УДК 681.5(042.3)

СИТУАЦІЙНЕ УПРАВЛІННЯ ДОСТУПОМ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

В.В. Семко, В.Л. Бурячок, С.В. Толюпа, П.М. Складанний
Державний університет телекомунікацій

Abstract *– We proposed and studied mathematical model of conflict management control object interaction in cyberspace with an open set of objects of observation in terms of limitations and uncertainties. The study determined that the use of semioticheskihsistem proved fruitful for solving problems upravleniyane only dynamic objects, but also non-classical, naproimer, cybernetic. The way one mapping parameters that characterize a formal model of conflict in cyberspace in the synthesis of universal strategies to address the conflict in the "small" and "large". Based on the model of conflict interaction of objects in cyberspace observation and research shows that the control method for the synthesis of strategies for solving the conflict has two stages: the synthesis of the model to describe the interaction of objects of conflict in cyberspace surveillance and research; the synthesis of the formal description of the space in which there is a guaranteed combined management of the facility. In this case, the task of resolving the conflict is presented as a variation and extreme element on the criterion of selection strategies to address is valid, despite the possible abrupt change in the state vector describing the formal environment of conflict. For resolvsyg the conflict interaction of objects in cyberspace provided a method of integral truncation options, which methodologically permits to find the solution of the conflict, subject to availability guaranteed object management, integrity and tseledostizhimosti his behavior..*

Анотація *– Виходячи з принципів побудови дискреційних моделей управління доступом в інформаційно-телекомунікаційних системах (ІТС), запропоновано та досліджено підхід до імітаційного моделювання можливості отримання системи за результатами переведення ІТС в новий стан при вирішенні задачі спостереження, пошуку та синтезу рішень щодо конфліктів в кібернетичному просторі. Синтезовано формальну модель конфлікту, яка є універсальною при синтезі стратегій вирішення конфлікту в «малому» та у «великому». Для вирішення конфлікту взаємодії об'єктів в кібернетичному просторі запропоновано метод інтегрального усікання варіантів, який методологічно дозволяє знаходити рішення задачі конфлікту в кібернетичному просторі спостереження та пошуку (КПСП) за умов наявності гарантованого управління об'єктом управління (ОУ), цілісності таціледосяжності його поведінки.*

Аннотация *– Исходя из принципов построения дискретных моделей управления доступом в информационно-телекоммуникационных системах (ИТС), предложен и исследован подход к имитационному моделированию возможности получения системы по результатам перевода ИТС в новое состояние при решении задачи наблюдения, поиска и синтеза решений по конфликтам в кибернетическом пространстве. Синтезирована формальная модель конфликта, которая является универсальной при синтезе стратегий разрешения конфликта в «малом» и в «большом». Для решения конфликта взаимодействия объектов в кибернетическом пространстве предложен метод интегрального усечения вариантов, который методологически позволяет находить решение задачи конфликта в кибернетическом пространстве наблюдения и поиска (КПСП) при условии наличия гарантированного управления объектом управления (ОУ), целостности и циледосяжности его поведения.*

Вступ

Забезпечення безпеки функціонування інформаційно-телекомунікаційних систем (ІТС) пов'язане, як відомо, з забезпеченням захисту від несанкціонованого доступу (НСД) до об'єктів цих систем. Враховуючи таке, відповідно до обраної політики без-

пеки та моделі доступу до об'єктів ІТС [1], необхідно визначити технічні та технологічні рішення, а також серед низки існуючих аналогів вибрати раціональні засоби щодо вирішення задачі унеможливлення реалізації таких спроб [2].

Вирішення такої задачі за своєю сутністю є вирішенням задачі конфлікту взаємодії об'єктів та суб'єктів ІТС [3, 4] з об'єктами кібернетичного простору, які можуть бути ініційовані будь-яким його суб'єктом або об'єктом. В процесі її розв'язання слід враховувати, що існуючі методи розв'язання конфліктів [3, 4, 7] мають низку методичних проблем, пов'язаних з так званим «ефектом доміно», «прокляттям розмірності» та неможливістю прийняття гіпотези про випадковий характер процесів за умов невизначеності, і які обумовлюються довільною системою обмежень та відкритою множиною об'єктів спостереження (ОС) в кібернетичному просторі спостереження та пошуку (КПСП) [8].

Виходячи з такого, в процесі досліджень було синтезовано формальну модель конфлікту [5, 6], яка є універсальною при синтезі стратегій вирішення конфлікту в «малому» та у «великому». Для вирішення конфлікту взаємодії об'єктів в кібернетичному просторі було запропоновано метод інтегрального усікання варіантів [7], який методологічно дозволяє знаходити рішення задачі конфлікту в КПСП за умов наявності гарантованого управління об'єктом управління (ОУ), цілісності та цілеспрямованості його поведінки.

I. Постановка проблеми

Виходячи з моделі конфлікту взаємодії об'єктів в КПСП, метод синтезу стратегій управління при вирішенні конфлікту вміщує два основних етапи, а саме: синтез моделі опису КПСП та синтез формального опису простору, в якому гарантовано існує комбіноване управління (ПРКУ) ОУ. В такому разі задача вирішення конфлікту представляється як варіаційна, а екстремальний елемент за критерієм вибору стратегій рішення є припустимим, незважаючи на можливу стрибкоподібну зміну вектора стану формального середовища опису конфлікту.

Актуальним є синтез формальної моделі конфлікту в кібернетичному просторі та алгоритмів розрахунку і формального відображення інформаційної множини КПСП, ПРКУ та методу синтезу стратегій оптимального управління ОУ за певним критерієм при вирішенні задачі конфлікту взаємодії з відкритою множиною ОС за умов невизначеності їх поведінки та довільної системи обмежень КПСП.

Критерій оптимального управління враховує принципи гомеостатичності функціонування технічної ергатичної системи [7].

В такому разі підхід до розв'язання конфлікту за методом інтегрального усікання варіантів, пов'язаний з побудовою мінімізуючої послідовності траєкторій (стратегій, ланцюжків) у просторі рішень (ПР), відображає принцип оптимальності при синтезі та виборі стратегії рішення конфлікту.

Метою дослідження є синтез моделі конфлікту взаємодії об'єктів в КПСП в умовах невизначеності поведінки відкритої множини ОС, неопуклості та небезперевності

КПСП. При цьому враховуються особливості стану і поведінки суб'єктів та об'єктів конфлікту. Саме ці особливості є визначальними при синтезі та виборі стратегії управління при вирішенні конфлікту.

II. Основна частина

При дослідженні системи захисту інформації (СЗІ) від НСД до суб'єктів та об'єктів, які складають множину елементів ІТС, оберемо модель дискреційного доступу [Discretionary Access Control (DAC)]. Виходячи з того, що КПСП є метричним і, за необхідності, може бути декомпозований на класи еквівалентності [9, 10], СЗІ можна представити у вигляді декартового добутку множин, складовими частинами яких є елементи системи захисту, а саме суб'єкти, об'єкти, рівні доступу, операції тощо.

В такому разі матриця доступу M на множині суб'єктів S та об'єктів O ІТС може бути визначена як декартовий добуток

$$M = S \times O. \tag{1}$$

Виходячи з співвідношення (1), для класів еквівалентності S і O визначимо права доступу для матриці M згідно з множиною прав доступу R та множини елементарних операцій

$$\alpha_z \in \alpha, \forall z \in Z, \tag{2}$$

які передбачені функціональністю ІТС та політикою безпеки СЗІ:

$$M[S_i, O_j] = R_k, \forall S_i \in S, \forall O_j \in O, \forall R_k \in R. \tag{3}$$

Значення Z у співвідношенні (2) визначається функціональністю ІТС.

Слід зазначити, що в співвідношенні (3) визначено

$$\begin{cases} i = \{1,\ldots,n\} \\ j = \{1,\ldots,m\}, \\ k = \{1,\ldots,l\} \end{cases} \tag{4}$$

де n – кількість суб'єктів S, m – кількість суб'єктів O, l – кількість суб'єктів R.

Результатом застосування політики безпеки, що задається моделлю безпеки до конкретного об'єкту захисту ІТС, є дозвіл або заборона виконання елементарних операцій α_z відповідно співвідношенню (2) над об'єктом захисту.

Таким чином, в результаті виконання елементарних операцій α відповідно матриці доступу M згідно з визначеною множиною прав доступу для класів еквівалентності S і O можна формально визначити перехід ІТС в результаті виконання елементарної операції p з множини α із стану $Q = (S, O, M)$ до стану $Q' = (S', O', M')$. Тобто у результаті виконання примітивного оператора з множини α здійснюється перетворення стану ІТС:

$$Q \underset{\alpha}{\mapsto} Q'. \tag{5}$$

Таким чином, співвідношення (1) - (5) визначають переміщення ІТС в КПСП.

Визначимо рівні безпеки суб'єктів *S* і об'єктів *O* за допомогою функції рівня безпеки [1]:

$$F : S \cup O \to L, \tag{6}$$

яка ставить у відповідність кожному об'єкту і суб'єкту рівень безпеки, що відносять до множини рівнів безпеки (секретності)

$$L, \bigcup_{d=1}^{D} L_d, \tag{7}$$

на якому визначена решітка

$$\Lambda = \left(L, \bigcup_{t=1}^{T} \Lambda_t \right). \tag{8}$$

У співвідношенні (7) L_d визначає рівні безпеки (секретності), наприклад, «несекретно», «секретно» тощо і може позначатись як вербально, так і кількісно. Для співвідношення (8) значення Λ_t визначає такі оператори, як нестроге відношення порядку для рівнів секретності, найменшої верхньої та найбільшої нижньої границі тощо.

Слід зазначити, що у співвідношенні (6) функція рівня безпеки F з решіткою рівнів визначає усі допустимі відносини доступу між суттєвостями ІТС. У такому разі множина станів ІТС може бути визначена набором

$$V = (F, M). \tag{9}$$

З врахуванням (9) модель системи

$$\Sigma = (v_0, R, T) \tag{10}$$

описує процес переходу ІТС з початкового стану v_0 до наступного стану v^* при запиті r за умови $r \in R$, де R – множина припустимих запитів до ІТС.

Тобто ІТС за функцією переходу

$$T : ((V \times R) \to V) \tag{10}$$

переходить у стан

$$v^* = T(v, r). \tag{11}$$

Слід зауважити, що стан ІТС $v \in V$ може бути досягнуто при виконанні послідовності n запитів та станів

$$\langle (v_0, r_0), \ldots, (v_n, r_n) \rangle \forall\, v_{i+1} = T(v_i, r_i), i \in [0, n]. \tag{12}$$

У такому разі з врахуванням основної теореми безпеки Белла-ЛаПадули та співвідношень (9) – (11) перехід ІТС із стану v_0 до стану v^* є тривіально досяжним та безпечним. При цьому теорема Мак-Ліна визначає умови безпечності функціонування ІТС

за умов зміни її стану. Незважаючи на це твердження, слід мати на увазі, що система може бути безпечною, але не мати безпечної функції переходу.

Операція зчитування між віддаленими об'єктами сприяє виникненню потоку інформації від об'єкта, з якого інформація зчитується, до об'єкта, з якого формується запит на зчитування інформації для відповідного суб'єкта. Потік, який з'являється при цьому, є безпечним у зв'язку з тим, що інформація є недоступною для неавторизованого суб'єкта. Разом з тим у розподіленій системі зчитування ініціюється запитом від одного об'єкта до іншого. Такий запит створює потік інформації, який йде в зворотному (неправильному) напрямку (запис в об'єкт з нижчим рівнем секретності або в об'єкт, для якого не передбачена взаємодія з об'єктом, який створив запит).

Слід мати на увазі, що в такому разі необхідно забезпечити безпеку ІТС в початковому та кінцевому стані, включаючи процес переходу між станами. Також для ІТС необхідно реалізувати таку функцію переходу, яка відповідала би вказаним умовам безпеки, а саме

$$C : S \cup O \to \square(S), \tag{13}$$

де $\square(S)$ - множина усіх підмножин S, що визначає підмножину суб'єктів, яким дозволено змінювати рівень безпеки для заданого об'єкта або суб'єкта.

Тоді з урахуванням співвідношення (13) модель системи

$$\Sigma = \left(v_0, R, T^{\alpha}\right) \tag{14}$$

складається з початкового стану v_0 множини запитів R і функції переходу T^{α}, яка переводить систему зі стану в стан по мірі опрацювання запитів. Це сприяє появі у функції переходу, яка визначає наступний стан системи після виконання певним суб'єктом деякого запиту ще одного аргументу – суб'єкта, від якого надходить цей запит, оскільки результат переходу залежить від того, який суб'єкт його ініціював:

$$T^{\alpha} : (S \times V \times R) \to V . \tag{15}$$

Виходячи із співвідношень (13), (14), (15), можна стверджувати, що ІТС, яка знаходиться у стані $v \in V$, переходить при отриманні запиту $r \in R$ від суб'єкта $s \in S$ із стану v до стану

$$\overset{*}{v} = T^{\alpha}(s, v, r) . \tag{16}$$

Важливо зазначити, що функція переходу (16) є авторизованою за умови, якщо для кожного переходу (16), для якого згідно із співвідношенням (9) $v = (F, M)$ та $\overset{*}{v} = (F', M')$

$$\forall x \in S \cup O \Leftrightarrow \overset{*}{F}(x) \neq F(x) \Rightarrow s \notin C(x), \tag{17}$$

що відповідає умовам безпеки згідно із співвідношенням (13).

Із співвідношення (17) випливає те, що в ході авторизованого переходу рівень безпеки суб'єкта або об'єкта може змінитися тільки тоді, коли суб'єкт, що виконує перехід, належать множині суб'єктів, уповноважених змінювати рівень цього суб'єкта або об'єкта.

Відношення щодо ініціації об'єкта суб'єктом чи іншим об'єктом є ключовими для аналізу можливостей здійснення переходу системи в незахищений стан при зміні характеристик матриці доступу, які передбачені функціональністю ІТС та політикою безпеки СЗІ згідно із співвідношенням (3).

З метою моделювання можливості отримання Z - системи за результатами переведення ІТС в новий стан доцільним є використання підходів щодо вирішення задачі спостереження та пошуку в підпросторі кібернетичного простору, який притаманний конкретній ІТС [5, 9], з використанням методів пошуку, які використовуються в системах штучного інтелекту.

Розглянемо похідний стан гіпотетичної ІТС (рис.1), який визначено правилами та відношеннями для підпростору кібернетичного простору в евклідовому математичному просторі для моделі M згідно із співвідношенням (1).

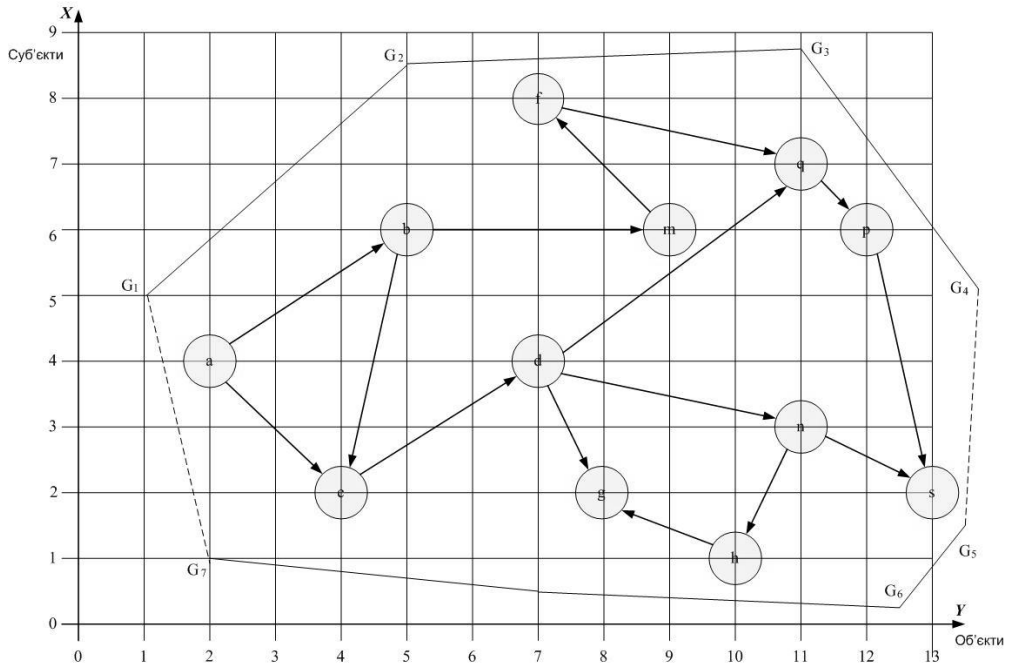

Рис. 1. Похідний стан взаємодії суб'єктів та об'єктів гіпотетичної ІТС

Стан гіпотетичної ІТС після виконання ланцюжка дій (рис. 2) згідно із співвідношенями (9) – (17) визначає виникнення нових відношень (рис. 2), які фактично дозволяють побудувати Z - систему.

Похідним об'єктом інформаційної взаємодії є об'єкт a. В якості кінцевого об'єкта технології інформаційної взаємодії ІТС визначено об'єкт s.

Згідно з правилами відношень та обчислюваним значенням функції переходу знаходимо оптимальний маршрут інформаційної взаємодії.

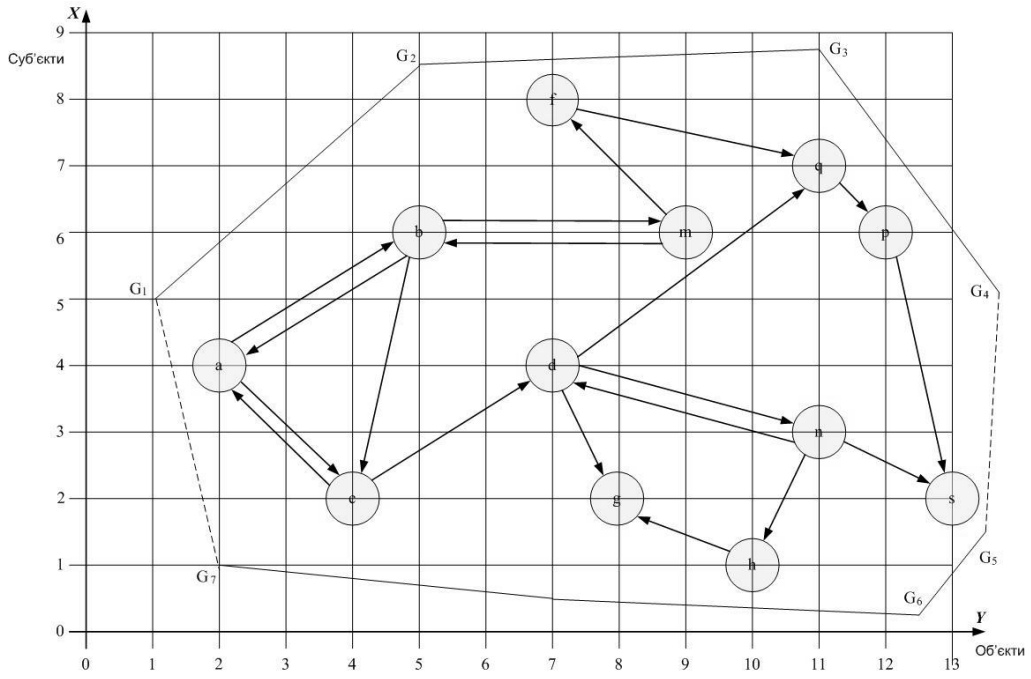

Рис. 2. Кінцевий стан взаємодії суб'єктів та об'єктів гіпотетичної ІТС

Алгоритм було реалізовано в середовищі розробки Visual Prolog. Функція ціни була обчислена за критерієм найменшої відстані (рис. 3).

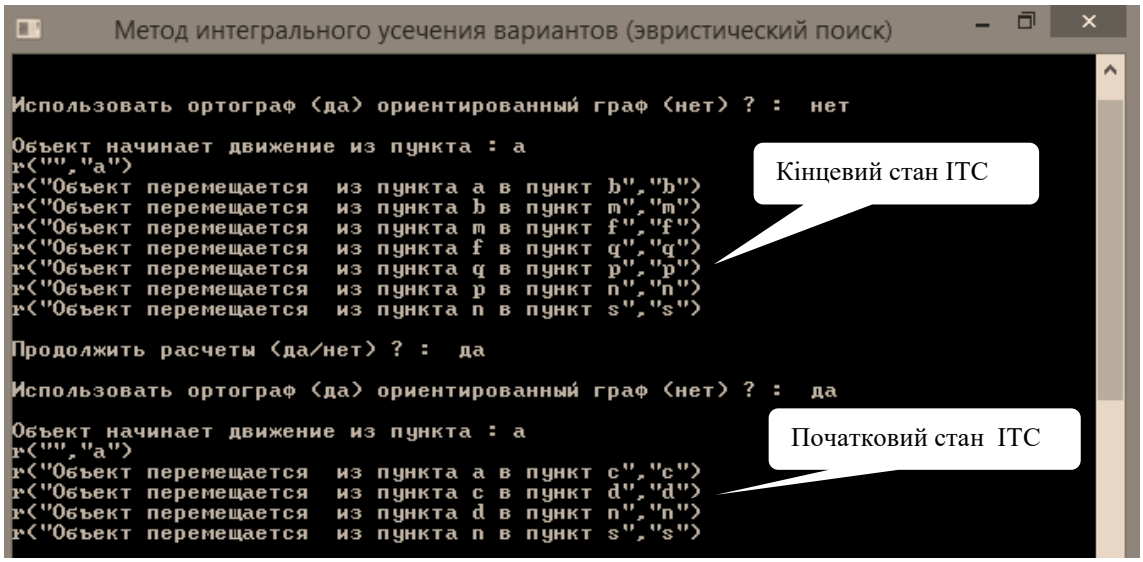

Рис. 3. Результати розрахунку маршруту проходження інформації в ІТС при переміщенні з початкового в кінцевий стан

Результат імітаційного експерименту щодо рішення задачі пошуку маршруту проходження інформації між об'єктами гіпотетичної ІТС (рис. 3) при зміні стану показує можливі шляхи проходження інформації за рахунок відкритих потоків обміну в багатозадачному обчислювальному середовищі.

Висновки

1. Сучасний рівень розвитку інформаційних технологій інформаційно-телекомунікаційних систем породжує нові моделі та методи аналізу процесів обробки інформації та синтезу рішень щодо побудови новітніх ефективних систем захисту інформації від несанкціонованого доступу.

2. Застосування методів штучного інтелекту дозволяє оцінювати та контролювати не тільки факт наявності інформаційних потоків в інформаційно-телекомунікаційних системах, але й оцінювати ступінь його допустимості в рамках політики безпеки

3. Використання методів штучного інтелекту дозволяє забезпечувати захист у інформаційно-телекомунікаційних систем від атак типу «Троянський кінь», контролювати «сховані» канали передачі інформації в комп'ютерних системах та мережах.

4. Запропонований підхід щодо імітаційного моделювання можливості отримання системи за результатами переведення інформаційно-телекомунікаційної системи в новий стан є новітнім при вирішенні задачі спостереження, пошуку та синтезу рішень щодо конфліктів в кібернетичному просторі.

5. Новітні системи інформаційної безпеки мають створюватись з використанням парадигм функціонального та логічного програмування.

Список літератури:

1. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. – М. : Радио и связь, 2000. – 192 с.

2. *Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В.* Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. – К. : ДУТ, 2015. – 345 с.

3. *Касьянов В.А.* Субъективный анализ: Монография. – К. : НАУ, 2007. – 512 с.

4. *Павлов В.В.* Конфликты в технических системах. – К. : Вища школа, 1982. – 184 с.

5. *Семко В.В.* Модель конфлікту взаємодії об'єктів кібернетичного простору // Проблеми інформатизації та управління. – 2012. – Вип. 2(38). – С. 88-92.

6. *Семко В.В.* Формальний опис простору пошуку при синтезі рішень // Проблеми інформатизації та управління. – 2013. – Вип. 2(42). – С. 104-111.

7. *Семко В.В.* Використання методу інтегрального усікання варіантів при вирішенні задач конфлікту взаємодії об'єктів в просторі спостереження // Інформаційні та телекомунікаційні технології. – 2015. – Вип. 1. – С. 59-66.

8. *Семко В.В., Семко О.В.* Дослідження властивостей рішення задачі конфлікту за методом інтегрального усікання варіантів // Проблеми інформатизації та управління. – 2013. – Вип. 2(46). – С. 60-71.

9. *Семко В.В.* Модель взаємодії кібернетичних організмів та синтез стратегій оптимального керування в кібернетичному просторі. // Проблеми інформатизації та управління. – 2013. – Вип. 3(43). – С. 75-82.

10. *Трауб Дж., Васильковский Г., Вожьняковский Х.* Информация, неопределенность, сложность. – М. : Мир, 1988. – 184 с.