1. Методы организации адаптивного планирования и управления в экономико-производственных системах / В.И. Скурихин, В.А. Забродский, П.А. Иващенко, О.Г. Штрассер. – К.: Наук. думка, 1980. – 272 с. 2. Романов А.Н. Советующие информационные системы в экономике / А.Н. Романов, Б.Е. Одинцов.– М.: ЮНИТИ-ДАНА, 2000.– 487 с. 3. Симанков В.С. Синтез адаптивных АСУ сложными системами с применением моделей распознавания образов / В.С. Симанков, Е.В. Луценко // Автоматизация и современные технологии. – 1999. – № 1. – С. 2–37. 4. Козаченко А.В. Экономическая безопасность предприятия: сущность и механизм обеспечения: монография / А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. – К.: Либра, 2003. – 280 с. 5. Адаптивные модели в системах принятия решений: монография / под ред. Н.А. Кизима, Т.С. Клебановой. – Х.: ИД "Инжэк", 2007. – 368 с. 6. Филипковская Л.А. Исследование структурно-аналитической модели распознавания образов в задачах управления и диагностики // Проблемы бионики.–Харьков: ХНУРЕ, 2000. – Вып. 53. – С. 51–53. 7. Филипковская Л.А. Информационная технология классификационной обработки данных производственных ситуаций // Вісн. Нац. техн. ун-та "Харк. політехн. ін-т". – Харків: НТУ "ХПІ", 2003. – № 7, Т. 2. – С. 93 – 98. 8. Филипковская Л.А., Скачков А.Н. Обеспечение экономической безопасности авиапромышленного предприятия // Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики. – Харків: Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ". – 2011. – № 2. – С. 100 – 112.

УДК 519.876.5:004.942

О.М. Васьків
Львівська державна фінансова академія

МОДЕЛЮВАННЯ ВИБОРУ СТРАТЕГІЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОБРОБКИ ІНФОРМАЦІЇ

Інформаційні технології використання математичних методів і моделей підвищують якість обробки інформації, професійні якості менеджменту, що є одним із важливих чинників під час прийняття оптимальних управлінських рішень. Застосування інформаційних технологій під час аналізу виробничої діяльності суб'єкта господарювання вимагає розробки стратегії, за якої суб'єкт господарювання відчуває себе конкурентноспроможним.

Ключові слова: інформація, інформаційні технології, моделювання, суб'єкт господарювання, прибуток, обробка інформації.

Information technologies of use of mathematical methods and models improves the quality of information processing, professional skills of management, which is an important factor in making optimal management decisions. The use of information technology in the analysis of production activities of enterprise requires develop a strategy in which the entity feels competitive.

Key words: information, information technology, modeling, entity, income, information processing.

Постановка проблеми

В умовах нестабільності зовнішнього середовища та необхідності раціонального використання наявних матеріально-трудових ресурсів велика увага приділяється вивченню та систематизації усієї сукупності чинників діяльності підприємства, а також вибору оптимальних стратегій його діяльності на ринку за умов невизначеності. Вибір кількох напрямків поточної діяльності та подальшого розвитку підприємства з метою отримання стабільних фінансово-

господарських показників характеризується конфліктними ситуаціями. Формалізацію конфлікту господарської діяльності підприємства варто подати у вигляді безмежної антагоністичної теоретико-ігрової моделі [1]: $\Gamma = \langle \Xi, \Psi, P \rangle$, де $\Xi = (x_1, x_2, ..., x_n)$ – множина можливих дій першого гравця, $\Psi = (h_1, h_2, ..., h_n)$ – множина можливих дій другого гравця, тобто множина чистих стратегій відповідних гравців, які визначають їх дію, P – функція корисності першого гравця або програш другого гравця, яка визначена на усіх парах можливих дій сторін конфлікту та дає змогу визначити стратегії господарської діяльності підприємств в умовах невизначеного ринку, здійснивши комп'ютерну реалізацію задачі.

Аналіз останніх досліджень та публікацій

Актуальність проблеми вибору оптимальних стратегій діяльності підприємства в умовах ринку та застосування інформаційної технології реалізації створеної моделі досліджується у [2, 3].

Формулювання цілі статті

Мета роботи – розробити методику для обчислення оптимальних напрямів господарської діяльності підприємства (стратегії діяльності підприємства) та стратегій ринку і розробити інформаційну технологію комп'ютерної обробки інформації.

Виклад основного матеріалу

У процесі аналізу господарської діяльності підприємств здійснюється впровадження сучасних інформаційних систем, що ґрунтується на досконалих програмних засобах, інформаційних технологіях використання математичних методів і моделей.

Розглянемо задачу моделювання вибору суб'єктом господарювання стратегії випуску продукції, що дає підприємству конкретний прибуток від її реалізації.

Деяке підприємство легкої промисловості здійснює виготовлення та реалізацію n типів продукції і для цього має виробничі потужності. Реалізація n типів продукції може принести підприємству певний сумарний прибуток P, який розраховують за формулою [4]:

$$P = \sum_{j=1}^{n} N_{nom}^{вир} q_j x_j H_{rj}\,, \tag{1}$$

де $N_{nom}^{вир}$ – виробничі потужності підприємства; q_j – прибутковість *j-го* типу продукції; x_j $(j = \overline{1,n})$ – відсотки (частка) виробничих потужностей підприємства, які виділені для виробництва *j-го* типу продукції; H_{rj} – ціна реалізації одиниці продукції на ринку.

Ціна реалізації продукції є функцією від її наявної кількості на ринку, тобто

$$H_{rj} = f_j(x_{k_j})\,, \tag{2}$$

де x_{k_j} – загальна кількість продукції *j-го* типу на ринку.

Однотипна продукція надходить на ринок від багатьох виробників, які конкурують між собою за її збут. Отже, загалом отримаємо

$$P = \sum_{j=1}^{n} N_{nom}^{вир} q_j x_j f_j(Sh_j)\,, \tag{3}$$

де S – загальна кількість усіх решти підприємств, на яких виробляється аналогічна продукція; h_j – частка виробничих потужностей інших підприємств, які задіяні для виробництва *j-го* типу продукції.

Оптимальний розподіл виробничих потужностей на види господарської діяльності підприємства можна подати у вигляді безмежної антагоністичної гри, тобто

$$\Gamma = \langle \Xi, \Psi, P \rangle\,, \tag{4}$$

в якій вектор

$$\Xi = (x_1, x_2, ..., x_n), \qquad x_j \geq 0, \qquad \sum_{j=1}^{n} x_j = 1 \tag{5}$$

визначає чисті стратегії виробника, тобто відсотки від загальної суми коштів реалізованої продукції, а вектор

$$\Psi = (h_1, h_2, ..., h_n), \quad h_j \geq 0, \quad \sum_{j=1}^{n} h_j = 1 \tag{6}$$

визначає стратегію ринку, тобто попит на певну продукцію і функція виграшу задається співвідношенням (3).

Аналіз ринку свідчить, що чим менше продукції на ринку, тим вища її ціна, і тому функція f_j зростатиме.

Припустимо, що зростання функції описується експоненціальним законом [5]:

$$f_j(x_{kj}) = 1 - e^{-\frac{1}{\overline{Y}} x_{kj}}, \tag{7}$$

і враховуючи вираз математичного сподівання $\overline{Y}$ для цього закону:

$$\overline{Y} \geq \frac{1}{\ln \frac{1}{b}}, \tag{8}$$

де b – деякий параметр, та підставивши (7 та 8) у (3) і зробивши деякі перетворення, поставлена задача зводиться до знаходження розв'язків рівняння (3):

$$P = \sum_{j=1}^{n} N_{пот}^{вир} q_j x_j (1 - e^{-\ln \frac{1}{b} Sh_j}). \tag{9}$$

Здійснивши деякі математичні перетворення у рівнянні (4.9), значення гри n можна визначити таким:

$$\nu = \min_{\xi} \max_{\eta} \begin{bmatrix} N_{пот}^{вир} \theta_1 \xi_1 e^{-ln\frac{1}{\beta} S\eta_1} + N_{пот}^{вир} \theta_2 \xi_2 e^{-ln\frac{1}{\beta} S\eta_2} + ... + \\ N_{пот}^{вир} \theta_j \xi_j e^{-ln\frac{1}{\beta} S\eta_j} + ... + N_{пот}^{вир} \theta_n \xi_n e^{-ln\frac{1}{\beta} S\eta_n} \end{bmatrix} = \tag{10}$$

$$= \min_{\xi} \max_{\eta} \begin{bmatrix} N_{пот}^{вир} \theta_1 e^{-ln\frac{1}{\beta} S\eta_1}; N_{пот}^{вир} \theta_2 e^{-ln\frac{1}{\beta} S\eta_2}; ...; \\ N_{пот}^{вир} \theta_j e^{-ln\frac{1}{\beta} S\eta_j}; ...; N_{пот}^{вир} \theta_n e^{-ln\frac{1}{\beta} S\eta_n} \end{bmatrix}.$$

Найменше значення останнього виразу досягається для деякої оптимальної стратегії ринку за умови

$$\begin{bmatrix} \theta_1 e^{-ln\frac{1}{\beta} S\eta_1} = \theta_2 e^{-ln\frac{1}{\beta} S\eta_2} = ... = \theta_j e^{-ln\frac{1}{\beta} S\eta_j} = ... = \theta_n e^{-ln\frac{1}{\beta} S\eta_n} \end{bmatrix}, \tag{11}$$

і прологарифмувавши (11), отримаємо систему рівнянь, яку використовують для визначення оптимальних стратегій ринку $h_i \left(i = \overline{1,n}\right)$, тобто попиту на певного типу продукцію на ринку:

$$\begin{gathered} \ln q_1 - \ln \frac{1}{b} Sh_1 = \ln q_2 - \ln \frac{1}{b} Sh_2, \\ \ln q_3 - \ln \frac{1}{b} Sh_3 = \ln q_4 - \ln \frac{1}{b} Sh_4, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \ln q_j - \ln \frac{1}{b} Sh_j = \ln q_{j+1} - \ln \frac{1}{b} Sh_{j+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \ln q_n - \ln \frac{1}{b} Sh_n = \ln q_1 - \ln \frac{1}{b} Sh_1, \\ h_1 + h_2 + ... + h_i + ... + h_n = 1. \end{gathered} \tag{12}$$

Для обчислення оптимальних стратегій підприємства потрібно знайти частинні похідні функції (9) за аргументами $h_i \left(i = \overline{1,n}\right)$.

Враховуючи, що

$$h_n = 1 - h_1 - h_2 - \ldots - h_{n-1}, \tag{13}$$

запишемо

$$\begin{aligned}
\frac{\partial P}{\partial h_1} &= \ln\frac{1}{b} SN^{вир} q_1 x_1 e^{-\ln\frac{1}{b} Sh_1} + \ln\frac{1}{b} SN^{вир} q_n x_n e^{-\ln\frac{1}{b} Sh_n}, \\
\frac{\partial P}{\partial h_2} &= \ln\frac{1}{b} SN^{вир} q_2 x_2 e^{-\ln\frac{1}{b} Sh_2} + \ln\frac{1}{b} SN^{вир} q_n x_n e^{-\ln\frac{1}{b} Sh_n}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\frac{\partial P}{\partial h_j} &= \ln\frac{1}{b} SN^{вир} q_j x_j e^{-\ln\frac{1}{b} Sh_j} + \ln\frac{1}{b} SN^{вир} q_n x_n e^{-\ln\frac{1}{b} Sh_n}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\frac{\partial P}{\partial h_{n-1}} &= \ln\frac{1}{b} SN^{вир} q_{n-1} x_{n-1} e^{-\ln\frac{1}{b} Sh_{n-1}} + \ln\frac{1}{b} SN^{вир} q_n x_n e^{-\ln\frac{1}{b} Sh_n}.
\end{aligned} \tag{14}$$

Прирівнявши праві частини (14) до нуля і врахувавши співвідношення (6), отримаємо систему рівнянь для визначення стратегії підприємства легкої промисловості, тобто тих часток виробничих потужностей, які варто виділяти для виробництва певного типу продукції:

$$\begin{aligned}
\ln\frac{1}{b} Sq_1 x_1 e^{-\ln\frac{1}{b} Sh_1} + \ln\frac{1}{b} Sq_n x_n e^{-\ln\frac{1}{b} Sh_n} &= 0, \\
\ln\frac{1}{b} Sq_2 x_2 e^{-\ln\frac{1}{b} Sh_2} + \ln\frac{1}{b} Sq_n x_n e^{-\ln\frac{1}{b} Sh_n} &= 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\ln\frac{1}{b} Sq_j x_j e^{-\ln\frac{1}{b} Sh_j} + \ln\frac{1}{b} Sq_n x_n e^{-\ln\frac{1}{b} Sh_n} &= 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\ln\frac{1}{b} Sq_{n-1} x_{n-1} e^{-\ln\frac{1}{b} Sh_{n-1}} + \ln\frac{1}{b} Sq_n x_n e^{-\ln\frac{1}{b} Sh_n} &= 0, \\
x_1 + x_2 + \ldots + x_i + \ldots + x_n &= 1.
\end{aligned} \tag{15}$$

Загальний дохід, отриманий підприємством від реалізації виготовленої продукції на ринку, розраховуватиметься за формулою (3). Значення параметра $a = 0{,}6$ $(0 \le a \le 1)$.

Математичне та комп'ютерне моделювання стратегії розвитку підприємства із залученням інформаційних технологій дає можливість провести необхідні розрахунки та проаналізувати отримані результати розв'язання поставленої задачі [6]. Знаходження розв'язків можна здійснити засобами пакета прикладних програм для математичних обчислень Microsoft Excel 2000.

Результуючі дані формуються програмою, написаною з використанням знань та навиків мови програмування Visual Basic for Applications. Створена програма працює на основі макросів, які забезпечують роботу кнопок головного меню. Передбачена можливість перегляду початкової інформації, формування бази даних, виведення на екран та на друк результуючих даних. Як приклад, можна навести фрагмент процедури формування робочого розрахункового листа (лістинг 1) [7].

Лістинг 1. Процедура F_R() (формування розрахунків)

```
Sub F_R()
'Заповнення результуючої таблиці інформацією
'Задається назва листа та діапазон комірок, з яких береться інформація
Sheets("Вид продукції").Select
```

```
ActiveCell.Offset(0, 0).Select
Range(“B106:B109”).Select
Selection.Copy
‘Задається назва та діапазон, куди інформація вставляється
Sheets(“Розрахунок”).Select
Range(“C9:C12”).Select
Selection.PasteSpecial Paste:=xlValues, Operation:=xlNone, SkipBlanks:= _
 False, Transpose:=False
……..…….
End Sub
```

Перед початком роботи зі створення робочого розрахункового листа потрібно очистити усі заповнені інформацією комірки. Для їх очищення наведено процедуру Clear(), текст якої подано на лістингу 2.

Лістинг 2. Процедура Clear()

```
Sub Clear()
Sheets(“Розрахунок”).Select
Range(“C9:C12”).Select
Selection.ClearContents
End Sub
```

Друк сформованих розрахунків здійснюється з використанням процедури Prn_F_R() (лістинг 3).

Лістинг 3. Процедура Prn_F_R()

```
Sub Prn_F_R()
Sheets(“Розрахунок”).PrintPreview
End Sub
```

Інформаційні технології дають змогу підприємствам підвищувати ефективність процесів управління, збору, обробки, передачі даних, а відкритість системи, впровадження та розвиток мереж змушують управлінців задуматись над проблемою захисту інформації [8].

Захист інформації у системі передбачає захист процесів створення даних, їх введення, обробку і виведення, а також забезпечення безперервності бізнесу та мінімізації бізнес-ризику.

Програма дає можливість захищати інформацію від несанкціонованого втручання. Задаючи параметри захисту, можна заборонити змінювати: інформацію в комірках, елементи діаграм, графічні об’єкти аркушів чи діаграм, а також захист може бути закріплений паролем.

Захищеність інформації, якою володіє підприємство, від несанкціонованого доступу здійснюється завдяки апаратному забезпеченню та установленими системами криптографії і міжмережевими екранами [7, 9].

Використання інформаційних технологій під час оброблення інформації, а також її захист є невід’ємними чинниками для ефективної роботи підприємства та для оптимальних розв’язків задач управління.

1. Дюбин Г. Н. Введение в прикладную теорию игр / Г. Н. Дюбин, В. Г. Суздаль. – М.: Наука, 1981. – 336 с. 2. Юринець В.Є. Вибір стратегії випуску готової продукції підприємствами в умовах невизначеного ринку / В.Є. Юринець, А.Є. Жмуркевич // Регіональна політика України: наукові основи, методи, механізми: зб. наук. пр. за матер. доп. на Міжнар. наук.-практ. конф. – Львів: Інститут регіональних досліджень НАН України, 1998. – Ч. ІІ. – С. 20–26. 3. Васьків О. М. Модель визначення стратегії діяльності підприємств легкої промисловості в ринкових умовах / О. М. Васьків // Вісник Львівської державної фінансової академії. – 2008. – №14. – С. 196–202. 4. Васьків О.М. Економіко-математична модель визначення стратегії господарської діяльності підприємств легкої промисловості в умовах невизначеного ринку / О. М. Васьків // Науковий вісник Буковинської державної фінансової академії: зб. наук. пр. – Вип. 2 (19): Економічні науки. – Чернівці: Технодрук, 2010. – С. 421–428. 5. Васьків О. М. Математична модель процесу розвитку виробничої діяльності підприємства в невизначеному ринковому середовищі / О. М. Васьків // Статистична оцінка соціально-економічного розвитку: зб. наук. пр. – 2010. – С. 205–207. 6. Заяць В. М. Роль інформаційних технологій у формуванні стратегічного мислення

менеджера / В. М. Заяць // Актуальні проблеми економіки. – 2009. – № 6 (96). – С. 280–288. 7. Гарнаев А. Ю. Самоучитель VBA / А. Ю. Гарнаев. – 2-е изд., перераб и доп. – СПб.: БХВ-Петербург, 2004. – 560 с. 8. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2, Т. 2. – С. 32–35. 9. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – М.: Изд-во "Интернет-университет информационных технологий – ИНТУИТ.ру", 2003. – 280 с.

УДК 003.26.09:004.032.24

О. Кравець, С. Лупенко, А. Луцків
Тернопільський національний технічний університет ім. І. Пулюя,
кафедра комп'ютерних систем та мереж,

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИПТОАНАЛІЗУ СУЧАСНИХ ПОТОКОВИХ ШИФРІВ

Розглянуто підвищення ефективності криптоаналізу сучасних потокових шифрів. Проаналізовано сучасне програмне забезпечення для здійснення алгебраїчного криптоаналізу потокових шифрів. Запропоновано шляхи оптимізації сучасних криптоаналітичних методів потокових шифрів шляхом використання паралельних та розподілених високопродуктивних обчислювальних засобів.

Ключові слова: криптоаналіз, потокові шифри, високопродуктивні обчислення, обчислювальні кластери.

Increasing efficiency of cryptanalysis of the modern stream ciphers this paper is devoted. Modern software for the algebraic cryptanalysis of stream ciphers are analyzed in article. The ways of optimization of modern cryptanalysis methods for stream ciphers by using parallel and distributed high-performance and data processing systems are proposed.

Key words: cryptanalysis, stream ciphers, high-performance computing, computational clusters.

Вступ. Загальна постановка проблеми

Криптостійкість потокових алгоритмів шифрування, тобто стійкість до криптографічної атаки за певних фіксованих умов вимірюється потрібною кількістю ресурсів для проведення криптоатаки. Ресурсами є такі величини:

1. Кількість інформації, яка необхідна для здійснення успішної атаки, а саме – необхідна кількість пар відомих або вибраних текстів.

2. Обчислювальна складність алгоритму криптоаналізу визначається ресурсами, необхідними для його виконання, і є функцією, яка визначає залежність обсягу роботи, що виконується цим алгоритмом від розміру вхідних даних. На практиці виділяють дві складові обчислювальної складності: T (часову складність) і S (просторову складність або вимоги до пам'яті). T і S, як правило, подаються як функції від n, де n – розмір вхідних даних, тобто кількість відкритих і/або зашифрованих даних.

Так, величина T – час, який необхідний для здійснення успішної атаки, визначається кількістю тестових операцій шифрування атакуючим алгоритмом, виконання яких за дотримання інших необхідних умов дає змогу, наприклад, визначити ключ шифрування.

Величина S – вказує на обсяг пам'яті, який необхідний для проведення успішної атаки. Ціла низка криптоатак не може бути реалізована на практиці у зв'язку з недостатнім обсягом оперативної та дискової пам'яті. Цей параметр визначає просторову складність криптоалгоритму.

Розглянемо детальніше ці складові.

1. Під час перехоплення трафіку переважно реалізується атака "man-in-the-middle", – тобто активне або пасивне перехоплення трафіку. Це завдання істотно спрощується, якщо