7.3. Налаштувати ці обмеження.

V Висновки

Результати виконаних досліджень і розроблена утиліта після можливої сертифікації (або отримання позитивного експертного висновку) дозволять, по-перше, в процесі створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах державних організацій застосувати на практиці рекомендації з конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2, і по-друге, в процесі контрольно–інспекційної роботи здійснювати перевірку параметрів безпеки ОС Microsoft Windows XP Professional SP2.

*Література: **1**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Експертний висновок. **2**. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. **3**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Інсталяція об'єкта експертизи та конфігурування параметрів безпеки. **4**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Технічні вимоги. **5**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Ідентифікація об'єкта експертизи під час проведення періодичних перевірок стану захищеності. Рекомендації. **6**. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2 (шифр – «Експертиза WXP_SP2»). Оновлення інстальованого програмного забезпечення об'єкта експертизи. Рекомендації.*

УДК 681.5:621.391

ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДКРИТИХ СИСТЕМ. Частина 2. ВЛАСТИВОСТІ ВІДКРИТИХ СИСТЕМ ТА ВИМОГИ ДО ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ

Володимир Кононович, Ірина Кононович*, Тетяна Тардаскіна**
*Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком", *Інститут комп'ютерних технологій ОДАХ, **Одеська національна академія зв'язку*

Анотація: **Аналізуються новітні науково-технічні досягнення у області інформатики, інформаційних технологій та виводяться основні принципи інформаційної безпеки відкритих систем, що характеризуються інтелектульним управлінням й активною взаємодією з іншими системами. Виявляються властивості відкритих систем та формульються вимоги до інтелектуального управління з точки зору їх інформаційної безпеки.**
Summary: **The newest scientific-technical achievements in informatics, information technologies and main principles of information security open systems, which characterized intellectual control and active interaction with other systems, are analyzed. Properties of open system are defined are formulated for intellectual control of them from the point of view of their information security.**
Ключові слова: **Інформаційна безпека, відкриті системи, інформодинаміка, інформатика, система управління, інтелектуальне управління, числення предикатів.**

I Вступ

Дане дослідження стосується сфери технічного захисту інформації та інформаційної безпеки систем, які об'єднуються під загальною назвою – інформаційні технології. Проблематика дослідження, аналіз досягнень та публікацій наведені в частині 1 цієї роботи [1]. *Аналіз останніх досягнень і публікацій* показує, що моделі системи процесів захисту інформації [2], інформації, як управління процесами відкритих систем, теорії інформодинаміки [3], та керованості й спостережності систем у сучасній теорії управління [4] мають дещо суттєве-спільне, що вимагає уважного дослідження. Відкриті системи існують лише як процес. Ізоляція відкритої системи від зовнішніх взаємодій приводить до її деградації. Нова парадигма інформаційної безпеки, що розвивається в США, розглядає інформаційні системи як принципово відкриті, де синергетика гомеостазу (стану усталеної рівноваги) визначається балансом

ентропії (мірою невизначеності) зовнішнього середовища та запасом живучості елементів [5]. Самоорганізація, яка властива відкритим системам, є однією з обов'язкових вимог до багатьох сучасних систем, наприклад, до сенсорних мереж, застосовуваних у телебіометриці, або до мереж типу «інформаційної матриці» [6]. Ряд інших властивостей відкритої системи, які слід вважати належними до сфери безпеки, органічно присутні у відкритих системах. Аналіз, систематизація цих властивостей відкритих систем та вдосконалення відповідної теорії та технології інформаційної безпеки є актуальною задачею.

Мета даної частини роботи: в рамках загальної мети – вироблення науково-методичних основ системи інформаційної безпеки відкритих систем – на основі аналізу й систематизації органічно присутніх у відкритих системах аспектів інформаційної безпеки сформулювати цілі інформаційної безпеки відкритих систем, визначити вимоги до інтелектуального управління з позицій інформаційної безпеки, продовжити уточнення практичних аспектів теоретико-інформаційних методів оцінки властивостей інформації та відкритих систем стосовно інформаційної безпеки.

Постановка задачі. З практики відомо, що погано запроектована система захисту інформації споживає ресурси системи, зменшує швидкість обробки інформації, вносить незручності користування нею, обмежує доступні функції й процедури, понижує ефективність функціонування системи і, в цілому, являє собою дещо обмежену закриту систему. Новий підхід до поняття відкритої системи співпадає з новими підходами до процесів та теорії інформаційної безпеки [2, 5] і дозволяє наблизитись до реального одночасного проектування системи управління відкритою системою та системою її інформаційної безпеки, більш органічно вбудувати їх у створювану відкриту систему. Тому будемо послідовно вирішувати наступні задачі, об'єднані поставленою метою: висвітлити принципові структурні властивості відкритих систем; прояснити роль інтелектуального управління в цих системах та їх органічну єдність з процесами забезпечення безпеки; сформулювати цілі інформаційної безпеки; сформулювати вимоги до системи інтелектуального управління з позицій інформаційної безпеки; намітити шляхи до створення технології й архітектури інформаційної безпеки відкритих систем та побудови системи інформаційної безпеки на законах функціонування відкритих систем.

II Структурні властивості відкритих систем

Даний розділ є продовженням розгляду загальних властивостей відкритих систем. Дамо короткий огляд принципових структурних властивостей відкритих систем, які детально висвітлені й обґрунтовані у монографії В. М. Лачинова і А. О. Полякова [3]. Але всі властивості будемо розглядати під кутом зору процесів забезпечення інформаційної безпеки.

Перш за все, слідом за авторами монографії, будемо вважати терміни «системно-складні об'єкти», «інтелектуальні системи», «відкриті системи», «надкібернентичні системи» синонімами. Відкриті системи володіють властивостями самоорганізації та інтелекту (розуму). Під інтелектом, у даному випадку, розуміється здатність мислення, раціонального пізнання, яке реалізується в процесі взаємодії у трійці: *суб'єкт – управляюча дія – об'єкт*, або, у загальному випадку, в послідовності *суб'єкт – управляюча дія – суб'єкт – управляюча дія ... – об'єкт*. Назвемо таку взаємодію *суб'єктно-об'єктною взаємодією*. Інтелектуальна система «інженерно» виникає лише тоді, коли в процесі пізнання суб'єкт і об'єкт періодично міняються місцями: суб'єкт переходить у стан об'єкту, а об'єкт стає відповідаючим джерелом активності – суб'єктом. Безперервно необхідне підтвердження – суб'єкт повинен ставати об'єктом для сприйняття правильності контекстного розуміння його повідомлення. Для планування наступної команди необхідно, як мінімум, бути впевненим у правильному контекстному розумінні попередньої. Інтелектуальна система подібна генератору, який виробляє управляючу інформацію.

Поняття відкритої системи, процитоване у частині 1 цієї роботи, відрізняється від класичного визначення системи тим, що воно враховує важливу роль в існуванні відкритої системи взаємодії з оточуючим середовищем. Відкрита система безперервно взаємодіє зі своїм оточенням. Взаємодія забезпечується як у силовій формі, так і у „несиловій" інформаційній формі. Більше того, відкрита система існує як безперервний процес взаємодії. Сприйняття відкритої системи можливе на основі технологічних правил цього процесу. Це віддалено нагадує процес виконання комп'ютерної програми, який перетворює комп'ютер у функціонуючу автоматизовану систему.

Відкрита система взаємодіє із зовнішнім оточенням, обмінюючись інформацією, енергією, матеріальними об'єктами. Безпека взаємодії складається із взаємопов'язаних між собою інформаційної безпеки, енергетичної безпеки, фізичної безпеки тощо. В процесі взаємодії з інформаційних, енергетичних, матеріальних потоків мають обиратися ті, які відповідають цільовій функціональності існування відкритої системи.

Відкриті системи мають органічно притаманні їм властивості самозберігаємості, самоорганізації, саморозвитку та інтелекту. Самозберігання, як буде показано далі, є однією з цілей і забезпечується самим принципом інтелектуального управління у відкритій системі. Властивість самоорганізації проявляється у процесі еволюції відкритої системи як процесу. Еволюція системи має бути керована у «критичних точках», зокрема у початковій точці при пуску системи. Цільова не спонтанна самоорганізація є однією з обов'язкових вимог до багатьох сучасних систем. Властивість саморозвитку забезпечує системам можливість адаптуватись до змін у зовнішньому середовищі. Вважається, що цілі існування штучних відкритих систем знаходяться поза цими системами. Інколи їх не можна чітко сформулювати. Саморозвиток може стати можливим тоді, коли цілі існування формулюються («усвідомлюються») самою відкритою системою.

Дані властивості, при їх розгляді під кутом зору забезпечення інформаційної безпеки відкритої системи, ставлять проблеми і умови постійної керованості, спостережності, а також повсюдності цих властивостей для тотожності визначення контексту в однакових умовах. Основу інформаційної безпеки відкритих систем складає умова спостережності всіх систем, явищ, процесів або об'єктів.

Відкриті системи описуються за допомогою контекстно-залежної мови. Тому, по перше, відкриті системи моделювати не можна, а по А. Колмогорову [7], складні системи не можна моделювати інакше, як повторивши усю історію їх виникнення. А по друге, необхідна якість управління системно-складними об'єктами може бути досягнута лише за рахунок використання контекстно-залежних мов їх представлення та системи управління, яка працює з такими мовами. Управління, в загальному випадку повинне починатись з попередньої оцінки об'єкта, який управляється, і вибору мови управління, яка відповідає об'єкту. Для замкнутих об'єктів ці мови мають математичну або алгоритмічну реалізацію. Для відкритих систем, при збереженні досить високого рівня своєї комунікативної функції відносно оточення, мови описання і управління стають контекстно залежними.

Нагадаємо, що контекст – це локалізована у просторі і часі сукупність висловлювань й термінів, які визначають поточні значення термінів або їх сукупностей. Контекстуальне визначення будується на знанні зв'язків визначуваного з поточним контекстом. Контекстно-залежна мова – це мова, смисл будь-якої послідовності речень якої може бути залежним від попереднього висловлювання цією мовою.

Відкрита система на сьогодні може бути побудована двома способами: на базі класичної машини фон нейманівської архітектури з контекстно залежною мовою; і на базі машин, побудованих за принципами теорії інформодинаміки, які здатні самостійно конструювати структури даних і свою загальну структуру.

В першому варіанті є можливість представлення контекстно-залежної проблемно-орієнтованої мови механізмом числення предикатів на основі алгебри змінюваних відношень. Для ілюстрації тут розглянемо принципи конструювання проблемно-орієнтованої мови із властивостями контекстної залежності на базі числення предикатів. Проблемно-орієнтована мова може забезпечити узгоджене сприймання та передачу інформації при організації управління мовою, яка володіє найбільшою комунікативною здатністю.

Числення предикатів засноване на формальній системі, якою називається скінченна множина символів, які називаються формулами та термами, і скінченна множина правил оперування цими символами. Числення предикатів опирається на численні висловлювання, які розчленовані на суб'єкт і предикат. Поняття формалізованої системи для цілей контекстної залежності визначається так: $M = (T, P, A, F, D)$, де перших чотири складові в дужках входять у класичне визначення формалізованої системи: T – множина базових елементів; P – множина синтаксичних правил, необхідних для побудови із T синтаксично правильних висловлювань; A – множина апріорно правильних висловлювань; F – семантичні правила виведення; а остання вводиться для отримання контекстної залежності: D – множина допустимих контекстів, які визначають поточну (змінну) логіку базових домовленостей.

На базі такого розширення поняття формалізованої системи можна побудувати проблемно-орієнтовану мову предметної області, яка заснована на використанні предикатів. Мова складається з дескрипторного словника й синтаксису, певної структури описання з довільного набору висловлювань (простих синтагм, предикатних форм) стандартного вигляду $A\boldsymbol{R}B$, де – A і B терми, $\boldsymbol{R}$ – відношення, яке відображає взаємовідносини явищ, об'єктів, прикмет у реальні дійсності.

У відкритих системах здійснено перехід від функціональних моделей систем, заданих мовою передаточних функцій, до реальних систем у їх зовнішньому оточенні, доступних нам без втрат лише на мові, рівень складності якої забезпечує їх понятійну взаємодію із «зовнішнім управителем» та ідентифікацію семантики їх взаємодії із зовнішнім світом.

Авторами теорії структурної узгодженості сформульовані гіпотези відносно управління контекстно-залежними мовами. Подамо ці гіпотези під кутом зору інформаційної безпеки.

Гіпотеза А. Все, що необхідно знати для системи інтелектуального управління та для системи інформаційної безпеки, може бути виражено у вигляді сукупності текстів звичайною природною мовою.

Іншими словами, всі відомості про об'єкт управління та систему інформаційної безпеки, цілях їх існування, критеріях управління й безпеки та множина можливих рішень з управління та інформаційної безпеки можуть бути повідомлені системі управління та інформаційної безпеки у вигляді послідовності фраз, написаних природною мовою.

Гіпотеза Б. Система управління відкритих систем не може бути замкнутою, тому процеси управління та інформаційної безпеки мають використовувати не математичні й математико-лінгвістичні, а структурно-динамічні й семантичні характеристики інформаційних потоків. Справедливість цих гіпотез буде видно при розгляді парадигми інтелектуального управління.

Відкриті системи можуть бути створені за допомогою технології конструювання відкритих систем, якою виступає теорія структурної узгодженості. У основу теорії структурної узгодженості покладено природно існуючий принцип взаємодії всього з усім – аксіома відкритості, яка узагальнює три властивості реального світу: квантованість (дискретність) Світу, узагальнений закон збереженості, принцип доповнюваності (компліментарності). Теорія структурної узгодженості встановлює ті загальні закони (правила), які непорушні для всіх без винятку систем, що володіють здатністю існувати в режимі активної взаємодії з оточуючим світом, властивостями самоорганізації та інтелекту (розуму). Єдина умова, важлива також з точки зору інформаційної безпеки, – це спостережність і повсюдність властивостей як тотожність визначення контексту в однакових умовах.

Перейдемо до аналізу парадигми інтелектуального управління та її методологічного зв'язку з парадигмою інформаційної безпеки.

III Взаємозв'язок процесів інформаційної безпеки та управління відкритих систем

Відкриту систему можна представити як сукупність декількох підсистем A, B, C, інформаційно зв'язаних з деякими серверами, їх базами і які користуються їх обчислювальними потужностями (рис. 1). Підсистеми зв'язані між собою інформаційними потоками I_{ij}, які замикаються через підсистему D з динамічною реконфігурацією структурних зв'язків. З оточуючим середовищем взаємодія відбувається через шумові F_k і керуючі (командні) F_y інформаційні потоки. Точка підключення кожного користувача або окремої автоматизованої системи до інформаційного середовища оформлюється в вигляді термінала – робочого місця, яке має програмне забезпечення, що базується на нормативно-правовій та нормативно-методичній інформації та визначає права доступу до інформаційних ресурсів.

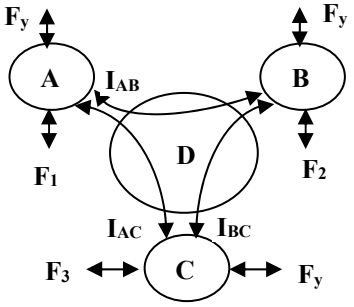

Рисунок 1 – Структура відкритих систем

Для прийняття рішень щодо управління та захисту необхідна інформація про інформацію, тобто метаінформація, або відомості, які характеризують динаміку інформаційної взаємодії. Мають бути враховані параметри, які характеризують інформаційні потоки: об'єми за одиницю часу, адресація і напрям, швидкість обробки, ідентифікація та персоніфікація джерела та обробника, тощо, які характеризують конкретику ситуації. Про підсистему треба мати всі прямі і контекстні відомості щодо поточного стану підсистеми, фактів і динаміки отримання або передачі інформації чи матеріальних об'єктів, тощо. Внутрішня семантика інформації потрібна також при прийнятті рішень щодо захисту.

Для управління відкритою системою та забезпечення безпеки необхідно створити систему роботи з інформацією у вигляді структури взаємодії управляючої системи (і, зокрема, її підсистеми інформаційної безпеки) з об'єктом. Ця структура має забезпечити можливість накопичення і використання метаінформації для можливості прийняття рішень щодо управління і захисту. Остаточно нас цікавить забезпечення захищеного обміну. Мають контролюватись процеси, які можуть привести систему до саморуйнування або до стану, близького до такого, при якому стає неможливим виконання функцій системи. Якщо попередити таке руйнування неможливо, то необхідно провести саморуйнування

(реструктуризацію) у «безпечній формі». Тим самим мають забезпечуватись замикання інформаційних потоків джерел і споживачів інформації всередині об'єкта, а також, у можливій степені потоків взаємодії з зовнішнім середовищем, через деяке контрольне середовище (підсистему *D* на рис. 1), яке виконує функції контролю та семантичного аналізу всіх інформаційних потоків, та стає єдиним дозволеним каналом для обміну інформацією і невід'ємною частиною об'єкта.

Це означає, що у контрольному середовищі постійно працює програма адресного збору інформації динамічних характеристик потоків інформації і характеристик захищеності та безпеки інформації. Кожна підсистема повністю і постійно відслідковується за цими характеристиками. Будь-яка зміна динаміки і семантики інформаційних потоків, які не передбачені технологією роботи, має генерувати сигнал для початку вироблення управляючих та захисних рішень. Саме таке повне і постійне слідкування за характеристиками усіх інформаційних потоків не реалізоване у сучасних комп'ютерних системах, які класифікуються як автоматизовані або інформаційно-телекомунікаційні системи. Це зумовлює нескінченну множину вразливостей, які продовжують експлуатувати зловмисники.

Витрати на додаткову обробку інформації можуть бути значними, але тільки вони дають контекстну інформацію, необхідну для досягнення безпечного інтелектуального управління. В безпечній інтелектуальній системі управління наявна практично вся інформація, яка може бути зібрана і використана при автоматичному прийнятті управлінських та захисних рішень. При цьому характеристики динаміки вже дають спостережність системи та інформаційного продукту, який вона виробляє. Система інформаційної безпеки вимагає визначення діапазонів свого стану стійкості, набору дозволених станів, частотних, статичних і динамічних оцінок. Повноцінний захист відкритої системи забезпечується завдяки вбудованому перехопленню й контролю всіх інформаційних потоків.

Врахування динаміки інформаційних потоків необхідне за двома базовими складовими: інформації-продукту та інформації-сировини. Інформація-продукт виробляється в підсистемі, наприклад, на робочому місці оператора, і має цінність новизни. Інформація-сировина та команди споживаються від джерел наявної інформації і служать для вироблення нової інформації. Тут потрібна також інформація про інформацію. Крім базових інформаційних потоків необхідно виділяти інформацію, яка регламентує зміст цих потоків з точки зору управління та безпеки. Для надійного захисту інформаційного середовища, яке має цінність для системи, від шумового впливу програмне забезпечення робочих місць має проводити фільтрацію потоків інформації як за внутрішньою не суперечливістю, так і на узгодженість з наявною інформацією, використовуючи методи семантичного аналізу.

У відкритій системі управління може бути лише інтелектуальним і може здійснюватись за допомогою інтелектуальних інформаційних баз. Управління – це посилання повідомлень, які ефективно впливають на поведінку керованої системи. Інтелектуальна система управління – це система управління, яка заснована на виробленні, структуризації та обміні інформацією. У свою чергу, інтелектуальна база управління – це активна система оцінювання результатів, яка основана на двохсторонній контекстуальній взаємодії.

Інтелектуальна база складається з машини бази даних, машини бази знань та системи управління. Машина баз знань – це механізм забезпечення управління для відкритих систем, орієнтований на практичну задачу сприйняття семантики інформації як управління з урахуванням всіх необхідних умов контекстного аналізу та реструктуризації зв'язків при роботі зі знаннями. У машині бази знань вхідна інформація є і управлінням і, одночасно, командою для організації дій з її обробки. Тут алгоритм задано в оброблюваному контекстно залежному записі. Процес управління організується на інформаційних потоках взаємодії з навколишнім оточенням з використанням структурно-динамічних і семантичних характеристик інформаційних потоків.

Формулювання «управління на потоках даних» означає, що потоки даних містять у собі деякі структури, виявлення, ідентифікація і правильне використання яких дозволяє машині баз знань мати властивість до самоструктурування і самоорганізації. В [3] висловлюється припущення щодо існування загальних законів взаємодії структур, які охоплюють не лише фізичні та енергетичні явища, а й інформаційні явища. Система інформаційної безпеки накладає на систему обмеження в ресурсах, виконуваних функціях, швидкодії. Класична система інформаційної безпеки робить систему, що захищається, закритою, що знижує її ефективність. Задача полягає в максимальному збереженні можливостей взаємодії з оточуючим середовищем і ефективності свого функціонування в умовах взаємодії з навколишнім оточенням, тобто побудувати систему інформаційної безпеки на законах функціонування відкритих систем, зберігаючи і не зменшуючи ефективність функціонування і зберігаючи необхідну свободу взаємодії. Захист інформації як і управління треба проводити на самому інформаційному потоці взаємодії з навколишнім оточенням. Забезпечення безпеки проводиться в процесі управління, коли в системі, що управляється, треба відчути направлений і «розумний з її точки зору» опір керованого об'єкта, треба одержати які-небудь підтвердження факту освоєння нею отриманої інформації і деякі гарантії

правильності, з точки зору управителя, її засвоєння.

Для знаходження місця процесам забезпечення інформаційної безпеки в інтелектуальній системі корисно врахувати відому теорію ієрархії потреб Маслоу, відповідно до якої усі потреби інтелектуальної системи може бути подано у вигляді піраміди (рис. 2): фізіологічні, безпеки, причетності, визнання, самовираження.

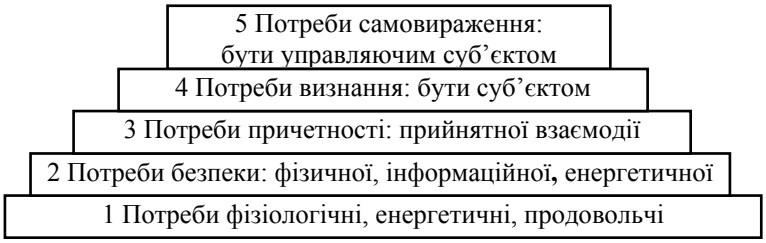

Рисунок 2 – Ієрархія потреб згідно з теорією Маслоу

З позицій теорії відкритих систем цю піраміду потреб можна коментувати таким чином. Перш за все повинні забезпечуватись потреби фізіологічні: енергетичні, продовольчі тощо. Потреби другого рівня піраміди пов'язані з бажанням та прагненням суб'єктів до стабільного й безпечного стану: фізичної, енергетичної, інформаційної безпеки. Після задоволення первинних потреб першого та другого рівня у суб'єкта виникає необхідність у задоволенні потреб причетності, прийнятної взаємодії з навколишнім середовищем. Потреби визнання реалізуються у взаємодії з іншими суб'єктами, які можуть виступати об'єктами і управляючими суб'єктами. П'ятий рівень ієрархії потреб можна трактувати як потребу виконувати функції управляючого суб'єкта.

З теорії потреб Маслоу випливає, що процеси забезпечення безпеки є однією з пріоритетних задач системи інтелектуального управління. Звідси ж випливає також ієрархічність системи інтелектуального управління. На задоволення потреб кожного рівня потрібен відповідний контур управління. Мінімальна кількість контурів управління становить чотири, якщо об'єднати контури, близькі за функціями й цілями. Процеси безпеки мають реалізуватись кожним рівнем інтелектуального управління, при цьому пріоритет належить першим контурам управління.

Тепер можна почати формулювати цілі інформаційної безпеки відкритої системи. У сфері захисту інформації такі цілі визначені новою парадигмою інформаційної безпеки інформаційних систем [6]. У цій парадигмі для повноцінної роботи або збереження мінімального набору критично важливих функцій система має володіти цілком визначеним запасом стійкості до зовнішніх дестабілізуючих впливів середовища. При цьому, порушення цілісності системи на фоні зниження активності її елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, а зниження живучості і порушення цілісності системи – втрату найважливіших функцій.

Тут виявляється принципова схожість цілей безпеки й управління у відкритих системах. Дійсно, інтелектуальне управління у відкритих системах направлене на підтримання стійкого стану знаходження системи на гомеокінетичному плато. Згідно з теорією інтелектуального управління самозберігаємість відкритої системи забезпечується самим принципом інтелектуального управління.

У відкритій системі існують не менш ніж три «управління»: внутрішнє, зовнішнє і компенсація не прогнозованих впливів зовнішнього світу (рис. 3). Три цикли управління мають таке призначення: I – управління для підтримання гомеокінетичної стабільності системи як деякий процес «внутрішнього переосмислення», внутрішньої реструктуризації, зміни цільових установок, зміни в процесі аналізу власної внутрішньої структури; II – управління для компенсації збурень F_k від зовнішнього світу; III – зовнішнє управління, як цілеспрямована дія F_y деякої зовнішньої системи, яка в даний момент виступає як суб'єкт. Всі ці управління реалізуються як однотипні на основі парадигми узгодження структури зв'язків даних і в повній логічній схемі передбачаються відповідно три цикли, три процедури суб'єктно-об'єктної взаємодії, які відповідають особливостям і смислу вказаних процесів управління.

Відповідно до поділу управління в інтелектуальній системі на внутрішнє, зовнішнє та компенсацію не прогнозованих впливів зовнішнього світу система забезпечення інформаційної безпеки відкритої системи теж має складатись не менш ніж з трьох процесів, цілі і механізми дії яких можуть відрізнятись.

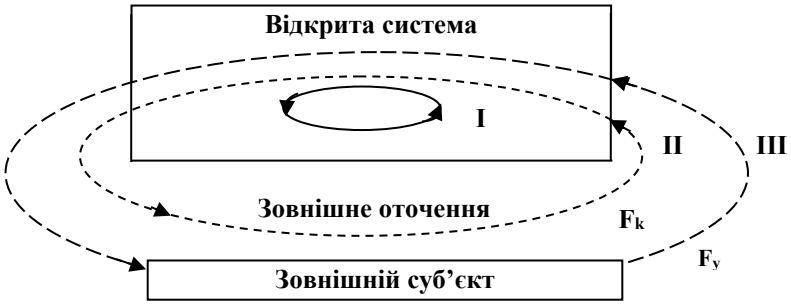

Рисунок 3 – Цикли управління відкритих систем

Найбільш складним щодо управління, безпеки і небезпечним для існування системи є зовнішнє управління. Поставити фільтр на вході зовнішнього інформаційного потоку буває важко, бо засоби семантичного аналізу та інші механізми прийняття рішень знаходяться далі у середині системи. Тому зовнішнє управління завжди має сприйматись через порівняння наявної структури з тією, яка повинна виникнути при позитивній реакції на управління. Конечна структура має бути «осмислена» через сприйняття накопиченого образу та логічних висновків щодо безпеки наслідків пропонованої реструктуризації даних. Відкрита система не має сприймати «самовбивчі» для неї команди. При виробленні логічних висновків із можливих наслідків запропонованої реструктуризації даних результат має попередити можливі катастрофічні наслідки.

Складною є також компенсація збурень за рахунок збурень від зовнішнього світу. Вони проявляються через зміну динаміки інформаційних потоків в об'єкті, що управляється. Компенсація зовнішніх збурень можлива, здебільшого, лише за рахунок розімкнутої системи управління. Дійсно, відновлення динаміки інформаційного потоку, необхідне для повернення об'єкта в усталений стан, можливе лише за рахунок перебудови його структури, зміни внутрішніх відносин між підсистемами, а вже потім, за рахунок впливу на зовнішній світ.

На рис. 4 наведені ілюстративні зображення гомеокінетичного плато для кібернетичних (закритих, рис. 4 а) і для відкритих (над кібернетичних, рис. 4 б) систем. *Гомео* – означає постійний. В біології *гомеостазом* називають набір взаємозв'язаних правил поведінки системи для підтримання її у стійкому стані. Під *усталеністю (стійкістю)* розуміється такий стан об'єкта, коли він справляється зі своїми функціями, зокрема, з функціями свого розвитку, а саме зі змінами в базі знань. Здатність системи залишатися в області стійкості називається *живучістю* системи. Всі системи високого рівня складності існують як процеси. В кожен момент часу вони знаходяться в стані нерівноваги – гомеокінезу. Для таких систем існує лише стан динамічної рівноваги, у якому вони намагаються втриматись.

У кібернетичних системах (рис. 4 а) усталеного стану замкнутої системи можна досягти, якщо використовувати негативний зворотний зв'язок – НЗЗ. У стані рівноваги НЗЗ сильніша за позитивний зворотний зв'язок – ПЗЗ і коливання в системі затухають. Поза областю між двома границями B_1, B_2 ПЗЗ сильніша НЗЗ, результуючий зворотний зв'язок позитивний, що веде до нестабільності і можливого руйнування системи. Лінія стабільної рівноваги між двома границями B_1, B_2 повинна мати деякий невеликий нахил. Рівновага досягається за рахунок постійного енергетичного підживлення. Процес вводу енергії в систему і процес обробки інформації має своєю метою зупинити тенденцію переходу системи у стан з більшою ентропією. По осям координат відкладаються конкретні фізичні величини. Прикладом може бути парова машина. Управляюча дія – це кількість палива, що згорає у топці. Якщо палива мало, то не утворюється пара і машина не здатна виконувати свої функції. Якщо палива надто багато, котел перегрівається і може вибухнути.

На рис. 4 б розглядається гомеокінетичне плато відносно інтелектуального управління. Управління динамікою інформаційних потоків та забезпечення безпеки передбачає безперервний контроль пересилок інформаційних потоків між підсистемами як за семантикою повідомлень, так і за темпами їх проходження та обробки. Такий контроль є необхідною складовою семантичного аналізу інформації в системі інформаційної безпеки і управління. Без цього частина семантики інформації буде втрачена, а направленість рішень з захисту і управління буде не відповідати цілям управління. Система зі зворотним зв'язком тут не підходить. Для вироблення прийнятних угод між суб'єктом і об'єктом у процесах захисту і управління необхідні структури даних і апарат узгодження структур даних. Кількісних оцінок тут не може бути, структурні перетворення у базах знань не характеризуються якоюсь метрикою.

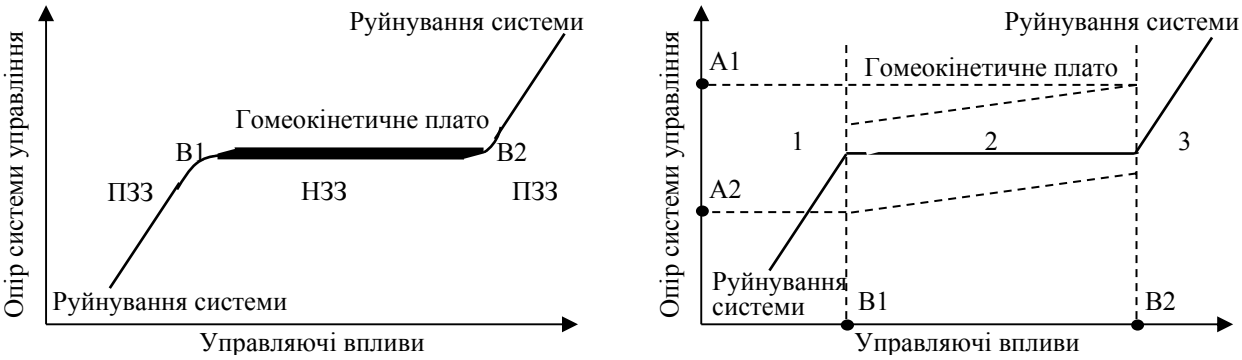

Рисунок 4 – Гомеокінетичне плато: а) кібернетичних систем; б) відкритих систем

По горизонталі на рис. 4 відкладається “величина” сумарного управляючого впливу на відкриту систему, яка складається із розузгодженості структур “знання – дані” в об’єкті й суб’єкті, що вноситься зовнішніми управляючими та збурюючими інформаційними потоками. По вертикалі відкладається аналогічна “величина” для внутрішнього управління станом системи в допустимих границях. Плато є деякою смугою, множиною станів, у яких може існувати система. Область 2 плато A_1, A_2, B_1, B_2 визначає діапазон можливих змін станів системи без її руйнування при сумарному вхідному впливові. Зліва від B_1 знаходиться область 1 руйнування системи при втраті нею “накопиченого досвіду”. Справа від B_2 знаходиться область 3, яку можна назвати перерегулюванням, коли зміни структури настільки великі, що це веде до зміни функціональних можливостей системи. Діапазон A_1-A_2 є ділянкою стабільності, при якій зберігаються цілі існування та функціональні можливості системи.

Для системи в структурі суб’єктно-об’єктної взаємодії гомеокінетичне плато існує як сукупність плато суб’єкта й об’єкта, які прагнуть до узгодженого існування, як область, де досягається узгодження структур суб’єкта й об’єкта. Якщо зовнішніх суб’єктів, які здійснюють управляючий вплив, декілька, то може бути множина гомеокінетичних плато, що характеризують кожну систему.

Таким чином, узагальнене інтелектуальне управління може бути визначене через його задачі: задачу стабілізації досягнутого стану, як внутрішню функцію певної внутрішньої реструктуризації системи, направлену на утримання системи на гомеокінетичному плато протягом максимально можливого часу; задачу переходу у новий стан, коли необхідно забезпечувати перехід системи з одного гомеокінетичного плато на інше або з однієї групи плато на деяку іншу групу; задачу забезпечення функцій, які відносяться до фізичної та інформаційної безпеки.

Для кожної системи існує оптимальне дозування управляючих впливів. Недостатнє управління може вивести систему у нестабільний стан з причини “зриву динаміки її існування”. У цьому випадку система немовби знаходиться у області дії “позитивного зворотного зв’язку”, який може привести систему до повного руйнування. Введення в систему надмірних управляючих впливів пригнічує смисл інтелектуального управління, веде до насильницької перебудови структур без процесу їх осмислення. У відкритих системах управління зв’язане зі змінами та перетвореннями структури інтелектуальної бази у циклі суб’єктно-об’єктної взаємодії. Гомеокінетичне плато є областю малих неузгодженостей та перетворень структур. Сильне управління прагне до радикального переводу системи в інший структурний стан, тобто на інше гомеокінетичне плато.

Можливі різні типи переходу до нових стабільних станів. Наприклад, перехід може мати гістерезисний характер, коли після одноразового «сильного» управляючого впливу, досягнувши точки A, система повертається не на попереднє плато 1, а починає існувати на новому плато 2 (рис. 5 a). Гістерезисний тип переходу може мати багаторівневий характер, при якому номер плато, на яке переходить система, залежить від інтенсивності одноразового управляючого впливу (рис. 5 b). Після досягнення точки A система переходить на плато 2, а після досягнення точки B – на плато 3. Послідовний характер переходу характерний тим, що при поступовому збільшенні інтенсивності управляючого впливу система послідовно переходить з плато 1 на плато 2, потім на плато 3 (рис. 5 c). Можна розглядати переходи «тригерного» типу. В них, при подачі управляючого впливу певної інтенсивності, система стрибком переходить на інше плато.

Реальна можливість визначення границь стійкості при роботі з інтелектуальними базами дозволяє використовувати ці границі для забезпечення необхідних реакцій з метою підтримки існування системи.

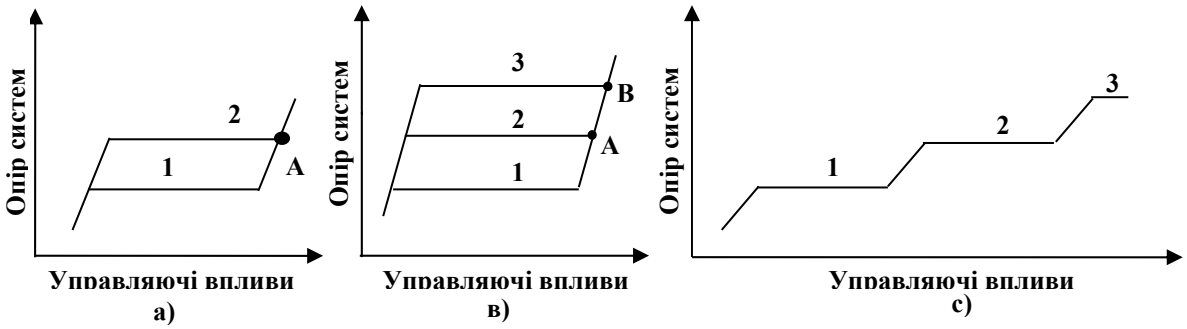

Рисунок 5 – Типи переходів відкритої системи на нові плато

Продовжимо аналіз структури інтелектуальної системи управління та розглянемо, які зміни треба внести до узагальненої функціональної структури інтелектуальної системи управління, наведеної в [3, рис.4. 4], для того, щоб в ній стала можливою реалізація процесу забезпечення інформаційної безпеки.

В інтелектуальній системі управління є система вводу та оцінки інформаційних потоків для сприйняття зовнішніх управляючих повідомлень і повідомлень із зовнішнього світу. Вихідним потоком інформації треба вважати конечний стан зв'язків даних, які встановлюються у інтелектуальній базі після всіх структурних узгоджень і перетворень. Структури об'єкта в кожен момент часу є «вихідним сигналом» для обробки наступної або поточної інформаційної посилки. Для безпеки пріоритет завжди віддається внутрішньому управлінню, тобто підтриманню стабільності своєї структури. Реакцією інтелектуальної системи може бути відмова від виконання зовнішнього управління, або адекватна реакція на небезпечне управління, яке веде до втрати стабільного стану. Таким чином, наявна система інтелектуального управління вже передбачає механізми забезпечення стійкості існування самої системи, тобто її живучості та фізичної безпеки. Залишається вияснити питання забезпечення стабільності функціонального призначення системи з урахуванням вимог до інформаційної безпеки. Таку узагальнену функціональну структуру інтелектуальної системи управління та інформаційної безпеки представлено на рис. 6.

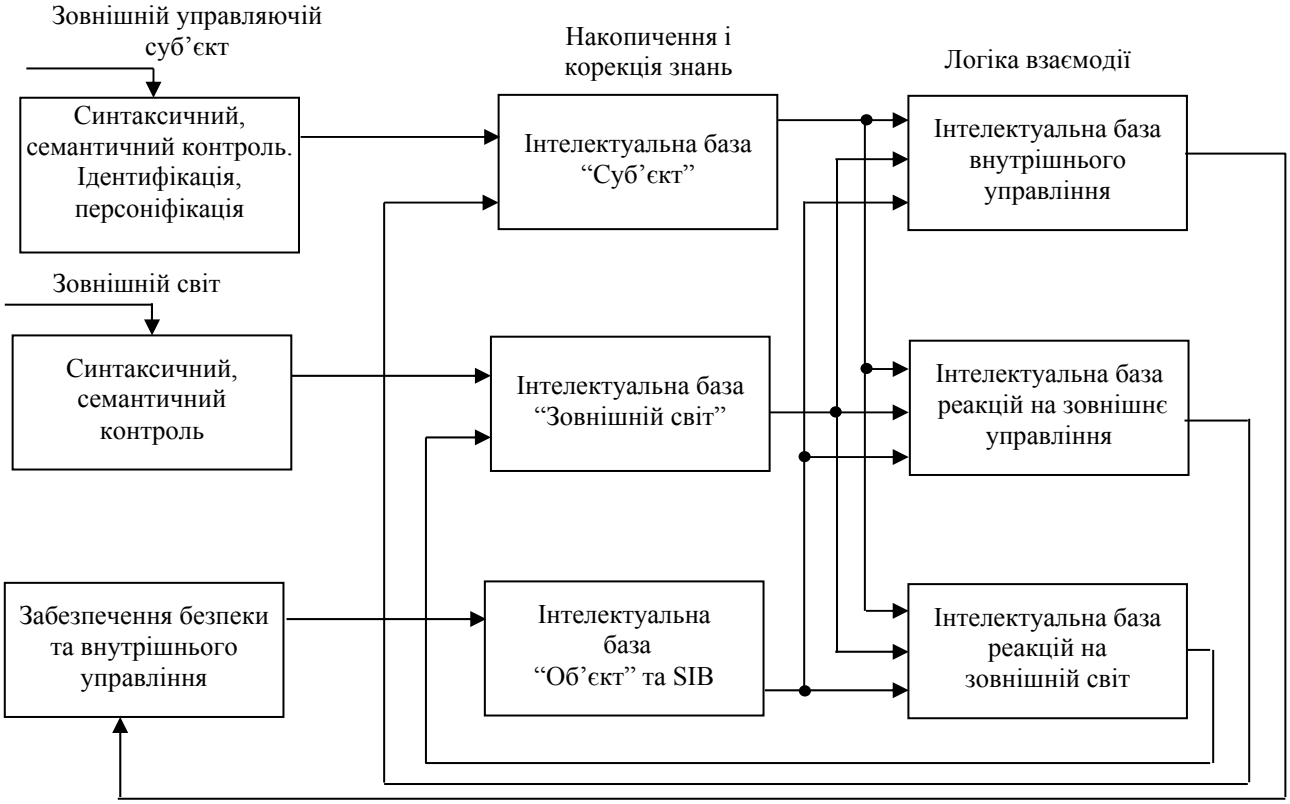

Рисунок 6 – Узагальнена функціональна (логічна) структура інтелектуального управління та забезпечення безпеки

Інтелектуальна система управління та безпеки повинна складатись не менше ніж із трьох здвоєних інтелектуальних баз, які відповідають управляючому суб'єкту, зовнішньому світу і об'єкту. Крім того, в ній присутні підсистеми, які приймають і контролюють інформаційні потоки від управляючого суб'єкта й зовнішнього світу, а також підсистема забезпечення безпеки та внутрішнього управління. Приймаючи інформаційні потоки від зовнішнього світу, відповідна підсистема забезпечує синтаксичний та семантичний контроль, а також ідентифікацію об'єктів зовнішнього світу. На базі цих інформаційних потоків формуються в інтелектуальній базі даних структури, які відповідають знанням, «образам» зовнішнього світу і які використовуються далі в контурі управління компенсацією впливів зовнішнього світу. Аналогічні процеси проходять з інформаційними потоками від управляючого суб'єкта, за винятком того, що додатково проводиться персоніфікація (автентифікація) суб'єкта.

Здвоєні інтелектуальні бази поділяються на ліву половину, де виконується накопичення і коригування знань, та праву половину, де зберігаються накопичені раніше знання (образи) та виробляються реакції на управління і впливи зовнішнього світу за допомогою логіки взаємодії. Логіка взаємодії побудована таким чином. Інтелектуальна база (ІБ) «Суб'єкт», прийнявши інформацію від зовнішнього управляючого суб'єкта негайно перебудовує всі свої зв'язки. Далі у правій половині ІБ «Суб'єкт» здійснюється порівняння наявної і нової структури для визначення збереження захищеності і стійкості системи, якщо вона згодна на таке управління. Аналогічно відбувається реструктуризація і контроль захищеності й стійкості в ланцюгу сприймання управління впливом від зовнішнього світу. Наслідки цього нецільового випадкового впливу менші й мають більшу невизначеність.

З метою забезпечення безпеки система ІБ «Об'єкт» ізольована від безпосередніх інформаційних потоків зовнішнього світу. Вона структурно залежить від прийнятого рішення і отримує нову інформацію лише в контурі внутрішнього управління після аналізу і вироблення реакції на зовнішні управління для утримання системи на гомеокінетичному плато. До складу інтелектуальної бази «Об'єкт» входить SIB – security information base (інформаційна база захисту), яка використовується в циклі контролю стану та управління безпекою.

Всі три половинки інтелектуальних баз приводяться до нової структури відповідно до вироблених рішень, які враховують всі структурні перетворення в ієрархії та відповідають вибраній політиці безпеки та управління. В решті решт, кожна з правих половинок інтелектуальних баз повідомляє лівій свій узгоджений стан і процес генерації нової інформації завершується, щоб початись далі спочатку.

IV Вимоги до управління у відкритій системі з точки зору інформаційної безпеки

Теорія і архітектура інформаційної безпеки відкритих систем повинна встановити загальні закони (правила) забезпечення інформаційної безпеки, непорушні для усіх без винятку систем, які здатні існувати в режимі активної взаємодії з оточуючим світом, володіють властивостями самоорганізації і інтелекту (розуму). Це не означає, що системи захисту не застосовуються «локально» в середині таких систем. Це означає побудову системи інформаційної безпеки об'єктів і систем інформаційної діяльності, яка в максимальній мірі не знижує ефективність функціонування останніх. Вимоги, що сформульовані нижче, мають попередній характер і будуть уточнюватись у наступних роботах при розробці загальної моделі інформаційної безпеки відкритих систем.

Цілі інформаційної безпеки, які співпадають з цілями інтелектуального управління. Виходячи з розглянутих властивостей відкритих систем та враховуючи нову парадигму інформаційної безпеки інформаційно-телекомунікаційних систем [5] цілі забезпечення інформаційної безпеки у відкритих системах можуть ставитись таким чином. Відкриті системи принципово повинні постійно взаємодіяти з оточуючим зовнішнім світом, у яке вони занурені, з метою адаптації до енергетичних та інформаційних потоків не рівноважного світу. Закриття системи, обмеження її зв'язків зменшує її можливості розвитку і може привести до деградації. Необхідно розробити систему інформаційної безпеки відкритої системи, яка забезпечила б інформаційно безпечне існування та розвиток відкритої системи в умовах взаємозв'язку з динамічними інформаційними процесами. Система інформаційної безпеки повинна забезпечити певний баланс між певною мірою закритості і збереженням можливостей для адаптації і розвитку. Збалансованість досягається забезпеченням стану стійкої рівноваги (гомеостазу) відкритої інформаційної системи, тобто балансу ентропії зовнішнього середовища та запасу живучості системи. У відкритій системі управління як процес повинно включати в себе процеси забезпечення інформаційної безпеки. Інтелектуальне управління слід перетворювати на безпечне інтелектуальне управління.

Принципи забезпечення інформаційної безпеки. А. Процеси забезпечення інформаційної безпеки, як і управління, повинні проводитись на інформаційних потоках внутрішньої і зовнішньої взаємодії з навколишнім оточенням та носіях цих інформаційних потоків. Б. Система інформаційної безпеки та механізми безпеки повинні бути не окремою виділеною системою, а органічно вбудованою невід'ємною

частиною системи обробки динамічних потоків інформації. С. Відповідно до поділу управління в інтелектуальній системі на внутрішнє, зовнішнє та компенсацію не прогнозованих впливів зовнішнього світу, система забезпечення інформаційної безпеки відкритої системи теж має складатись з не менш ніж з трьох процесів, цілі і механізми дії яких можуть відрізнятись. Д. Проблема обмеження зростання кількості контрольованих сутностей і потоків вирішується разом із системою інтелектуального управління шляхом реструктуризації, а саме створенням структур наступних рівнів. Рішення щодо реструктуризації приймаються з урахуванням вимог до інформаційної безпеки. Необхідно зробити зауваження щодо проблеми цінності інформації, що розглядалась у першій частині цієї роботи. У відкритих системах об'єктивної оцінки чи функції цінності інформації не існує, бо оцінка інформації локалізована у конкретній взаємодії. Можна сказати, що «цінність інформації», а не сама інформація, завжди існує лише в контексті, який розглядається, і є породженням трійки: «користувач – задача – вміст бази». У відкритих системах цінність, корисність, функція старіння конкретних даних, знань, інформації, структур інформації існують в конкретній взаємодії, класифікуються за типами взаємодій і можуть розглядатись як контекстно-залежні функції від поточного контексту. А це співпадає з управляючою функцією інформаційного потоку [5]. Тому мають розглядатись як параметри інтелектуального управління. Цінність належить до категорії управляючих функцій інформації.

Задачі інформаційної безпеки. Класична система інформаційної безпеки робить систему, яка захищається, закритою, що понижує її ефективність. Одна з головних задач полягає в максимальному збереженні можливостей взаємодії з оточуючим середовищем і ефективності свого функціонування в умовах взаємодії з навколишнім оточенням, тобто будувати систему інформаційної безпеки згідно з законами відкритих систем, зберігаючи і не зменшуючи ефективність функціонування і зберігаючи необхідну свободу взаємодії.

Процеси забезпечення безпеки є однією з пріоритетних задач системи інтелектуального управління. Пріоритет завжди віддається внутрішньому управлінню, тобто підтриманню стабільності власної структури. Задачі системи інформаційної безпеки можуть бути класифіковані в такому порядку: забезпечити стійкість і поведінкові (цільові) аспекти системи, що управляється; компенсувати випадкові впливи, які збурюють систему; досягти стану, при якому скомпенсовані випадкові впливи, виявлені, а також блоковані зовнішні впливи, які не відповідають цільовій направленості функціонування системи.

Будь-які, завчасно не передбачені відхилення практичного стану об'єкта від його теоретичного описання повинні бути заблоковані таким чином, щоб вони не вели до катастрофічних наслідків. Система інформаційної безпеки інтелектуальних систем повинна використовувати можливості й засоби роботи з контекстно-залежною інформацією, передбачати підтримку контекстної залежності даних у SIB, забезпечити роботу системи управління на різних контекстах інформаційних потоків у різних ситуаціях.

Вимоги до системи інтелектуального управління щодо інформаційної безпеки. Властивості самозберігаємості, самоорганізації, саморозвитку та інтелекту з точки зору забезпечення інформаційної безпеки відкритої системи ставлять проблеми і вимоги постійної керованості, спостережності, а також повсюдності цих властивостей для тотожності визначення контексту в однакових умовах. Основу інформаційної безпеки відкритих систем складає вимога спостережності всіх систем, явищ, процесів або об'єктів. Проблема спостережності набуває важливого значення тому, що інтелектуальна система управління класу «суб'єктно-об'єктної взаємодії» має область невизначеності. Вона не в змозі інформувати, як вона дійшла до певного рішення, і яке рішення буде сприйняте її оточенням як правильне. Це система з не програмованими рішеннями або рішеннями з нечітко вираженою структурою.

У безпечній інтелектуальній системі управління наявна практично вся інформація, яка може бути зібрана і використана при автоматичному прийнятті управлінських та захисних рішень. Інформаційні потоки між підсистемам для забезпечення інформаційної безпеки та управління повинні бути контрольовані. Має бути забезпечене повне і постійне слідкування за характеристиками всіх інформаційних потоків.

Проблема інформаційної усталеності (стійкості) вирішується створенням ієрархічної структури, в якій кожен новий рівень може створюватись виходячи із своїх оцінок ефективності функціонування (способу адресації, точніше, способу вибірки знань із бази дані-знання). При досягненні верхньої границі допустимого числа зв'язків проводиться автоматична генерація наступного одного або декількох рівнів ієрархії інформаційного банку, необхідних для забезпечення стійкості системи.

Правильний вибір інформаційних границь об'єкту, які мінімально залежать від зміни оточення об'єкту, дозволяє спростити систему інформаційної безпеки. Максимальне інформаційне забезпечення внутрішніх підсистем внутрішніми зв'язками при можливій мінімізації їх зв'язків із зовнішнім світом може бути однією з цілей створення відкритої системи.

Принципово важливою вимогою є адаптивність системи інформаційної безпеки й динамічний характер

її роботи. Механізми безпеки мають бути адаптивними для динамічно змінних потоків інформації.

Розглянуті підходи до забезпечення інформаційної безпеки у відкритих системах співзвучні новій парадигмі інформаційної безпеки інформаційно-телекомунікаційних систем. Системи безпеки майбутнього повинні не тільки і не стільки обмежувати допуск користувачів до програм і даних, скільки визначати і делегувати їх повноваження у корпоративному вирішенні задач, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації й усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів. Вирішення такої задачі дасть можливість оптимізувати також й існуючі системи інформаційної безпеки закритих систем, сучасна теорія яких частково вирішує задачу захисту відкритих систем.

Результати та висновки

В цій частині роботи вирішені такі задачі, об'єднані поставленою метою вироблення науково-методичних основ системи інформаційної безпеки відкритих систем:

- розглянуто принципові структурні властивості відкритих систем;
- роз'яснена роль інтелектуального управління у відкритих системах та їх органічна єдність з процесами забезпечення безпеки; зроблено висновок щодо співпадання цілей, методів контролю, механізмів забезпечення безпеки, які мають системи управління та системи інформаційної безпеки; знайдено висновок, що системи інтелектуального управління за своїм принципом дії виконують певну частину задач інформаційної безпеки, зокрема повну спостережність системи та утримання системи в стані гомеокінетичного плато, тобто забезпечують фізичну безпеку;
- сформульовано цілі інформаційної безпеки та вимоги до системи інтелектуального управління з позицій інформаційної безпеки; сформульовані гіпотези щодо системи інформаційної безпеки, споріднені з аналогічними гіпотезами щодо інтелектуального управління.

Крім того, намічені шляхи до створення технології й архітектури інформаційної безпеки відкритих систем та побудови системи інформаційної безпеки на законах функціонування відкритих систем. Напрямом подальшої роботи може бути: обґрунтування способу побудови інтегрованої в систему управління чи окремої системи інформаційної безпеки відкритих систем; розробка комплексної системи вимог до власне системи інформаційної безпеки відкритих систем. Важливим напрямком досліджень є розробка принципів і реалізація адаптивних систем захисту інформації та розробки систем інформаційної безпеки в зовнішньому контурі управління відкритою системою.

Література: ***1.*** *Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих системою Частина 1. Міри інформації та властивості інформаційних процесів відкритих систем. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С. 44 – 55.* ***2.*** *Потий А. Эталонная модель системы процессов защиты информации. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С. 31 – 43.* ***3.*** *В. М. Лачинов, А. О. Поляков. Информодинамика или Путь к Миру открытых систем. Санкт-Петербург, Издат. СПбГТУ, 1999. – С. 364. (http//www.polyakov.com/informodynamiks).* ***4.*** *Чаки Ф. Современная теория управления. Нелинейные, оптимальные и адаптивные системы. Пер. с английского. – М.: Мир, 1975. 424 с.* ***5.*** *Леваков А. Анатомия информационной безопасности США. Jet Info online #6(109), 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – 74 с.* ***6.*** *Кононович В., Тардаскін М. Парадигма інформаційної безпеки телебіомерики та сенсорних телекомунікаційних мереж. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С 56 – 65.* ***7.*** *Колмогоров А. Н. Жизнь и мышление как особые формы существования материи. // О сущности жизни. М.: Наука 1964, с. 48 – 57.*

УДК 004.82, 007.04, 681.3, 681.518.54

ПРИМЕНЕНИЕ ПРИНЦИПА БИОАНАЛОГИИ ДЛЯ СИНТЕЗА СИСТЕМ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИЙ

Сергей Гладыш

Одесская национальная академия связи им. А. С. Попова

Анотація: **Досліджено можливості застосування методів штучного інтелекту у процесах керування інформаційною безпекою телекомунікаційних систем. Як новий методологічний підхід**