боротьби є несанкціонований доступ до інформаційних систем конкурентів. Проведено дослідження розподілів вірогідності контролю долей ринку.

Ключові слова: *безпека, інформаційна система, захист інформації, інформаційна асиметрія, конкурентне середовище, ринок, несанкціонований доступ, витік інформації.*

Вступ

У постіндустріальному суспільстві матеріальні ресурси поступово втрачають свою вагомість, натомість цінність нематеріальних – інформаційних – ресурсів зростає. Витік закритої інформації може завдати серйозного удару будь-якій організації, її економічному стану. Тому саме сьогодні необхідно приділяти належну увагу проблемам захисту інформації, у тому числі від несанкціонованого доступу, її цілісності та безпеки.

Аналіз публікацій. В сучасних публікаціях виділяється два класи заходів із забезпечення інформаційної безпеки[1]:

– програмно-апаратний: кодування, регламентація доступу, розпізнавання спроб вторгнення і зламу захисту;

– організаційно-правовий: складання списків загроз і ризиків, формування інструкцій і правил, створення надбудов над виробничими підрозділами - підрозділів аналітичного контролю і забезпечення безпеки основних підрозділів підприємства.

Основні положення публікацій другого класу можна узагальнити так [2]:

– для створення ефективної системи комплексної безпеки об'єкту необхідно, щоб система заходів захисту була адекватна всім існуючим для об'єкту загрозам. Вирішити таку складну задачу можна тільки з використанням наукових методів і залученням висококваліфікованих фахівців;

– при підвищених вимогах до інформаційної безпеки для оцінювання захищеності підприємства доцільно використовувати метод детального аналізу ризиків. В цьому випадку необхідно використовувати комплексні показники захищеності.

Постановка задачі. Новизна проблеми безпеки інформаційних систем обумовлює необхідність розробки систем імітаційних моделей для інтенсивного випробування нових методів забезпечення безпеки інформаційних систем підприємств і організацій. Задачу інформаційної безпеки важко виділити з множини задач бізнес-системи, невідомо як структурувати ці задачі.

На сьогоднішній день фактично неможливо встановлювати апріорі структури моделей задач інформаційній безпеки підприємств чи організації. Тому обрано методологію створення систем моделей, суть якої полягає в побудові систем моделей навколо «центрів кристалізації» – теоретично обґрунтованих і практично ефективних моделей [3, 4].

В якості таких напрацьованих моделей вибраний комплекс елементарних моделей [5], моделей на базі методу оптимального агрегування [6] і узагальнених імітаційних моделей розподілених систем класу «N виробників на ринку M продуктів» [7]. Особливість останньої моделі – відтворення поведінки кожного елементу системи виробників певного галузевого сегменту ринку продуктів або послуг. Це дозволяє імітувати ситуації конкуренції (у тому числі недобросовісної) певних вибраних елементів «на фоні» повної системи.

У роботі [8] в першому наближенні промодельовані і проаналізовані ризики ринку для системи в цілому і окремих елементів системи. У результаті можна поставити конкретну задачу – відображення в моделях [7, 8] інформаційних «війн» між певними елементами направлених на витіснення з ринку, або поглинання конкурента.

Мета роботи. На основі вищесказаного метою даної статті є розробка та дослідження моделей для комплексної оцінки безпеки і проведення досліджень:

– модель функціонування системи «N виробників на ринку M продуктів» з урахуванням інформаційних взаємодій, зокрема витоку інформації;

– модель інформаційної взаємодії двох конкурентів при витоку інформації в «недружньому середовищі».

Аналіз моделей для оцінки наслідків витоку і спотворення інформації

Конкуренція вважається необхідною умовою стійкості та розвитку ринкової економіки, постулат якої: на вільному ринку перемагає кращий продукт, за кращим виробником тягнуться інші. Проте це правило не завжди працює, зокрема, через недобросовісну конкуренцію (вторгнення в інформаційні системи конкурента для крадіжки і викривлення інформації, дезінформація про конкурента і його продукцію, підробки під бренд).

Недобросовісна конкуренція зазвичай призводить до таких наслідків:

– зниження ефективності об'єкту, уповільнення зростання, спад виробництва, втрата частки ринку;

– вихід з бізнесу в даному сегменті ринку, банкрутство.

Формалізуємо поняття «безпека підприємства» для задачі даної роботи. Визначимо його через первинні поняття.

Стан підприємства $\mathrm{Sp}^{\langle t\rangle}$ – структура даних (скаляр, вектор, матриця, вектор, складений з матриць тощо), яка характеризує істотні для конкретної задачі аспекти діяльності бізнес-одиниці у момент часу *t*.

Рівень випадкових збурень $\mathrm{W}^{\langle t\rangle}$ – структура даних, що характеризує інтенсивності істотні для конкретної задачі зовнішніх і внутрішніх збурень.

Модель процесу функціонування підприємства

$$\mathrm{Sp}^{\langle t+1\rangle} = \mathrm{Fts}\left(\mathrm{Sp}^{\langle t\rangle}, \mathrm{U}\left(\mathrm{Sp}^{\langle t\rangle}\right), \mathrm{W}^{\langle t\rangle}\right), \qquad (1)$$

де Fts – оператор переходу між станами; $\mathrm{U}\left(\mathrm{Sp}^{\langle t\rangle}\right)$ – оператор управління; $\mathrm{W}^{\langle t\rangle}$ – випадкові збурення.

При використанні звичайних можливостей і технологій програмування завжди можна звести модель будь-якого об'єкту або процесу до форми (1). У [5 – 7] представлені приклади побудови таких моделей, зокрема, в [7] використана модель, зібрана з двох десятків функціональних модулів. Ця модель еквівалентна системі з сотень нелінійних різницевих рівнянь. Після того, як модель великої мережевої системи зібрана, користувач може оперувати з цілісним об'єктом, та одночасно повинен мати можливість контролювати процеси в кожному окремому елементі.

Ризики діяльності підприємства – відповідно до етапів бізнес-циклу можна виділити ризики виробництва, постачання як ринків ресурсів так і продуктів. Припустимо, що як міра ризиків вибрані відхилення певних показників і задані відповідні розподіли ймовірності. Наприклад, найпростіша модель виробництва:

$$\mathrm{Y} = \mathrm{FV}(\mathrm{X}, \mathrm{A}, \mathrm{w}, \mathrm{s}), \qquad (2)$$

де $\mathrm{FV}(\ )$ - функція виробництва, позитивна, неспадна; X, Y – виробничі витрати та випуск продукції; $\mathrm{A}, \mathrm{w}, \mathrm{s}$ – параметри функції виробництва, які мають інтерпретацію "амплітуда", ефективність", "нечутливість" [6].

Параметр *A* - випадкова величина, яка має розподіл $\mathrm{p}(\mathrm{A}) = \mathrm{dp}(\mathrm{A}, \mathrm{Ao}, \sigma)$, звичайно стандартний. Прибуток виробничого елементу дорівнює

$$\mathrm{PR}(\mathrm{X}) = \mathrm{Y} - \mathrm{X} = \mathrm{FV}(\mathrm{X}, \mathrm{A}, \mathrm{w}, \mathrm{s}) - \mathrm{X}. \qquad (3)$$

За допомогою імітаційної моделі можна отримати розподіл ймовірності прибутку, точніше гістограму на даних віртуальній реальності. Так отримано можливість дати кількісну оцінку ризику. Ризик отримання збитків дорівнює:

$$\mathrm{rzb} = \int_{\mathrm{PR}_{\min}}^{0} \mathrm{dpryb}(\mathrm{PR}, \mathrm{Vp})\,\mathrm{dPR}, \qquad (4)$$

де $\mathrm{PR}_{\min}$ – мінімальний прибуток (максимальний збиток); $\mathrm{V_p}$ – вектор параметрів, який задається користувачем-аналітиком.

Безпека підприємства. На базі виконаної формалізації (2) – (4) можна конструктивно визначати показники безпеки підприємства. Сформуємо ці показники як **функції впливу певних інформаційних дій,** як випадкових (стихійних) так і цілеспрямованих ворожих.

Опишемо **формальну процедуру аналізу безпеки підприємства** щодо несанкціонованого доступу до його інформаційних ресурсів.

Множина ситуацій витоку та викривлення інформації може бути впорядкованою з безперервною шкалою рівнів, дискретною впорядкованою та неврегульованою. В рамках даної роботи розглянуто два граничні випадки.

1). Функції впливу для випадку неперервної шкали інформаційних втрат.

$$\mathrm{dpryb}\left(\mathrm{dIef}, \mathrm{Sp}^{\langle t\rangle}, \mathrm{Szo}^{\langle t\rangle}\right),, \ \mathrm{rzb}\left(\mathrm{dIef}, \mathrm{Sp}^{\langle t\rangle}, \mathrm{Szo}^{\langle t\rangle}\right), \qquad (5)$$

де dIef – падіння ефективності інформаційної системи підприємства $0 \le \mathrm{dIef} \le 1$; $\mathrm{Sp}^{\langle t\rangle}$, $\mathrm{Szo}^{\langle t\rangle}$ – стан підприємства і стан зовнішнього оточення (ціни, стани ринків тощо).

Функції (5) фактично є програмними модулями, функція $\mathrm{dpryb}(\ )$ бере відповідні параметри і повертає щільність розподілу ймовірності можливих значень прибутку, функція $\mathrm{rzb}(\ )$ бере ті ж параметри, а повертає вірогідність збитків. Ці функції зв'язані через (4).

2). Функції впливу для випадку для невпорядкованої множини ситуацій інформаційних втрат.

$$rzb\left(Zj, Sp^{\langle t\rangle}, Szo^{\langle t\rangle}\right), \quad rzb0\left(Zj, Sp^{\langle t\rangle}, Szo^{\langle t\rangle}\right), \quad (6)$$

де Zj – загроза витоку і використання інформації конкурентами, елемент відповідної множини загроз j = 1 .. Nz.

Введені моделі оцінки ризиків та безпеки підприємства при порушеннях інформаційної безпеки дозволяють отримати задовільні оцінки втрат, за наявності моделі функціонування підприємства (це може бути банк, гіпермаркет, комп'ютерна сервісна система, електронний магазин, рейтингове агентство тощо). Тепер можна замкнути систему моделей. Для цього слід побудувати модель функціонування автоматизованої інформаційно-управлінської системи підприємства у формі (1).

Наявність узагальненої моделі інформаційно-обчислювальної системи, як багатофазної, багатоканальної, багатопріоритетної системи дозволяє отримати кількісні оцінки ефекту і витрат на підвищення надійності та захищеності від загроз і атак інформаційно-управлінської системи, тобто отримати функцію ефективності витрат на її захист.

Логіка процесу оцінки безпеки та управління її рівнем на базі моделювання буде такою:

– визначення зменшення ефективності інформаційно-управлінської системи і втрат прибутку залежно від наслідків несанкціонованого доступу до неї;

– визначення витрат на захист і підвищення рівня ефективності інформаційно-управлінської системи;

– побудова функцій «витрати на безпеку – зменшення втрат».

Аналіз наслідків витоку інформації підприємства до конкурентів. Система імітаційних моделей для моделювання систем класу «N виробників на ринку M продуктів» [7, 8] (26 виробників, 20 продуктів) дозволяє формувати певні сценарії взаємодії елементів системи, у тому числі і ситуації несанкціонованого доступу до інформаційної системи конкурента. Елементи системи застосовують різні правила прийняття рішень. Нові правила прийняття рішень дають велику конкурентну перевагу, поки вони не стануть загальновідомими.

На рис. 1 і 2 подані приклади аналізу наслідків витоку інформації для процесів і частотних розподілів змодельовані в пакеті програм MathCAD на основі моделей описаних в [7,8].

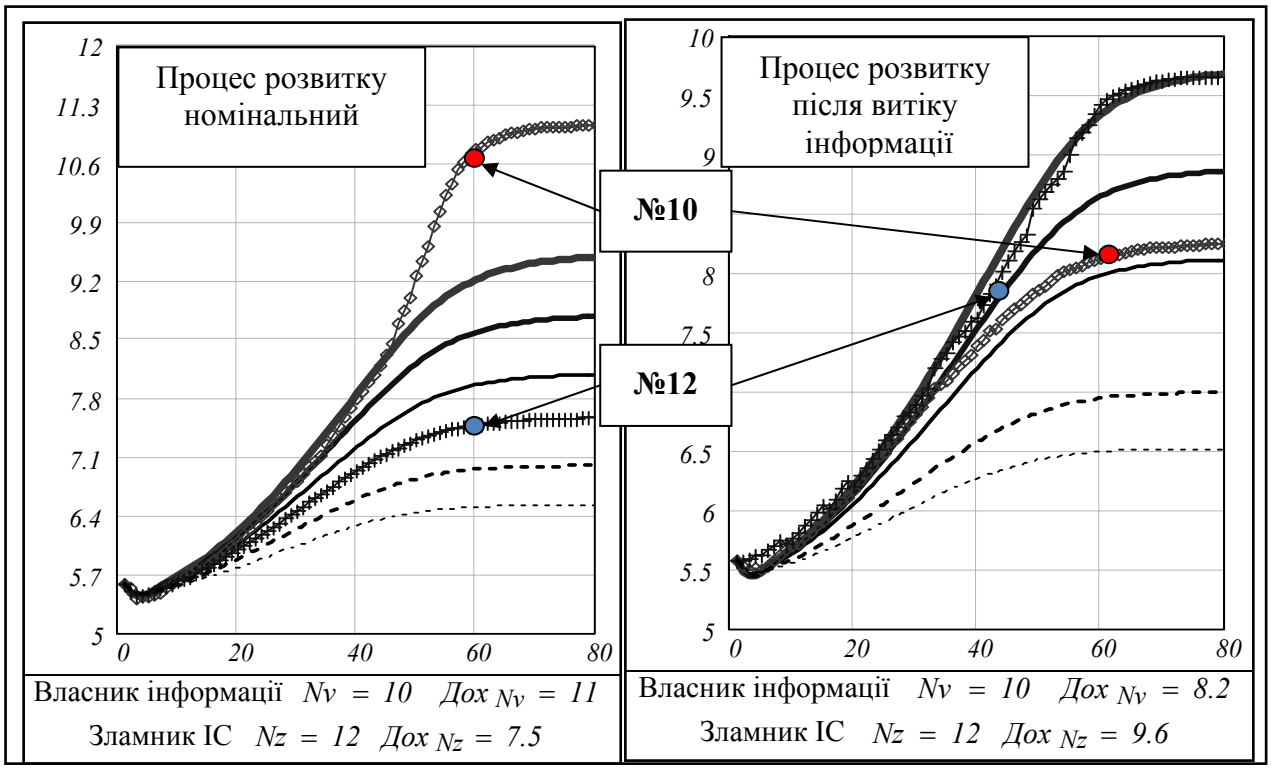

Рис. 1. Аналіз наслідків використання конкурентами інформації

На рис. 1 подані (вибірково) процеси перерозподілу нового сегменту ринку. Виробник №10 – середній за рейтингом продуктивності, в середньому стає лідером ринку (рис. 1, ліворуч) за рахунок ефективного управління. Найближчий конкурент – виробник №12, отримує несанкціонований доступ до інформаційних ресурсів і використовує їх з власною метою. В результаті він стає лідером ринку за темпами №10 – лише четвертий, з падінням прибутку на 30%.

Значна частина успіхів китайського бізнесу обумовлена саме збором незахищеної інформації по всьому світу.

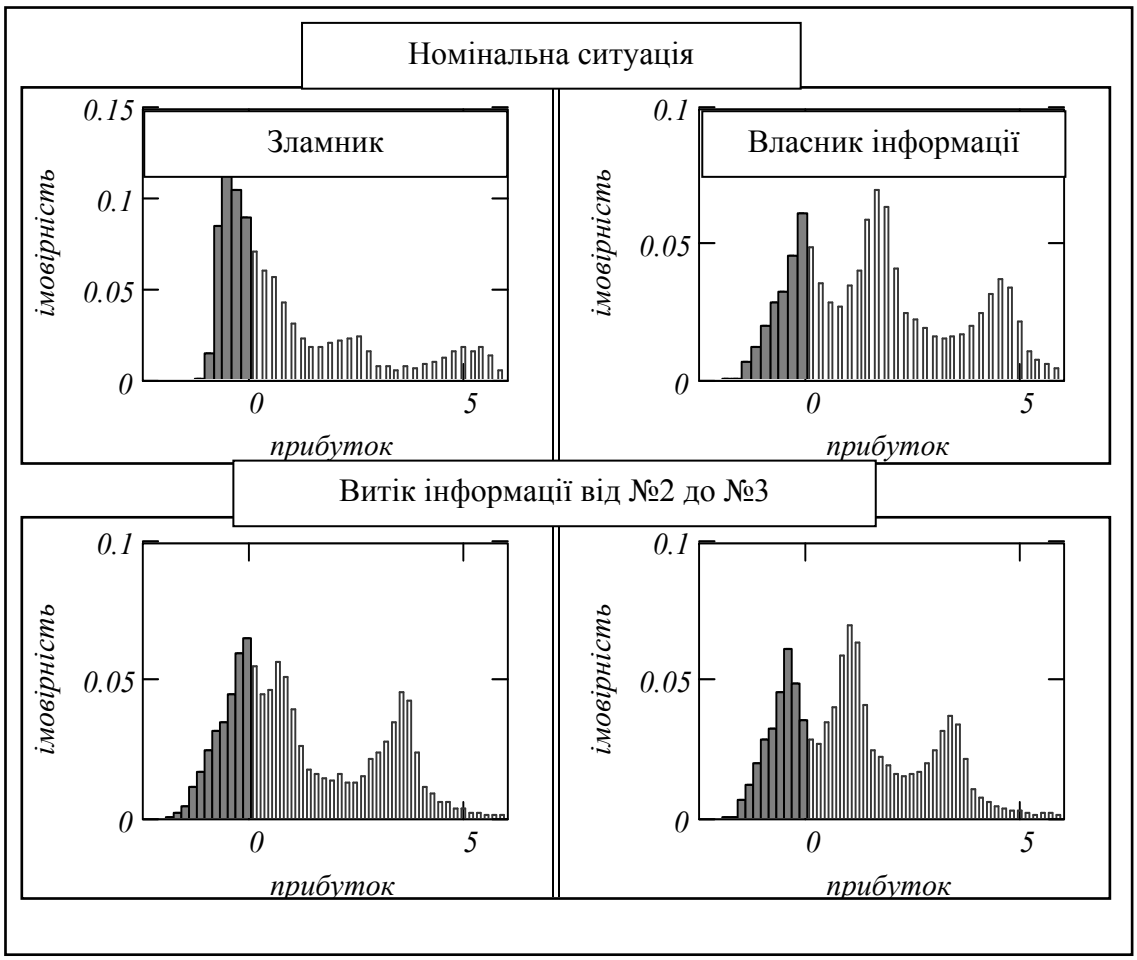

Рис. 2. Аналіз наслідків використання конкурентами інформації. Частотні розподіли

На рис. 2. подано два набори частотних розподілів прибутку для двох конкурентів для тієї ж інформаційної ситуації. З рисунку видно, що при витоку інформації прибутки зламника зростають, а власника інформації зменшуються.

З проведеного моделювання можна зробити висновок, що в певних ситуаціях навіть малі збурення можуть спричинити істотну втрату позицій підприємства (прибуток, частка ринку). Для таких ситуацій в першу чергу повинні прийматися адекватні заходи із захисту інформації.

Аналіз наслідків витоку інформації на ринку з інформаційною асиметрією. В даному випадку термін «інформаційна асиметрія» означає, що інформація продавця (виробника) і покупця (споживача, клієнта) не є ідентичною. Розглядаємо певний сегмент ринку, на якому присутні два виробники, – якісного продукту і неякісного, але з меншою собівартістю. Вважаємо, що продукт (або споживач) є новим, і споживачі спочатку не віддають переваги якомусь продукту. Модель такої системи побудована, вона виявилася нетривіальною. Зокрема в ній важко відобразити ситуації банкрутства, поглинання, санації підприємства внаслідок витоку, втрати, викривлення інформації. На рис. 3. показано приклад процесу перерозподілу ринку: спочатку виробник неякісного продукту витісняє виробника якісного продукту, потім споживачі навчаються розрізняти продукти різних виробників, і виробник неякісного продукту покидає ринок.

У такій системі для виробника якісного продукту існує ситуація загрози безпеці підприємства, істотно залежна від інформованості, щодо наявних ресурсів у конкурента. На рис. 4 подано дві ситуації процесу розподілу ринку: номінальну і **при витоку інформації, щодо фінансового стану підприємства**.

У певний момент ресурс (капітал) виробника якісного продукту досягає мінімуму (стрілка). Якщо це стане відомо конкурентові, він може вдвічі (змінна gaz) збільшити витрати на рекламу і просування свого продукту, істотно зменшити свої прибутки, але довести конкурента до банкрутства і залишитися монополістом ринку.

Таким чином, аналізуючи модель можна визначити критичну для безпеки підприємства ситуацію, яка вимагає радикальних заходів щодо захисту інформації. Отже, навіть спрощена модель ринку з інформаційною асиметрією дозволяє виявляти небезпечні для підприємства і його інформаційної системи ситуації.

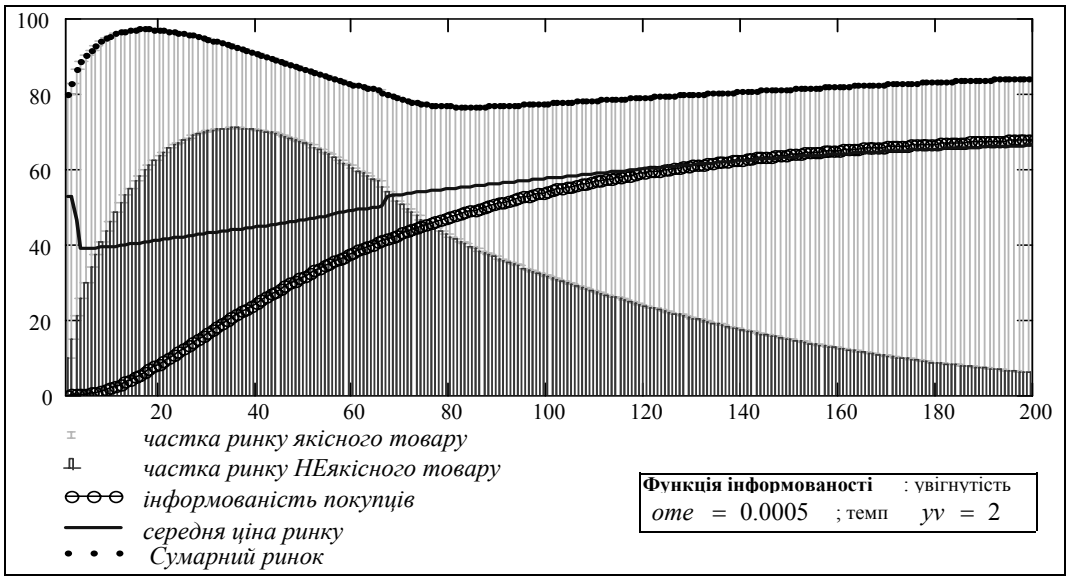

Рис. 3. Процеси перерозподілу ринку
з інформаційною асиметрією

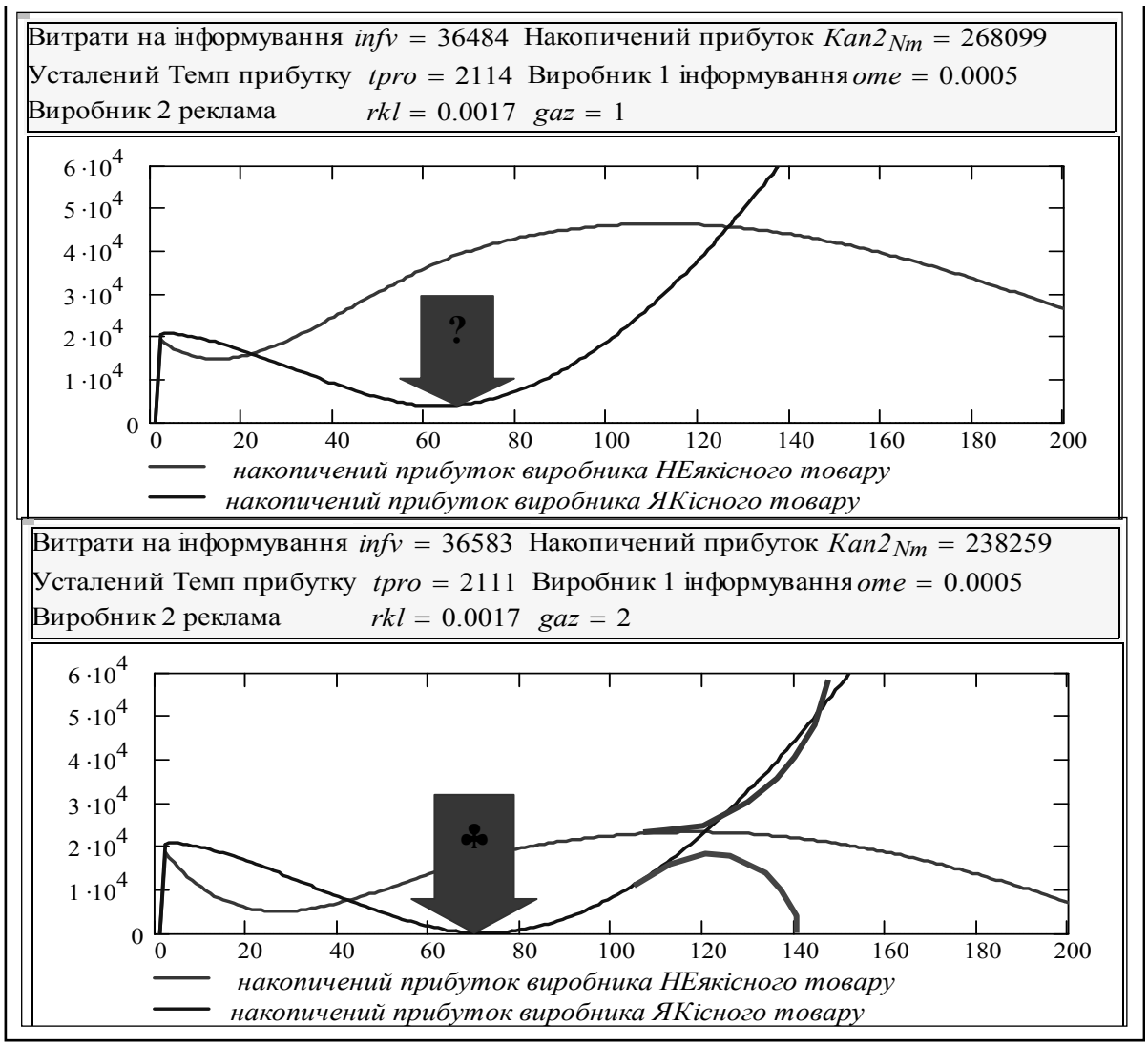

Рис. 4. Аналіз наслідків витоку і використання конкурентами інформації
на ринку з інформаційною асиметрією

Об'єм статті не дозволяє розглянути ситуацію з позицій виробника якісного продукту – за наявності дійсно продукту з високим показником «цінність/ціна» існують радикальні і легальні інформаційні стратегії збереження і розширення частки ринку.

Висновки

Розглянуті задачі інформаційної безпеки бізнес-систем і бізнес-одиниць. Запропонований підхід на базі раціональних технологій побудови імітаційних моделей складних розподілених систем.

Для аналізу безпеки використовувалися імітаційні моделі двох рівнів:

– модель функціонування системи в цілому – джерело задач для підсистеми безпеки і функцій «інформаційні втрати – втрати системи в цілому», яка показала, що навіть незначні збурення в системі (витік інформації про особливості управління на підприємстві) може призвести до значних втрат на ринку;

– модель функціонування інформаційно-обчислювальної системи – засіб для випробування методів захисту інформації та джерело для побудови функцій «витрати на захист інформації – рівень захисту інформації», яка дозволила зробити висновок про небезпечні ситуації, що можуть виникнути при асиметричному ринку.

Запропонована система конструктивних визначень понять для задачі інформаційної безпеки. В подальшому планується дослідити й інші ситуації, що виникають у конкурентному середовищі.

Список літератури

1. Лужецький В.А. Інформаційна безпека / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.

2. Дудатьєв А.В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А.В. Дудатьєв // Вісник Черкаського державного технологічного університету. – 2008. – № 1. – С. 3-8.

3. Аакер Д.А. Бизнес-стратегия: от изучения рыночной среды до выработки беспроигрышных решений / Д.А. Аакер. – М.: Эксмо, 2007. – 464 с.

4. Райс Э. Маркетинговые войны / Э. Райс, Дж. Траут. – СПб.: Питер, 2000. – 256 с.

5. Боровська Т.М. Основи теорії управління та дослідження операцій. Навчальний посібник / Т.М. Боровська, І.С. Колесник, В.А. Северілов. – Вінниця: УНІВЕРСУМ-Вінниця, 2008. – 242 с.

6. Боровська Т.М. Оптимізація розподілу обмеженого ресурсу у виробничій системі на базі агрегування виробничих функцій / Т.М. Боровська, І.С. Колесник, В.А. Северілов // Інформаційні технології та комп'ютерна інженерія. – 2005. – № 1. – С. 12-18.

7. Боровська Т.М. Моделювання розвитку підприємства "на фоні" підприємств і споживачів сегменту ринку. / Т.М. Боровська, І.С. Колесник, В.А. Северілов // Вісник ВПІ. – 2009. – № 1. – С. 28-36.

8. Колесник І.С. Розробка імітаційних моделей для оцінки ризиків ринку./ І.С. Колесник, П.В. Северілов, В.А. Северілов // Економічна безпека сучасного підприємства: матеріали V Міжн. НПК. – Вінниця: УНІВЕРСУМ-Вінниця, 2008 – С. 66-71

Надійшла до редколегії 5.05.2010

Рецензент: д-р тезн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ОЦЕНКА ВЛИЯНИЯ УТЕЧКИ ИНФОРМАЦИИ НА СОСТОЯНИЕ ПРЕДПРИЯТИЯ

И.С. Колесник, А.В. Дудатьев, О.П. Войтович

Поставлена и решена задача построения модели для комплексной оценки безопасности информационной деятельности организаций в условиях глобализированных «недружественных» рынков, где одним из средств конкурентной борьбы является несанкционированный доступ к информационным системам конкурентов. Проведены исследования распределений вероятности контроля долей рынка.

Ключевые слова: *безопасность, информационная система, защита информации, информационная асимметрия, конкурентная среда, рынок, несанкционированный доступ, вытек информации.*

ASSESSING THE IMPACT OF INFORMATION LEAKAGE ON THE ENTERPRISE STATE

I.S. Kolesnik, A.V. Dudatyev, O.П. Войтович

The problem of models designing for integrated assessment data activities of enterprises security organizations in terms of globalized "nonfriendly" markets, where one of the funds is a competitive struggle unauthorized access to informational systems competitors is set and solved. The distribution of probability of market shares control is researched.

Keywords: *safety, informative system, defence of information, informative asymmetry, competition environment, market, unauthorized division, escaped information.*