УДК 681.322

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Соколов Костянтин Олександрович
начальник управління
Управління інформаційних технологій
Міністерства оборони України
Соколов Константин Александрович
начальник управления
Управление информационных технологий
Министерства обороны Украины
Sokolov Konstantin
Head of department
Department of information technologies of the
Ministry of Defense of Ukraine

ПИТАННЯ СИНТЕЗУ СТРУКТУРИ ТА ПАРАМЕТРІВ СИСТЕМИ (ПІДСИСТЕМИ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ВОПРОС СИНТЕЗА СТРУКТУРЫ И ПАРАМЕТРОВ СИСТЕМЫ (ПОДСИСТЕМЫ) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

QUESTIONS OF SYNTHESIS OF STRUCTURE AND PARAMETERS OF INFORMATION SECURITY SYSTEM (SUBSIDIARY)

Анотація. *В статті наведений синтез структури системи (підсистеми) інформаційної безпеки держави з обґрунтуванням її основних параметрів.*

Ключові слова: *інформаційна безпека, система інформаційної безпеки, параметри, синтез.*

Аннотация. *В статье приведен синтез структуры системы (подсистемы) информационной безопасности государства с обоснованием ее основных параметров.*

Ключевые слова: *информационная безопасность, система информационной безопасности, параметры, синтез.*

Summary. *The article describes the synthesis of the structure of a system (subsystem) of state information security with the justification of its main parameters.*

Key words: *information security, information security system, parameters, synthesis.*

Вступ. В воєнних конфліктах сучасності спостерігається стійка тенденція застосування їх учасниками у масовому порядку високотехнологічних зразків озброєння та військової техніки, інноваційних технологій управління ними. При цьому, як правило, такі засоби, навіть при локальному використанні, забезпечують вирішальний вплив на хід і результати конфлікту. Сучасні інформаційні технології передбачають, що вплив буде здійснюватись, перш за все, по найважливіших об'єктах із забезпеченням гранично досяжних швидкості й точності дії на їх «критичні» складові, здебільшого одночасно на всій території держави (регіону). Реалізація таких підходів забезпечує найбільш ефективне досягнення мети. Системи забезпечення національної безпеки будь-яких держав світу мають уразливі точки (підсистеми, складові, об'єкти), які отримали назву «слабких ланок», «слабких місць», «больових» або «критичних» точок, вплив на які або знищує систему або неприпустимим чином змінює її характеристики й алгоритми функціонування. Порушення їхнього функціонування або знищення позбавляє державу, по якій завдаються удари, здатності подальшого ведення війни. Завдяки використанню інноваційних технологій у цих війнах став можливим перехід від дій загальноруйнівного характеру до дій із перевагою функціонально-структурного, виборчого впливу на супротивника. Базовий принцип досягнення мети дій полягає в інформаційно-технологічно-економіко-силовому протиборстві. Акцент методів,

що використовуються у протиборствах зміщується у бік широкого застосування інформаційних, кібернетичних, політичних, економічних, інформаційних, гуманітарних і інших невоєнних заходів, що реалізуються із задіянням протестного потенціалу населення.

Тому виникає актуальне наукове завдання, що полягає у створенні систем (підсистем) інформаційної безпеки на різних рівнях державного управління (далі — систем інформаційної безпеки).

Виклад основного матеріалу дослідження. Основними завданнями систем (підсистем) інформаційної безпеки можуть бути: виявлення, оцінювання та прогнозування розвитку потенційних та реальних інформаційних загроз; проведення попереджувальних інформаційних та інших заходів щодо їх нейтралізації; протидія зовнішньому інформаційному впливу (інформаційним заходам), спрямованому на послаблення обороноздатності держави; забезпечення розвитку і кіберзахисту інформаційної інфраструктури та інформаційних ресурсів держави; підготовка та захист об'єктів критичної інформаційної інфраструктури держави та інші.

Для реалізації основних завдань систем (підсистем) забезпечення інформаційної безпеки формується її структура із наступних складових (підсистем): виявлення, оцінювання та прогнозування розвитку інформаційних загроз, планування заходів інформаційної безпеки; інформування громадськості про діяльність органу управління (органу державної влади); захисту інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органу управління (органу державної влади) від кіберзагроз; інформаційної протидії (у т.ч. щодо реагування на кризові ситуації в інформаційному просторі; підготовки і ведення інформаційно-психологічних операцій (заходів) та операцій (заходів) в кіберпросторі); управління заходами забезпечення інформаційної безпеки та інші.

Для реагування на визначені вище інформаційні загрози з метою протидії негативному інформаційному впливу в межах органів управління (органів державного управління) існують, трансформуються і нарощуються структури, функціональні спроможності систем (підсистем) забезпечення інформаційної безпеки. З точки зору науково-технологічного підґрунтя для формування цих систем (підсистем) використовується ідеологія побудови ієрархічної розподіленої складної ергатичної системи із надмірною статичною основою.

Основою для оснащення системи (підсистем) інформаційної безпеки є програмно-апаратний комплекс, як складна розподілена інформаційно-керуючої системи (далі — ІКС) реагування на кризові ситуації (далі — КС), яка забезпечує реалізацію процесів моніторингу, накопичення і обробки інформації моніторингу, виявлення КС (інформаційних загроз), вироблення і реалізацію цільових дій та оцінювання їх ефективності. З урахуванням зазначеного матимемо загальний обрис структури програмно-апаратного комплексу системи (підсистеми) інформаційної безпеки, поданий на рис. 1.

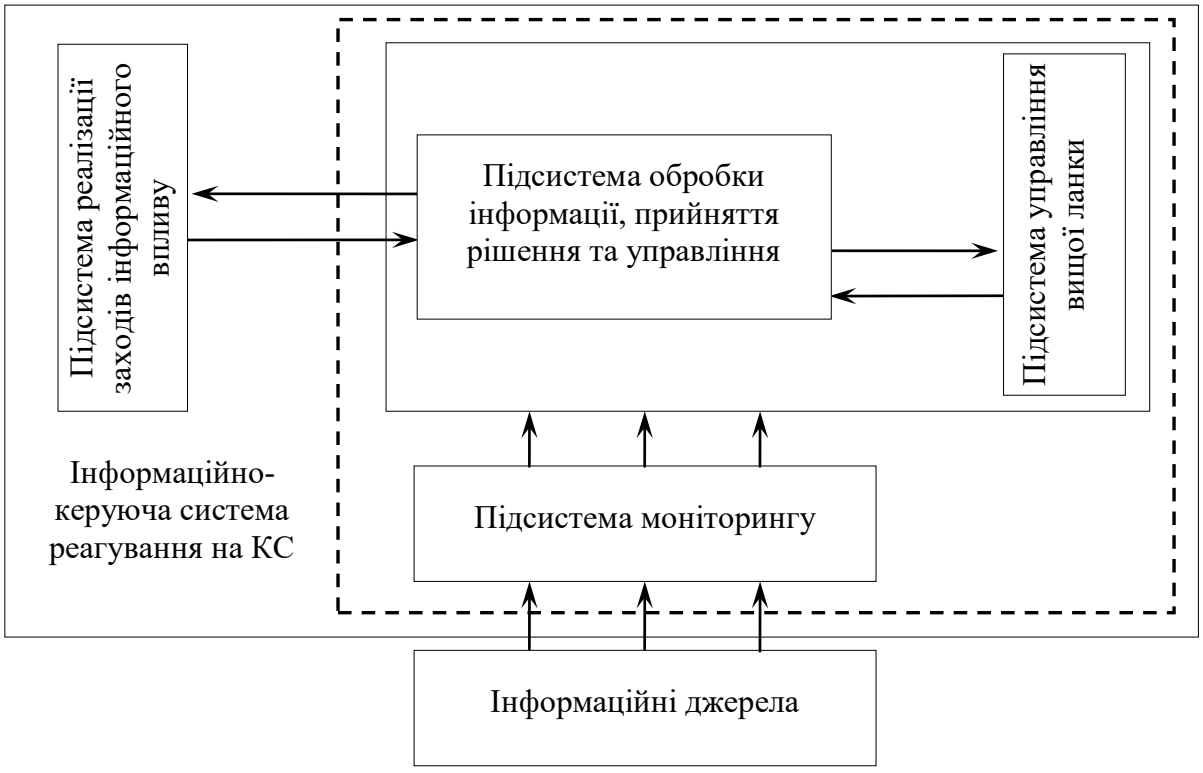

Рис. 1. Загальний обрис структури програмно-апаратного комплексу

Сучасні умови реалізації заходів інформаційної безпеки відбуваються в умовах значної кількості та щільності потоку КС. Тому, необхідним є поглиблений аналіз методів ідентифікації контрольованих ситуацій із впровадженням самоорганізації, теоретичних основ ситуативного управління, синтезу складних ІКС реагування на КС, як програмно-апаратної основи систем (підсистем, системи) інформаційної безпеки та оцінювання ефективності побудови і функціонування системи забезпечення інформаційної безпеки із впровадженням процесів ситуаційного управління.

Для вироблення рішень реагування на КС активного застосування набули технології побудови ІКС із впровадженням ситуаційних центрів (далі — СЦ). СЦ є основою сучасного науково-технологічного середовища, що сприяє оперативному інформаційно-аналітичному забезпеченню керівництва в надзвичайних (нештатних), кризових ситуаціях та забезпечує прийняття ефективних управлінських рішень.

Традиційні технологічні засади складних ІКС базуються на принципах організації модульних розподілених систем з мережевою передачею даних для створення єдиного інформаційного простору з охопленням усіх інформаційних засобів і потоків передачі даним. Основна ідея їх створення і функціонування полягає у досягненні інформаційної надмірності нарощуваної структури з відкритою архітектурою для ефективного вирішення завдань моніторингу і управління.

Будь-яка складна система визначається трьома категоріями: елементами, відношеннями, властивостями. Однозначний і повний опис цих категорій визначають систему, її структуру, параметри та ефективність. Метою синтезу системи є конкретизація і визначення оптимальних (раціональних) рішень для указаних категорій. У свою чергу синтез складної системи передбачає розв'язання задач структурного та параметричного синтезу.

Структурний синтез складної системи розглядався у працях А. Д. Цвіркуна, І. В. Кузьміна, А. М. Вороніна, Ю. К. Зіатдінова, Г. Л. Баранова, Т. Р. Брахмана та інших, зокрема етапи формування вимог до системи; вибір складових системи, рівня їх деталізації, формування варіантів побудови системи та опис взаємодії їх компонент; вибір оптимального варіанта побудови системи [1; 2; 3–7; 8; 9; 10]. Розв'язанню задачі параметричного синтезу складних систем присвячено значну кількість робіт, найбільш показовими з яких є праці Т. Р. Брахмана, А. М. Вороніна, Ю. Х. Вермішева, Г. С. Антушева [11; 2; 3–7]. За класичним трактуванням задача параметричного синтезу складної системи полягає у визначенні параметрів елементів заданої структури [11], зокрема у виборі числових характеристик або системи в цілому, або окремих її компонент.

Аналіз відомих методологічних та технологічних підходів до реалізації процесів та побудови ІКС і результати їх практичного застосування переконливо доводить наявність проблем у принципах побудови та методологічній базі обробки в них інформації. Першопричиною цього є інформаційна надмірність даних моніторингу, що породжена самоціллю створення, розвитку та застосування єдиного інформаційного простору. Характерним, при цьому є постійне зростання кількості інформаційних джерел та технічних засобів моніторингу різного типу, формату даних, повнотою, достовірністю та своєчасності первинної інформації, а також споживачів інформації. Зазначене посилюється значною динамікою зміни зовнішньої обстановки і щільності потоку КС.

Головна ідея ситуаційного управління в складних системах чи складними системами полягає у зміні її властивостей, поведінки, або параметрів відповідно до поточної зовнішньої чи внутрішньої обстановки — ситуації — КС. Як правило, ситуативне управління реалізується на підставі ретельного дослідження умов практичного застосування такої системи з формуванням, модифікацією і розвитком бази даних і бази знань про КС. Завдяки цьому і через властивості ситуативності такі системи мають властивості інтелектуальних. ІКС з ситуативним управлінням загалом мають класичну архітектуру за винятком потужної інтелектуальної компоненти в якості складного програмного додатку у вигляді розрахункової програми, експертної системи чи системи підтримки прийняття рішень. В основу програмного забезпечення ІКС ситуативним управлінням покладене потужне математичне забезпечення цього процесу.

Традиційно реалізація ситуаційного управління базується на принципі вироблення і реалізації сценаріїв із функціональних етапів функціонування ІКС. Тобто управління з відпрацюванням КС реалізується через зміну функцій, діях і відповідно властивостей компонент та системи у цілому. Основоположним принципом є реалізація процесів ситуативного управління на існуючий структурі — фактично без зміни структурних параметрів самої системи та у межах її елементів.

Крім того, не дивлячись на видимість завершеності та проробки технологій ситуативного управління існують значні його недоліки, що полягають у суб'єктивізмі методів управління, обмеженості технологічних та теоретичних методах і моделей його практичного застосування.

Аналіз відомих методологічних засад синтезу структур складних ІКС показує, що в більшості випадків структурний і параметричний їх синтез здійснюється за однокритеріальними моделями, що не забезпечує повною мірою врахування усього спектра суперечливих вимог до системи і призводить до зниження якості результатів синтезу. Окрім того, у кожному конкретному випадку для визначення оптимальної за структурою і параметрами ІКС обираються відповідні методи з урахуванням специфіки розв'язуваних цільових задач.

У зв'язку з цим необхідним є запровадження багатокритеріальних підходів до структурного і параметричного синтезу складних ІКС.

Багатокритеріальна методика ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки (конфігурування системи) включатиме наступні етапи:

1) формування сегменту початкових даних — формулярів КС, автоматизованих робочих місць, технічних (нетехнічних) засобів моніторингу — шляхом ідентифікації виниклої КС за інформацією апріорно сформованих баз даних і баз знань;

2) визначення оптимального кількісного складу автоматизованих робочих місць системи обробки інформації, необхідних технічних засобів моніторингу і обумовлених виконавчих елементів з використанням відповідних оптимізаційних моделей;

3) синтез якісної структури системи реагування на КС для рівня інформаційно-керуючих кластерів;

4) за результатами п. 3 формування інформаційно-керуючих кластерів складної ергатичної розподіленої інформаційно-керуючої системи реагування на КС: її структури і параметрів — відповідно до сегменту початкових даних — формулярів КС, автоматизованих робочих місць, технічних (нетехнічних) засобів моніторингу та переліку виконавчих елементів;

5) при зміні поточної ситуації реалізується повторення п. 1–5 методики.

Висновки. Розроблена методика базується на принципі ситуаційного управління, реалізованому з використанням методів багатокритеріального аналізу стосовно задачі аналізу і синтезу складних систем. Особливість методики полягає в спільному рішенні задачі структурного і параметричного синтезу системи.

Етап структурного синтезу реалізований в явному вигляді, а вибором параметрів системи є опосередкований процес інтерпретації результатів структурного синтезу і прийняття відповідних відібраним автоматизованим робочим місцям, технічним (нетехнічним) засобам моніторингу, виконавчих елементів і технічних характеристик в якості параметрів системи. В результаті отримано науково-методичне підґрунтя для створення (удосконалення) систем (підсистем) інформаційної безпеки органів управління (органів виконавчої влади) у вигляді програмно-апаратного комплексу, як складної розподіленої ІКС реагування на КС, що забезпечує реалізацію процесів моніторингу, накопичення і обробки інформації моніторингу, виявлення КС (інформаційних загроз), вироблення і реалізацію цільових дій та оцінювання їх ефективності із впровадженням принципів ситуаційного управління, багатокритеріального аналізу та самоорганізації.

Напрямком подальших досліджень є розробка методу ідентифікації загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення.

Література

1. Баранов Г. Л. Структурное моделирование сложных динамических систем / Г. Л. Баранов, А. В. Макаров. — К.: Наук. думка, 1986. — 272 с.

2. Брахман Т. Р. Многокритериальность и выбор альтернатив в технике / Т. Р. Брахман. — М.: Радио и связь, 1984. — 288 с.

3. Воронин А. Н. Многокритериальное распределение ограниченных ресурсов / А. Н. Воронин // Проблемы управления и информатики. — 2010. — № 4. — С. 143–150.

4. Воронин А. Н. Многокритериальный синтез динамических систем / А. Н. Воронин. — К: Наук. думка, 1992. — 160 с.

5. Воронин А. Н. Сложные технические и эргатические системы: метод использования / А. Н. Воронин, Ю. К. Зиатдинов, А. В. Харченко, В. В. Осташевский. — Харьков: Факт, 1997. — 240 с.

6. Воронин А. Н. Вложенные скалярные свертки векторного критерия / А. Н. Воронин // Проблемы управления и информатики. — 2003. — № 5. — С. 10–21.

7. Воронин А. Н. Методика многокритериальной оценки эффективности научных космических проектов / А. Н. Воронин, Л. Н. Колос, Л. В. Подгородецкая // Проблемы управления и информатики. — 2004. — № 5. — С. 46–56.

8. Основы моделирования сложных систем: учеб. пособие для студ. вузов / под ред. И. В. Кузьмина. — К.: Высш. шк., 1981. — 360 с.

9. Цвиркун А. Д. Имитационное моделирование в задачах синтеза структуры сложных систем (оптимизационно-имитационный подход) / А. Д. Цвиркун, В. К. Акинфиев, В. А. Филиппов. — М.: Наука, 1985. — 173 с.

10. Цвиркун А. Д. Основы синтеза структуры сложных систем / А. Д. Цвиркун. — М.: Наука, 1982. — 200 с.

11. Антушев Г. С. Методы параметрического синтеза сложных технических систем / Г. С. Антушев. — М.: Наука, 1986. — 88 с.