віброакустики: Учебник для вузов. - СПб.: Политехника, 2000.-482 с.: ил. Библиогр.: с. 482. ***3.*** *Скрытые марковские модели в структурном анализе сигналов / Моттль В. В., Мучник И. Б. - М.: Физматлит, 1999.* ***4.*** *Л. Рабинер, Б. Гоулд. Теория и применение цифровой обработки сигналов. - М.: Мир, 1978. –с. 852.* ***5.*** *Астафьева Н. М. Вейвлет анализ: основы теории и примеры применения. Успехи физических наук. Том 166. № 11. 1996, с. 1145 – 1170.* ***6.*** *Володарський Є. Т., Шантир Д. С. Дослідження похибки значень коефіцієнтів вейвлет-перетворення // Наукові вісті НТУУ "КПІ". - 2006. - №3. – С. 91 – 98.*

УДК 681.3.06

АСПЕКТИ ЗАСТОСУВАННЯ ТЕОРІЇ ФУНКЦІОНУВАННЯ ОРГАНІЗАЦІЙНИХ СИСТЕМ ДО ВИРІШЕННЯ ЗАДАЧ КЕРУВАННЯ ЗАХИСТОМ ІНФОРМАЦІЇ

Віктор Жора
Інститут програмних систем НАН України

Анотація: **Інформаційно-телекомунікаційна система розглядається як дворівнева активна організаційна система. Для вирішення задач керування захистом інформації в інформаційно-телекомунікаційних системах пропонується застосовувати методи теорії функціонування організаційних систем.**
Summary: **Information and telecommunication system is considered as a two-level active organization system. Methods of theory of functioning of organization systems are proposed to be applicable in solving problems of information protection management in information and telecommunication systems.**
Ключові слова: **Інформаційно-телекомунікаційна система, організаційна система, керування, захист інформації.**

I Вступ

Задача ефективного забезпечення захисту інформації в інформаційно-телекомунікаційній системі (ІТС) містить в собі декілька складових: створення релевантних моделей загроз і порушника, аналіз ризиків і відповідне концептуальне планування системи захисту, розробка політики безпеки інформації і формування технічних та організаційних вимог до системи захисту відповідно до її положень, врешті – реалізація і впровадження заходів і засобів захисту. В сукупності з випробуваннями системи зазначених складових цілком достатньо для введення комплексної системи захисту інформації в промислову експлуатацію. Далі алгоритм функціонування захищеної ІТС визначається згідно з заздалегідь розробленим планом захисту інформації, посібниками адміністраторів і користувачів, інструкціями, іншою експлуатаційною документацією. Природною є подальша актуалізація моделі загроз, політики безпеки, адаптація системи захисту до змін у різноманітних середовищах функціонування ІТС: фізичному, обчислювальному, інформаційному, середовищах користувачів та технології обробки. Вся зазначена діяльність безпосередньо відноситься до керування захистом інформації. Отже, керування захистом є важливим етапом діяльності у сфері захисту інформації, від якої напряму залежить успішність заходів із забезпечення безпеки інформації.

Враховуючи наведені міркування, доходимо висновку, що однією з головних властивостей ІТС, окрім захищеності, має бути керованість, зокрема, керованість в сенсі захисту інформації. Актуальними задачами наразі є пошук механізмів керування захистом, аналіз застосовності існуючих підходів до керування складними системами саме у сенсі безпеки інформації, формулювання умов для найбільш ефективного керування.

II Базові визначення та постановка задачі

Сформулюємо загальну задачу керування захистом інформації в ІТС. Нехай стан системи описується змінною $y \in \mathbf{Y}$, що належить деякій припустимій множині $\mathbf{Y}$. В даному випадку під множиною $\mathbf{Y}$ будемо розуміти множину всіх станів захищеності системи. Стан системи в деякий момент часу залежить від керуючих впливів $\eta \in \mathbf{H}$: $y=\mathrm{G}(\eta)$. Припустимо, що на множині $\mathbf{H}\times\mathbf{Y}$ заданий функціонал $\Phi(\eta, y)$, що визначає ефективність функціонування системи [1]. Величина $K(\eta)=\Phi(\eta,\mathrm{G}(\eta))$ називається *ефективністю керування* $\eta \in \mathbf{H}$. Задача керівного органу полягає у виборі такого припустимого керування, яке б максимізувало значення його ефективності за умови, що відома реакція системи на керуючі впливи:

$K(\eta) \to \max\limits_{\eta \in \mathrm{H}}$.

Об'єктна модель ІТС являє собою узгоджену сукупність об'єктів, пов'язаних між собою. Згідно з [2, 3] об'єктна модель ІТС містить активні об'єкти, а саме об'єкти-користувачі та об'єкти-процеси. Активність цих двох груп об'єктів полягає насамперед у можливості виконання операцій над іншими об'єктами. Припустимо, що серед множини активних об'єктів є керовані, тобто такі, поведінку (стан) яких можна змінити за допомогою зовнішніх (керуючих) впливів. Насправді, дане припущення є цілком природним, оскільки практичні реалізація ІТС і систем захисту за замовчуванням передбачають керованість їх компонентів. В сенсі теорії керування *активність* системи означає, що в системі наявний хоча б один активний керований елемент, що передбачає свободу цілеспрямованого вибору власного стану. Останнє передбачає наявність у об'єкта власних інтересів. Зауважимо, що дана активність відрізняється від тієї, що розглядається в сенсі класифікації об'єктів ІТС, оскільки об'єкт-процес не повинен мати можливість обирати свій стан. Дана властивість має бути (і власне кажучи, так і є) виключною прерогативою об'єкта-користувача. Таким чином, користувач характеризується певною поведінкою і стратегією в ІТС. Тому, багатокористувацька ІТС безумовно є активною системою, і для вирішення задач керування можуть бути застосовані методи керування активними системами, межу застосовності яких потрібно чітко окреслити. Обов'язковим елементом є зовнішнє середовище, зв'язки якого як з центром, так і з елементами забезпечують повноту картини функціонування організаційної системи [4].

Стан ІТС в будь-який момент часу унікально характеризується сукупністю станів окремих її елементів, включно до останнього рівня декомпозиції. В такій моделі пасивні об'єкти фактично є об'єктами зовнішнього впливу з боку активних об'єктів, тим самим слугуючи базою для формування критеріїв захищеності системи, оскільки саме з ними пов'язані фундаментальні властивості захищеної інформації, такі як конфіденційність, цілісність і доступність.

Роблячи припущення про здійснення керуючого впливу на систему як сукупності задіяних в кожний момент часу процесів з боку об'єктів-користувачів, приходимо до трансформування багаторівневої об'єктної моделі ІТС в модель дворівневої пасивної системи. Як центр такої системи розглядається користувач, як елементи – процеси.

Отже, задача керування захистом інформації може бути розділена на дві складові: з одного боку є загальна задача керування діяльністю користувачів, спрямована на забезпечення визначеного рівня захищеності, а з другого – загальна задача керування системою захисту інформації як сукупністю елементів, що реалізують певні функції захисту.

В разі постановки задачі забезпечення захисту інформації в ІТС та керованості процесів захисту цільовій функції системи, що характеризує рівень захищеності, співставляється виробнича функція, що задає максимальний рівень захищеності залежно від заданих рівнів витрат. Таким чином, загальна задача захисту також може бути сформульована як задача пошуку виробничої функції.

ІІІ Основна частина

Основна відмінність активної системи від системи з пасивними елементами полягає в тому, що керовані об'єкти схильні до вибору станів, найкращих з точки зору їх власних інтересів при заданих або прогнозованих значеннях керуючих впливів. Керуючі впливи, в свою чергу, залежать від станів керованих елементів. Задача вибору оптимального керування $\eta^* = \tilde{\eta}(y) \in \mathrm{H}$, $\tilde{\eta} : \mathrm{Y} \to \mathrm{H}$ в такому випадку має наступний вигляд: знайти

$$\eta^* \in Arg \max_{\eta \in \mathrm{H}} K(\eta) = \left\{ \eta \in \mathrm{H} \middle| \forall \nu \in \mathrm{H},\ K(\eta) \geq K(\nu) \right\}. \qquad (1)$$

Проведемо тепер ідентифікацію моделі ІТС згідно з наведеною в [1, 5] класифікацією моделей активних систем.

15. Склад системи є сукупністю керуючого центра і активних елементів. Залежно від класифікації ІТС згідно з [6] модель активної системи може бути або одно-, або багатоелементною.
16. Структура системи є сукупністю інформаційних, керуючих та інших зв'язків між учасниками активної системи, включаючи відношення підпорядкованості і розподіл прав прийняття рішень. За типом структури активні системи можуть поділятися на дворівневі (один керуючий орган і один або декілька підпорядкованих йому керованих об'єктів – активних елементів), трирівневі і т. і. За типом підпорядкованості активні системи поділяються на системи з унітарним контролем (віялоподібного типу, коли кожний активний елемент підпорядковується одному і тільки одному керуючому органу) та з розподіленим контролем (активний елемент може бути одночасно підпорядкований декільком

керуючим центрам). Самі ж активні елементи можуть бути незалежними або мати слабкі чи сильні зв'язки.

17. Щодо порядку функціонування активної системи, то він може бути стандартним чи нестандартним. У визначенні базової моделі активної системи [1] встановлений стандартний порядок функціонування.
18. За числом періодів функціонування активні системи можуть бути статичними (учасники здійснюють вибір стратегій одноразово) і динамічними. Останні, залежно від взаємозв'язків періодів функціонування та ступенів врахування учасниками впливу наслідків рішень, що приймаються, на подальше функціонування системи, можуть розділятися на активні системи з далекоглядними і недалекоглядними активними елементами, адаптивні і неадаптивні, тощо.
19. Цільові функції (інтереси учасників) впливають на тип задачі, що постає: стимулювання, планування чи інші типи.
20. Припустимі множини є незалежними або взаємозалежними множинами можливих виборів станів учасників. За розмірністю простору індивідуальних станів активних елементів активні системи можуть поділятися на системи зі скалярними або векторними уподобаннями активних елементів.
21. За ступенем інформованості учасників активні системи можуть поділятися на системи з симетричною і асиметричною інформованістю. Також можуть бути детерміновані та індетерміновані активні системи. Щодо типу невизначеності, то вона може бути внутрішньою (відносно параметрів самої системи), зовнішньою (відносно параметрів зовнішнього середовища) або змішаною. За видом невизначеність може бути інтервальною (учаснику відома множина можливих значень невизначеного параметру), ймовірнісною (відомий розподіл ймовірностей), нечіткою (відома функція приналежності), а також мішаною. Принципи поведінки учасників також можуть бути різними: використання максимального гарантованого результату, очікуваних корисностей, максимально недомінованих альтернатив, повідомлення інформації, тощо.

Розглянемо багатокористувацьку ІТС, модель якої визначено в [3]. Згідно з наведеною класифікацією, модель ІТС є:

- багатоелементною з незв'язаними активними елементами; в даному випадку припускаємо, що користувачі ІТС діють незалежно один від одного;
- дворівневою з унітарним контролем; припускаємо, що керуючим центром виступає суперкористувач або доглядач ІТС, що формує політику безпеки в системі і поширює її на активні елементи;
- динамічною з далекоглядними активними елементами; в даному випадку природним є для користувачів змінювати свої уподобання протягом життєвого циклу системи; припускаємо також, що реакція керуючого центру (штраф чи стимулювання) на прояв стратегій активних елементів враховується активними елементами в процесі коригування уподобань;
- зі стандартним порядком функціонування;
- з векторними уподобаннями активних елементів;
- з асиметричною інформованістю, оскільки природним є те, що керуючий центр має більше інформації про активну систему, ніж елементи, що знаходяться на нижчому рівні ієрархії;
- індетермінованою зі змішаною невизначеністю, як в сенсі типу, так і виду невизначеності, тобто активні елементи (користувачі) мають і внутрішню, і зовнішню невизначеність, а теоретична невизначеність параметрів може бути як інтервальна, так і ймовірнісна і нечітка, залежно від умов функціонування ІТС.

Щодо принципу поведінки учасників, то метод максимального гарантованого результату логічно не вписується в рамки задач функціонування ІТС, оскільки в такому разі активний елемент вважає, що внаслідок функціонування системи реалізується найгірша для нього обстановка. Керуючий центр при цьому розраховує на найгірший для нього вибір активного елемента. На противагу методу максимального гарантованого результату є гіпотеза доброзичливості, згідно з якою центр вважає, що активні елементи обирають з множини розв'язків найбільш прийнятні для центра дії.

Нехай $y = (y_1, y_2, ..., y_n) \in \mathrm{Y} = \prod_{i=1}^{n} \mathrm{Y}_i$ – вектор дій активних елементів, компоненти яких вони можуть обирати незалежно (згідно з гіпотезою незалежної поведінки). В результаті вибору дії $y \in \mathbf{Y}$ під впливом обстановки (сукупності факторів, що формуються під впливом інших активних елементів, керуючого центра, зовнішнього середовища) реалізується результат діяльності активного елемента $z \in \mathbf{Y}_0$, де $\mathbf{Y}_0$ – множина можливих результатів діяльності. Запровадивши поняття функції корисності $u: \mathrm{Y}_0 \to \mathrm{R}^1$, що співставляє результату діяльності певну цінність, виражену дійсним числом, та цільової функції, що задає уподобання елементу на множині його дії, можна аналізувати поведінку того чи іншого елемента як

окремо, так і в контексті роботи всієї системи. Якщо взяти за цільову функцію центру забезпечення максимального рівня захищеності, що, зокрема, може мати ймовірнісний характер, з'являється можливість стимулювання діяльності активних елементів, фактично здійснюючи керуючий вплив на забезпечення захисту інформації в ІТС. Структурну схему системи наведено на рисунку.

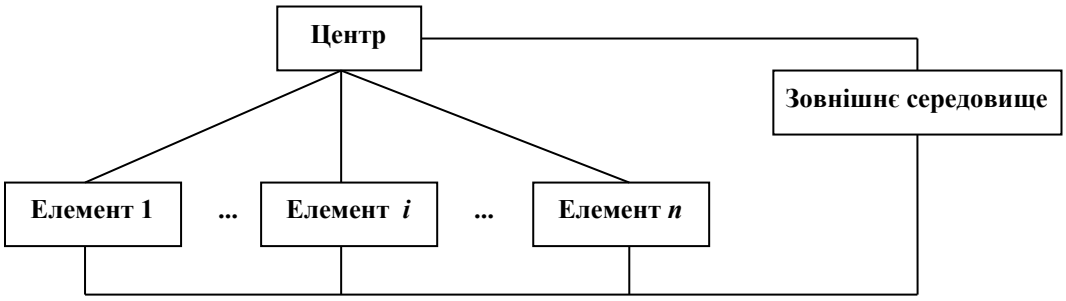

Рисунок – Структурна схема дворівневої організаційної системи

IV Висновки

В рамках представлення моделі ІТС як моделі активної організаційної системи отримані властивості моделі на основі класифікації моделей активних систем. Дані результати дозволяють використовувати відомі методи керування організаційними системами, в тому числі з урахуванням отриманих властивостей. Таким чином, на початковому етапі дослідження вже можна вести мову про застосовність теорії функціонування організаційних систем до вирішення задач керування захистом інформації в ІТС.

*Література: **1**. Новиков Д. А., Петраков С. Н. Курс теории активных систем. – М.: Синтег, 1999. – 104 с. **2**. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с. **3**. Антонюк А. О., Жора В. В. Використання доказового методу для проектування та оцінки рівня захищеності інформаційно-телекомунікаційної системи. // Пробл. программирования. – 2007. - №3 (у друці). **4**. Бурков В. Н., Кондратьев В. В. Механизмы функционирования организационных систем. – М.: Наука, Главная редакция физико-математической литературы, 1981. – 384 с. **5**. Бурков В. Н., Новиков Д. А. Теория активных систем: состояние и перспективы. - М.: Синтег, 1999. – 128 с. **6**. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.*