Таблиця 2 – Модель загроз в КМЗ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Джерело
Непередбачені помилки					
1	Помилки маршрутизації	низька	к, ц, д, с	високий	внутр. зовн.
2	Програмні помилки	низька	к, ц, д, с	середній	внутр. зовн.
3	Відмови в роботі апаратури, що обумовлені впливом зовнішнього середовища	низька	к, ц, д, с	середній	внутр. зовн.
4	Фактор людини	висока	к, ц, д, с	високий	внутр. зовн.

Слід врахувати, що наведені оцінки ймовірностей та величини можливої шкоди кожної із загроз в даному прикладі моделі загроз носять ілюстративний характер. Для випадків конкретних АС ці величини мають бути визначені фахівцями служби захисту відповідного підприємства.

Література: ***1****. Буточнов О. М., Гончар Г. В., Деревянко С. М., Короленко М. П. Захист інформації в комунікаційній мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 − 58.* ***2.*** *Maximum Security: AHacker's Guide to Protecting Your Internet Site and Network (http://zaphod.redwave.net/books/hackg/index.htm).* ***3.*** *TCP під прицілом (http://www.hackzone.ru/articles/tcp.html).* ***4.*** *Деякі проблеми FTP (http://www.hackzone.ru/articles/ftp.html).* ***5.*** *Атака на DNS або Нічний кошмар мережного адміністратора (http://www.hackzone.ru/articles/dn s−poison.html);* ***6.*** *Медведовский И. Д. Семьянов П. В. Леонов Д. Г."Атака на Інтернет" М.:Видавництво ДВК 1999;* ***7.*** *Соболоев К. И. Дослідження системи безпеки з Windows NT 4.0 HackZone: Територія злому. №1−2, 1998.* ***8.*** *Переповнення буфера в WIN32 (http://www.void.ru/stat/9907/20.html).* ***9.*** *EXPLOIT'и переповнення буфера на PERL'е (http://www.void.ru/stat/0102/02.html).* ***10.*** *Теорія й практика атак FORMAT STRING (http://www.void.ru/stat/0102/27.html+http://www.void.ru/stat/0102/28.html).* ***11.*** *Перехоплення пакетів TCP: Захист від флуда (http://www.void.ru/stat/9907/19.html).* ***12.*** *Матов О. Я., Василенко В. С., Будько М. М Оцінка захищеності в локальних обчислювальних мережах. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 59 − 73.*

УДК 681.5:621.391

ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДКРИТИХ СИСТЕМ. ЧАСТИНА 3. ІЄРАРХІЯ СИСТЕМ ТА ВИМОГ ДО БЕЗПЕКИ

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: **З позицій теорії систем та синергетики аналізуються основні ієрархічні властивості інформаційної безпеки складних відкритих систем, що розвиваються. Формулюється ієрархія вимог до інформаційної безпеки відкритих систем.**

Summary: **It is analyzed, from positions of theory of the systems and synergetic, basic hierarchical properties in relation to information security of the difficult open systems which develop. The hierarchy of requirements to informative safety of the open systems is formulated**.

Ключові слова: **Інформаційна безпека, відкриті системи, кібернетика, ієрархічні системи, параметри порядку, саморганізація.**

I Вступ

Дане дослідження стосується сфери технічного захисту інформації та інформаційної безпеки систем, які об'єднуються під загальною назвою – інформаційні технології з акцентом на відкриті системи. Проблематика дослідження, аналіз стану досліджень наведені в частинах 1, 2 цієї роботи [1, 2].

Аналіз останніх досягнень і публікацій показує розвиток уявлень щодо ієрархічних властивостей складних систем. Складні системи розглядаються як ієрархія рівнів, нижні з яких є найбільш простими, а верхні – найбільш складними. Відповідно ієрархічною є мова чи спосіб описання систем. Прикладом є ієрархія мов програмування – машинні, асемблерні, високого рівня, об'єктно-орієнтовані тощо – або ієрархія конструкторської документації – принципові, структурні, функціональні схеми. В кібернетичних системах ієрархія рівнів застосовується, перш за все, з метою подолання складності [3]. Складна система декомпозується на прості підсистеми. На верхніх рівнях зручніше оперувати з укрупненими об'єктами так, щоб у цілому складна система залишалась осяжною та контрольованою. Нові рівні можуть створюватись за трьома методами: інтерпретації, трансляції або процедурного розширення. Використовується дві основні стратегії розробки багаторівневих систем: стратегія «зверху вниз» та стратегія «знизу вверх», які були логічно еквівалентними і розрізнялись, в основному, лише зручністю використання. Значним розвитком методів розробки ієрархічних систем було винайдення об'єктно-орієнтованого проектування (та програмування) як потужного засобу розробки складних інформаційно-технічних систем [4]. У об'єктно-орієнтованому проектуванні найважливішими стали, на наш погляд, методи конструювання об'єктів з новими властивостями й змінними та розповсюдження ідеї ієрархії рівнів не лише на структуру, організацію, а також на процеси, архітектуру тощо. Зокрема, плідним виявився ієрархічний підхід до архітектури взаємодії відкритих телекомунікаційних систем [5], так що можна вважати його однією з найважливіших чинників бурхливого розвитку телекомунікаційних технологій.

За принципом ієрархічної організації будується будь-яка управлінська структура, як суспільна – управління підприємством, галуззю чи державою, так і складна технічна – приміром, енергетична система, телекомунікаційна система, роботизоване виробництво. Розвинуто ієрархічний підхід при моделюванні складних багаторівневих систем, у основу якого покладено підхід з «гнучким» управлінням [6]. Глобальна задача системи великої розмірності замінюється послідовністю відносно незалежних задач меншої розмірності і здійснюється цілеспрямоване узгодження їх рішень. Розроблена типова організаційна структура багаторівневої моделі як статичних так і динамічних систем, процедури узгодження локальних управлінь та реакцій підсистем у єдиній цілісній системі, розроблені процедури аналізу та синтезу станів ієрархічних систем, придатних для практичного використання.

Ієрархічні системи широко розповсюджені не лише у штучних, розроблених людиною, системах, у промисловості, економіці, організаційних системах управління тощо, а й у неживій та живій природі. Універсальні закономірності побудови та розвитку ієрархічних систем знаходять обґрунтування у синергетиці (від грецького слова synergena сумісна дія, співробітництво; термін, введений німецьким фізиком Германом Бакеном у 1974 році, акцентує на узгодженості частин при утворенні структури як єдиного цілого) – науці, яка вивчає процеси самоорганізації й виникнення систем, підтримання функціонування, стійкості та розпаду систем самої різноманітної природи [7]. Концепція самоорганізації виникла на основі статистичної фізики (І. Пригожин, Г. Хакен), загальної теорії систем, кібернетики (Н. Вінер). Якщо відкрита система отримує ззовні упорядковану енергію деякої потужності і потоком негентропії, то незворотні процеси в середині системи приводять до народження ентропії [8], причому невелика частина негентропії, що поступила в систему, витрачається на підтримку і удосконалення внутрішньої структури системи. Народжена в системі ентропія разом з надлишковою масою викидається на зовні у вигляді відходів, викликаючи «теплове забруднення» середовища. При цьому, в системах із складно організованою внутрішньою структурою можливо розшарування єдиної системи на дві, тісно пов'язані між собою підсистеми: силову чи динамічну і управляючу чи інформаційну. Структурні елементи, які можуть сильно впливати на функціонування системи малими сигналами (збуреннями), виділяються у структуру управління. Таким чином, складні динамічні системи можуть розшаровуватись на два рівня ієрархії. Управляюча система є теж динамічною системою, тільки вона може функціонувати з набагато слабшими процесами обміну енергіями, тобто, з «сигналами». Управляюча система стає, так би мовити, інформаційною системою. Складна динамічна система може сама по собі розшаровуватись на два рівня ієрархії. В результаті, структурна ієрархія складних фізичних систем виявляється більш енергетично вигідною відносно однорідної системи. Дана закономірність є наслідком принципу мінімальної енергії. При значних успіхах у дослідженнях складних відкритих систем залишається невирішеним проблема інформаційної безпеки систем, зокрема впливу ієрархічності систем на вимоги до системи інформаційної безпеки.

Мета даної частини роботи: в рамках загальної мети – вироблення науково-методичних основ системи інформаційної безпеки відкритих систем – виявлення впливу ієрархічних властивостей на інформаційну безпеку та розробка вимог до інформаційної безпеки складних відкритих систем.

Постановка задачі. Ієрархічна закономірність організації відноситься до універсальних властивостей відкритих систем різноманітної природи. Широко відомі і глибоко досліджені ієрархії управління, систем

управління та низка ієрархій у обчислювальній техніці. Синергетичний погляд на процеси у відкритих системах виявляє ряд їх нових властивостей, пояснює їх закономірності і дає можливість сформувати підходи до інформаційної безпеки. Розуміння загальних начал синергетики дозволяє передбачити і пояснити ряд нових явищ у системах інформаційної безпеки. Тому проаналізуємо нові властивості відкритих систем порівняно з замкнутими, вияснимо, зокрема, природу самоорганізації ієрархічних відкритих систем, систему ієрархій у інформаційно-телекомунікаційних системах та продовжимо пошук шляхів створення технології й архітектури інформаційної безпеки відкритих систем і побудови системи інформаційної безпеки з врахуванням законів функціонування відкритих систем.

II Загальносистемні закономірності замкнутих та відкритих систем

Ієрархічність входить до складу взаємопов'язаного комплексу закономірностей, характерних для великих складних технічних й соціальних систем, які називають загальносистемними: 1) цілісність і цілеспрямованість систем, 2) ієрархічність (кібернетична), 3) уніфікованість і сумісність, 4) функціонально-модульна організація. На відміну від замкнутих систем, у відкритих системах при синергетичній парадигмі додаються закономірності [9]: функціонування й буття – 5) гомеостатичності і 6) ієрархічності (синергетичної); та розвитку й становлення – 7) не лінійності, 8) нестійкості, 9) не замкнутості, 10) динамічної ієрархічності, 11) спостереженості. Закономірності функціонування і буття характеризують фази стабільного функціонування системи, так званої фази «порядку», наявність стійких дисипативних структур-атракторів, на яких функціонує система. Закономірності розвитку й становлення характеризують фазу оновлення системи, народження нової структури, нового порядку.

1. Закономірність цілісності проявляється у тому, що при об'єднанні елементів у систему виникають нові якості (функції, об'єкти, властивості, цілі тощо), не властиві складовим частинам. Цілісність визначається метою, для виконання яких призначена система. Глобальною метою створення системи інформаційної безпеки певного інформаційного об'єкту є створення (ієрархічного, як буде показано далі) комплексу заходів і засобів (комплексу інформаційної безпеки, служб, послуг та механізмів захисту), які задовольняють вимогам користувачів за рівнем захищеності за умови збереження заданого рівня ефективності функціонування інформаційного об'єкту, та мінімізації витрат на розробку, випробування й експлуатацію системи інформаційної безпеки до рівня, зіставного з рівнем можливих втрат при порушенні безпеки.

2. Ієрархічність – загальна закономірність побудови світу та будь-якої виділеної з нього системи. Ієрархічність, яку тут будемо тимчасово називати кібернетичною за сферою науки, де вона була вперше сформульована і досліджена, була винайдена як ефективна методика подолання складності. Закономірність ієрархічності означає побудову системи в вигляді багаторівневої структури, в якій функції, об'єкти, управління чи взаємодія розподілені між субпідрядними рівнями. Будь-які системи є елементами наступного більш високого рівня, а елементи даного рівня, в свою чергу, є системами більш низького рівня. На кожному з рівнів ієрархії проявляється закономірність цілісності, бо система утримується в стійкому стані. На кожному з рівнів виникають нові властивості, які не є простою сумою властивостей окремих елементів. Принцип ієрархічності може відноситись до організації, структури, управління, взаємодії, функцій, топології, архітектури тощо. В міжнародних рекомендаціях та стандартах з телекомунікацій ієрархію взаємодії називають архітектурою взаємодії [5]. Ієрархічність управління передбачає підпорядкування рівнів за управлінням. Функція управління старших рівнів носить більш загальний характер і конкретизується на нижчих рівнях. Ієрархічність простежується, перш за все, в описі систем, процесів, функцій. Найнижчим рівнем електронно-технічних систем можна вважати рівень елементної бази. З транзисторів, інтегральних схем, резисторів тощо будуються вузли, потім блоки, апаратура, станції й мережі.

3. Закономірність уніфікованості й сумісності визначають гнучкість реалізації функцій системи, адаптованість до різноманітних вимог, можливість розвитку на основі сумісності частин один з одним та зберігання цілісності. Життєздатність систем, ефективність їх розробки, виробництва й експлуатації, досягається послідовним застосуванням цих принципів. Уніфікованість й сумісність дає можливість провести комплексну оптимізацію і мінімізацію систем на всіх ієрархічних рівнях: рівні структури, рівні розподілу функцій між модулями, рівні параметрів апаратури, схемотехніки, конструкції, елементної бази.

4. Функціонально-модульний принцип організації систем дозволяє ефективно реалізувати закономірність уніфікованості й сумісності технічних засобів систем. На кожному рівні ієрархії система розчленовується на функціональні модулі. Функціональним модулем називається функціонально й конструктивно закінчений пристрій, який застосовується для компоновки систем, задовольняє вимогам інформаційної, програмної та конструктивної сумісності та забезпечує ефективність створення, застосування й обслуговування цього модуля. У машинобудуванні аналогом функціонального модуля є

агрегат, який складений з уніфікованих сумісних частин. Функціонально-модульний принцип організації систем, який базується на їх уніфікації, дає можливість розширення систем шляхом нарощування кількості модулів. Зокрема, магістрально-модульна структура мікропроцесорних та обчислювальних систем надає апаратурі гнучкість, універсальність, незалежність від функцій, які вона має реалізувати, стимулює сумісність і активність апаратури до різних умов застосування. Для об'єднання функціональних модулів у цілісну систему передбачається їх конструктивна, електрична, логічна, функціональна, програмна (алгоритмічна) сумісність. Сумісність модулів забезпечується стандартним інтерфейсом та протоколом взаємодії модулів. Типізація та стандартизація взаємодії на всіх рівнях штучних систем має важливе загально державне значення: стандартизація, проведена у цілому по країні та в усьому світі, дає значний економічний ефект. У природних системах уніфікація взаємодії виражається у принципі мінімуму енергетичних витрат.

5. Закономірність гомеостатичності стосується суто відкритих систем. Гомеостаз – це підтримання цільової програми функціонування системи, її внутрішніх характеристик у деяких рамках, які дозволяють їй прямувати до своєї цілі [9]. Коригування поведінки системи здійснюється за рахунок негативного зворотного зв'язку, який ліквідує будь-яке відхилення в цільовій програмі поведінки системи, що виникає внаслідок дії зовнішнього середовища. Цільову програму поведінки системи в стані гомеостазу фізики в нелінійній динаміці називають атрактором, що означає «притягуюча множина» (від англ. *attract* – притягувати, заваблювати). Атрактори існують лише доти, доки в дисипативну систему подається потік речовини, енергії, інформації. Дисипативною системою, що далека від рівноваги, називають структуру, яка розсіює енергію, інформацію. Без споживання потоку зовнішньої речовини, енергії, інформації дисипативна система руйнується. Наприклад, людські спільноти без надходження коштів та інформації розпадаються.

Гомеостаз часто здійснюється на рівні лінійних коливань коло оптимальних параметрів системи, при яких діє принцип суперпозиції: результат сумарної дії на систему є сума лінійних відгуків системи на кожну дію, де лінійний відгук системи прямо пропорційний впливу. Поблизу границь гомеостазу, границь цілісності системи її поведінка, як правило, нелінійна. Малі дії можуть спричиняти значні зміни поведінки системи і її перехід до стану нового гомеостазу.

6. Закономірність синергетичної (назва умовна) ієрархії характеризує складову природу вищих рівнів відносно нижчих. Закономірність ієрархії можна формулювати для систем різної природи: наприклад у ієрархії природи – елементарні частки, атоми, молекули, речовина; у ієрархії мови – звуки, слова, фрази, тексти тощо. Всякий раз елементи, які зв'язуються в структуру, передають їй частину своїх функцій, ступенів свободи і у створеній колективній системі виникають функції, яких на рівні елементів може й не бути. Колективні змінні на високому ієрархічному рівні, наслідуючи Г. Хакена, називають параметрами порядку. Ці параметри саме й описують смисл поведінки та цілі системи. Згідно з принципом підпорядкування, зміни параметрів порядку одночасно впливають на поведінку множини елементів нижнього рівня, які утворюють систему. Синергетичний принцип підпорядкування Хакена сформульований для, так званої, часової ієрархії. Розглядаються три довільних сусідніх рівня: мікро-, макро- й мегарівні, відповідно. Параметри порядку розглядаються як довго живущі колективні змінні, які задають мову макрорівня. Вони утворені і управляють швидкими, коротко живущими простими змінними, які задають мову мікрорівня. Наприклад, на мікрорівні – це параметри «теплового» хаотичного руху молекул газу, а на макрорівні – це параметри тиску, температури, тощо. Наступний, вищий мегарівень, утворений над повільними змінними, які виконують для макрорівня роль параметрів порядку і в даній тріаді рівнів називаються параметрами управління. Згідно з принципом підпорядкованості довго живущі змінні управляють коротко живущими, верхній рівень управляє нижнім.

Для системи інформаційної безпеки принцип підпорядкованості відіграє суттєву роль. Нажаль він справедливий не завжди і порушується. Нижні рівні можуть управляти верхніми і управління може оминати сусідні рівні, порушуючи ієрархію управління. Це свідчить, що всяка ієрархія не може бути раз і назавжди встановлена. Для її підтримання необхідні засоби забезпечення принципів становлення й розвитку, які розглядаються далі і характеризують фазу оновлення в процесі розвитку (еволюції) системи. При оновленні системи вона проходить стадії загибелі старого порядку, стадії хаосу випробувань альтернатив і стадію народження нового порядку. Система при оновленні може ввійти в стадію хаосу, як правило, за рахунок позитивного зворотного зв'язку, який посилює у системі зовнішні впливи. Крім того, система повинна мати властивості не лінійності, не стійкості, не замкнутості.

7. Закономірність нелінійності – це порушення принципу суперпозиції у деякому явищі. Результат суми впливів не рівний сумі їх результатів. Будь-яка границя цілісності об'єкта, його руйнування, поділу, поглинання передбачає нелінійні ефекти [9]. Щоб перейти від одного стану гомеостазу до іншого необхідно зайти в область сильної не лінійності. Не лінійною завжди є задача прийняття рішення, вибору в

кризових ситуаціях.

8. Закономірність не замкнутості притаманна лише відкритим системам. Для замкнутої системи справедливі фундаментальні закони збереження енергії, імпульсу, моменту імпульсу тощо. Це спрощує описання простих систем. У замкнутих системах справедливий другий закон термодинаміки: ентропія, як міра хаосу, з часом зростає чи залишається постійною. Тобто, в замкнутій системі хаос може лише зростати, порядок зникає. Навпаки, у відкритих системах, які споживають речовину, енергію, інформацію, ентропія може зменшуватись [9]. Саме відкритість системи дозволяє їй еволюціонувати від простого до складного. Ієрархічний рівень може виникати, розвиватись й ускладнюватись лише при обміні речовиною, енергією, інформацією з іншими рівнями – зокрема, нижчими або однорівневими та розташованими в іншій системі.

9. Закономірність нестійкості необхідна при переході з одного положення гомеостазу до іншого і тісно пов'язана з двома попередніми закономірностями. Перехід до нестійкого стану можливий лише в нелінійних системах. При переході до нового положення гомеостазу система стає відкритою, стає чутливою до дій інших рівнів. Такими властивостями володіють усі системи, що навчаються, в ситуації вибору або генерації цінної інформації. Стан нестійкості носить назву біфуркація (від англ. *fork* – вилка) і є рубежем між старим і новим. Важливе те, що в точках біфуркації можливо малими діями, слабкими впливами, несиловим, інформаційним способом вплинути на вибір поведінки системи. Говорять, що біфуркації – це точки народження цінної інформації.

10. Закономірність динамічної ієрархічності або емерджентності (від emergence – виникнення, поява нового) є узагальненням принципу підпорядкованості на процеси розвитку, становлення системи. Це основний принцип проходження системою точок біфуркації і виникнення нової якості системи в межах одного рівня при взаємодії з верхнім та нижнім рівнями. Повільна зміна управляючих параметрів мегарівня може приводити до біфуркації, нестійкості системи на макрорівні та перебудови його структури [9]. Параметри порядку макрорівня повертають свої степені свободи у хаос мікрорівня, розчиняючись у ньому. Потім, при взаємодії мега- і мікрорівнів народжуються нові найшвидші параметри порядку оновленого макрорівня. У точці біфуркації на мікрорівні проходить вибір, тобто еволюційний відбір альтернатив розвитку макрорівня.

У процесах розвитку, становлення відкритої системи при міжрівневій взаємодії можуть виникати характерні загрози інформаційній безпеці. *Перша характерна загроза* може виникати на рівні, який є верхнім для даного (на мегарівні). На верхньому рівні може бути здійснене несанкціоноване формування управляючих параметрів, які можуть привести до нестабільності і розвитку системи до незапланованого стану. *Другою характерною загрозою* інформаційній безпеці відкритих систем є несанкціоноване втручання у міжрівневу взаємодію з нижнім мікро-рівнем у критичних точках процесу розвитку, становлення системи. Після входження системи по плановому сигналу з верхнього мегарівня в процесі перебудови структури, під час проходження точки біфуркації може бути сформовано малу несанкціоновану дію, яка може привести до іншого, незапланованого стану гомеостазу.

11. Закономірність *спостережності* має пряме відношення до інформаційної безпеки і підкреслює обмеженість і відносність наших уявлень про всі рівні ієрархічної системи у кінцевому експерименті. Принцип відносності до засобів спостереження сформульовані у теорії відносності і квантовій механіці. У синергетиці – це відносність інтерпретацій до масштабів спостережень та очікуваного результату. Те, що було хаосом з позицій макрорівня є структурою при переході до масштабу мікрорівня. Цілісне описання ієрархічної системи складається в результаті комунікації між спостерігачами різних рівнів. Друга характерна загроза інформаційній безпеці має значно менший масштаб спостереження і може *маскуватись* під хаотичний процес на нижньому рівні (на мікро-рівні).

Таким чином, ієрархічний принцип організації структур, напевне, має універсальне розповсюдження, якщо, звичайно, він не є іманентною властивістю нашої свідомості [цитується за 10]. Але на нинішньому етапі розвитку науки це є важко вирішуваним питанням. Характерні для ієрархічних систем загрози приводять до необхідності формування спеціальних вимог до системи інформаційної безпеки як на кожному з рівнів, так і до безпеки міжрівневої взаємодії з нижнім і верхнім суміжними рівнями у процесах розвитку, становлення відкритої системи.

III Ієрархічність інформаційно-телекомунікаційних систем та систем інформаційної безпеки

Системи інформаційної безпеки мають наслідувати принцип ієрархічності інформаційних систем. Інформаційно-телекомунікаційні мережі – це найбільш складні на теперішній час штучні структури. Їх характеризує комплекс ієрархій: ієрархія структурної організації, ієрархія функцій, ієрархія цілей та вимог. Верхню ступінь ієрархії вимог складають вимоги користувачів до параметрів інформаційно-

телекомунікаційних послуг: вірність передачі інформації, імовірність доставки повідомлення за адресою та втрати повідомлень (мінімально допустимий рівень втрат повідомлень), обмеження часу доставки, надійність, живучість та сталість систем тощо. Взаємодії та функції, які виконують інформаційно-комунікаційні мережі, також відрізняються складністю і їх поділяють між рівнями. Найнижчим є фізичний рівень, тобто рівень утворення фізичного каналу, яким передається інформація. Найвижчим є рівень взаємодії між внутрішніми або людино-машинними процесами, що виконуються за допомогою терміналів, ЕОМ, концентраторів, локальних обчислювальних мереж тощо.

Широко відома семирівнева еталонна модель архітектури взаємодії відкритих систем (ВВС) і, зокрема телекомунікаційних систем [5], розроблена сумісно Міжнародним консультативним комітетом з телефонії та телеграфії й Міжнародною організацією зі стандартизації, детально описана в численних підручниках та навчальних посібниках. У даному контексті відкритою (організаційно) називається така система, в якій гарантується її взаємодія з будь-яким абонентом, який дотримується приписаного для даної системи набору правил. Основні аспекти цієї моделі такі. У моделі ВВС виокремлюються сім рівнів опрацювання інформації: 1 – фізичний; 2 – канальний; 3 – мережний; 4 – транспортний; 5 – сеансовий; 6 – представний; 7 – прикладний. Кожен рівень виконує певні завдання та функції й забезпечує умови функціонування суміжних рівнів. Функції кожного рівня можуть бути реалізовані апаратним чи програмним способом. У моделі ВВС на кожному рівні існують об'єкти, сервіси та послуги. Об'єктом може бути, наприклад, програма обробки інформації. Кожен рівень надає набір послуг (тобто сервіс) суміжному верхньому рівневі й використовує при цьому послуги, які надаються суміжним нижнім рівнем. Набори послуг, надаваних рівнем, називають *сервісами*. Об'єкти рівня взаємодіють з об'єктами суміжних рівнів у межах системи і з об'єктами цього ж рівня, котрі перебувають в інших системах обробки інформації. В цьому полягає основне призначення мережі. Взаємодія об'єктів суміжних рівнів здійснюється через *інтерфейси*. Через міжрівневий інтерфейс кожен рівень отримує послуги (сервіс) рівня, що лежить нижче. Взаємодія об'єктів одного рівня, які перебувають в різних системах в моделі архітектури взаємодії відкритих систем, описується протоколами. *Протоколи* охоплюють уніфіковані правила, формати даних і порядок перебігу встановлення зв'язку поміж користувачами і мережею, а також поміж користувачами через мережу. Протокол стандартизує всі можливі ситуації, які можуть виникнути при взаємодії об'єктів, кодування цих ситуацій й приписує (формує) правила реагування на кожну з них. Прикладами можливих ситуацій є ситуації «виклик», «відбій», «помилка», «перезапит», «абонент зайнятий» тощо. Формат повідомлення – це стандартизоване розташування елементів повідомлення: знаків початку повідомлення, заголовка, адреси, тексту повідомлення, кінцівка.

Функції й протоколи зв'язку моделі ВВС дозволяють створювати служби. Послуги телекомунікацій надаються користувачам лише за допомогою певних служб. *Служби* характеризуються технічними, експлуатаційними показниками й показниками обслуговування. Ці показники описують усі функції та протоколи зв'язку, необхідні для здійснення зв'язку в певній службі. ITU (міжнародний союз телекомунікацій) стандартизує такі служби: телеслужби, служби передавання, служби безпеки. Під *телеслужбами* розуміють служби для безпосереднього зв'язку поміж користувачами із зазначенням функцій прикінцевих пристроїв. Прикладами телеслужб були: телефонна, телетекс, телефакс, відеотекс. У телекомунікаційних мережах майбутнього служби конвергуються і абонент матиме можливість отримувати будь-які телекомунікаційні та інформаційні послуги. Служби передачі призначені для незалежного від коду та застосувань передавання даних. Послугу зв'язку може бути надано споживачам через мережу. Технічні положення служби передавання охоплюють функції, які виконуються на рівнях від першого до четвертого і є зорієнтованими на транспортування повідомлень. Служби безпеки забезпечують безпеку системи. Під терміном б е з п е к а с и с т е м и розуміють такий стан системи, за якого мінімізовані вразливості цінностей, наявних у системі. *Вразливість* – це будь-яка слабкість, що її може бути використано для порушення структури системи чи інформації. *Загроза* – це потенційне порушення безпеки.

Архітектура взаємодії систем описує взаємовідносини між рівнями та іншими частинами систем, й зокрема протоколи, формати і логічні структури, які забезпечують цілеспрямований зв'язок між абонентами. В процесі обміну інформацією окремі рівні незалежні один від одного. Протоколи кожного рівня реалізуються незалежно від протоколів інших рівнів. Тек протоколів організований так, що взаємодіють лише протоколи суміжних рівнів. Об'єкти кожного даного рівня в системі-джерелі і в системі-одержувачі взаємодіють не безпосередньо, а мають для цього звертатись до нижнього суміжного рівня. Об'єкти кожного нижнього рівня також взаємодіють, користуючись протоколами цього рівня та звертаючись для реалізації цієї взаємодії до рівнів мережі, що лежать нижче. І лише об'єкти фізичного рівня (електричний струм, електричні, оптичні чи електромагнітні сигнали) безпосередньо взаємодіють через фізичні канали.

Системи інформаційної безпеки інформаційно-телекомунікаційних систем мають ієрархію двоякого роду: власну ієрархію як комплексна складна система та ієрархію, успадковану від системи, на кожному з рівнів якої забезпечується заходи безпеки. Власна ієрархія системи інформаційної безпеки може бути описана рядом: механізми безпеки; функціональні послуги безпеки; комплекси засобів захисту, зокрема забезпечення функціональних профілів захищеності; служби безпеки; комплекси інформаційної (та фізичної) безпеки інформаційних об'єктів; мережні системи інформаційної безпеки; національні системи інформаційної безпеки. Послуги безпеки можуть бути надані лише за допомогою служб безпеки. Служба безпеки реалізує набір функціональних послуг безпеки (сервіс безпеки). Наприклад, служба захисту від несанкціонованого доступу реалізує функціональний профіль захищеності інформаційного об'єкту. *Функціональним профілем захищеності* називають функціонально повний перелік мінімально необхідних рівнів послуг безпеки, який реалізується комплексом засобів захисту системи аби задовольнити певні вимоги щодо захищеності інформаційних ресурсів системи. Для вибору функціональних профілів нормативна база сфери технічного захисту інформації України надає широкий набір стандартних функціональних профілів захищеності. Кожна функціональна послуга реалізується одним чи більш механізмами безпеки. Кожен механізм може використовуватись для реалізації кількох функціональних послуг.

Прикладом найбільш розвинутої ієрархічної системи інформаційної безпеки є модель ешелонованої багаторівневої системи інформаційної безпеки національного стандарту ISO/IEC 15408. Цей стандарт став міжнародним, багато держав прийняли його як національні стандарти. Порівняно з нормативними документами України (НД ТЗІ 2.5-005-99 «Класифікація автоматизованих і стандартні функціональні профілі захищеності інформації від несанкціонованого доступу») стандарт ISO/IEC 15408 передбачає на рівні служб організацію набору служб (класів послуг), які забезпечують ешелонований захист інформаційних ресурсів. До складу цього набору служб входять: служба захисту від несанкціонованого доступу, яка дозволяє запобігти проникненню; служба виявлення інцидентів з безпекою, яка виявляє факт порушення та локалізує об'єкт вторгнення, служба обробки інцидентів, яка дозволяє нейтралізувати та видворити порушника; служба відновлення, яка відновлює втрачені функції системи інформаційної безпеки. В сукупності набір служб утворює комплекс інформаційної безпеки інформаційного об'єкту.

Ієрархія системи інформаційної безпеки, успадкована від системи, що захищається тісно зв'язана з принципом безперервності захисту: *захист інформаційних ресурсів відкритої системи має забезпечуватись на всіх етапах життєвого циклу системи та на всіх її ієрархічних рівнях.* На кожному з рівнів ієрархії інформаційно-телекомунікаційної системи передбачаються спеціальні та загальні засоби й служби захисту, що в сукупності забезпечують створення мережної системи інформаційної безпеки. Розподіл механізмів, функціональних послуг безпеки за рівнями ієрархії та побудови комплексної системи інформаційної безпеки телекомунікаційних мереж загального користування детально розглянуті в [11, 12]. На вищому рівні сукупність мережних систем інформаційної безпеки мереж комунікацій різного типу складають національну систему інформаційної безпеки. На сьогодні можна і необхідно вести мову про створення й глобальної системи інформаційної безпеки.

Одною з цілей даного розділу є також фіксація уваги на проблемі загроз при міжрівневій взаємодії з несуміжними рівнями. Такі взаємодії в правильно спроектованій системі завжди є несанкціонованими. Дана проблема існує і в реальних існуючих автоматизованих системах. Взаємодія з несуміжними рівнями в існуючих операційних системах обчислювальної техніки є, певно, головною причиною того, що безпечних операційних систем поки що не розроблено. Реальні операційні та прикладні програмні системи для ефективності широко використовують різного роду утиліти, доступ до яких можливий з декількох рівнів. У зв'язку з необхідністю вирішення проблеми міжрівневої взаємодії можна припустити, що є справедливою наступна гіпотеза: *в ефективно захищених ієрархічних відкритих системах кожна елементарна міжрівнева взаємодія має контролюватись та ідентифікуватись, а будь-яка взаємодія з несуміжними рівнями повинна бути заблокована*. Для будь-якої взаємодії є шкали (масштаби), зв'язані з багатьма аспектами взаємодії. Для більшості способів взаємодій масштаби різних одиниць, які використовуються для опису взаємодії, можуть змінюватись відповідно до багатьох величин. Деякі відкриті системи, наприклад, людський організм, виробниче підприємство тощо має методи сприймання більш, ніж у одній шкалі. Багаторазовість методів сприймання в багаторазових масштабах дозволяють системі перевіряти робастність інформації, отриманої при взаємодії через різні канали сприймання. Треба звернути увагу на необхідність розгляду феномену різноманіття масштабів і взаємодії шкал. Використання аутентифікації чи забезпечення інформаційної чи фізичної безпеки може бути хибним, якщо при взаємодії застосовується невідповідний масштаб.

IV Основи теорії організації, самоорганізації та рівнів

Світ та його складові є суттєво структуровані, організовані та ієрархічні. Структуроутворення підпорядковане низці закономірностей. Тут дамо короткий огляд їх основних положень з позицій інформаційної безпеки. Ілюстрації теорій організації, ієрархії та рівнів розглянемо на прикладі інформаційної (автоматизованої) системи. Огляд теорії організації та ієрархії представлено, наприклад, у [13]. Там же викладена аксіоматична система для описання і аналізу складних відкритих систем. Передбачається, що такі системи є організованими і мають структуру. Організація – це комплекс взаємодій та властивостей структури, які роблять можливим увічнення цієї структури. Сутністю структури є те, що вона складається з інших структур (об'єктів). Термін об'єкт приймається як «примітивний термін». Введено концепцію *мінімальної діалогової структури* як епістемологічне обмеження на структурну нескінченність реальних систем. Ряд термінів визначені або як відношення між об'єктами структури отриманих властивостей, що випливають з об'єднання таких об'єктів у об'єкти більш високого порядку, або умови, необхідні для їх об'єднання. Організація – складний термін, який складається із взаємозалежності, координації, інтеграції, й ієрархії. Оцінка повної організації об'єкта теоретично можлива через параметризацію і квантифікацію, тобто через визначення кількості компонентів організації.

Основні положення теорії організації. Для екологічних систем, які відносяться до складних відкритих систем, введені наступні аксіоми та визначення [14]: кожен об'єкт має структуру, яка складається з інших об'єктів. Структура об'єкта – це внутрішній комплекс інших об'єктів і їх статичних зв'язків один з одним; кожна структура є сукупністю властивостей і взаємодій об'єктів низького рівня в межах високорівневого об'єкта; структура об'єкта змінюється. Організація – це спосіб динамічного увічнення структури. Організація включає взаємодії і зв'язки (з'єднання) серед структурних елементів, які дозволяють статичній структурі бути сталою. Крім того, вводиться таке поняття, як Мінімальна діалогова структура (MIS - Minimum Interactive Structure). Об'єкти MIS можуть мати ієрархічну структуру, відкриту вниз і агрегуватись, тобто об'єднуватись вверх без очевидного обмеження. Смисл MIS у тому, що на одному рівні ми бачимо структуру як об'єкт, в той час як на наступному нижньому рівні, ми бачимо структуру як комплекс підоб'єктів. На ще більш низькому рівні з'являється структура підоб'єктів. Ізоморфізм MIS об'єкта між послідовними моментами часу є достатнім критерієм для визначення його ідентичності, наприклад, для автентифікації. Функція – це та частина взаємодії компонента MIS, яка вносить вклад у постійність високорівневих об'єктів. Серед функцій MIS має бути реалізована функція інформаційної та фізичної безпеки. Компоненти MIS є комплементарними, де комплементарність – це здатність об'єктів залишатись компонентами MIS, діючи як функціональні доповнення один до одного, або залежачи від кожного іншого.

Спираючись на аксіоматичноу основу зроблені такі твердження, сформульовані у вигляді теорем. 1. Структура є ієрархічною. Ієрархія – це умова того, щоб бути складеним із субблоків, тобто елементів блоку. 2. Об'єкти нижчих рівнів змінюються з більш високими частотами, ніж високорівневі об'єкти. Зміни вимагають видалення, доповнення й заміни об'єктів більш низького порядку. 3. Для об'єктів, які стійкі, зміни структури обмежені таким способом, що MIS зберігається (консервується). Під координацією розуміється дія одного елемента MIS у відповідь на поведінку іншого (інших) така, що вони залишаються комплементарними. Тільки певна специфічна форма комунікацій, яка закінчується координацією, визначена як інформація. Інтеграція – це є сукупність показників як координації, так і інтенсивності зміни конфігурації в межах MIS. 4. Об'єкту здається, що він завжди менш інтегрований ніж його складові об'єкти.

Основні положення теорії інтегральних рівнів. В [15] введені деякі закони рівнів: кожен рівень організується з блоків даного рівня або нижнього рівня плюс деяка нова якість, яка виникає на стадії становлення; видима складність рівнів збільшується вверх; у будь-якій організації більш високий рівень перебуває на утриманні нижнього; у будь-якій організації, більш низький рівень управляється вищим; для організації на будь-якому даному рівні її механізм знаходиться на рівні нижче, а її цілі на рівні вище; порушення (наприклад інформаційної чи фізичної безпеки), введене в організацію на будь-якому рівні, відбівається на всіх рівнях, які його охоплюють; час, необхідний для змін в організації скорочується при підвищенні рівня; чим вище рівень, тим менші його популяції різновидів; неможливо понизити більш високий рівень до більш низького; організація на будь-якому рівні – це дисторсія (від лат. distortion – викривлення) нижнього рівня; події, зокрема деструктивні, на будь-якому даному рівні стосуються організацій на інших рівнях; будь що знаходиться під впливом, оскільки організація має деякий ефект як організація. З останніх законів випливає основна властивість системи інформаційної безпеки: *рівень захищеності системи визначається рівнем захищеності найменш захищеної ланки (блоку), що знаходиться на найменш захищеному рівні ієрархії.*

Крім того, наведені деякі правила пояснення: визначення будь-якої організації має бути наведене на самому низькому рівні, який забезпечить достатнє пояснення; визначення будь-якої організації має бути наведене на самому високому рівні, який цього визначення вимагає; організація належить до її самого високого рівня; кожну організацію необхідно пояснити нарешті на її власному рівні; ніяку організацію не можливо визначити повністю в термінах більш низького або більш високого рівня.

Згідно з універсальним принципом ієрархії для кожного рівня існує група підрівнів.

Основні положення теорії ієрархій. У теорії ієрархій [13] розрізняють два типи ієрархій: скалярну ієрархію вкладених розширень та ієрархію специфікацій, упорядковану за нелінійним підвищенням складності, яка моделюється інтегральними рівнями. Прикладом скалярної ієрархії є ієрархія мов програмування. Програмне застосування є сукупністю програмних модулів, програмні модулі є послідовністю команд, команди реалізуються мікропрограмами, мікропрограми є послідовністю мікрокоманд, мікрокоманди реалізуються мікропрограмним автоматом. З підвищенням рівня складність зростає скалярним способом, Сукупність властивостей на верхньому рівні є скалярною сумою властивостей на нижньому рівні. Нових властивостей не виникає. Прикладом ієрархії складності може бути ієрархія

{фізичний світ {хімічний світ {біологічний світ {соціальній світ {інтелектуальний світ}}}}}.

На верхньому рівні виникають нові властивості, яких не має на нижчому рівні. Ієрархія специфікацій надає модель розвитку – від унікального індивідуального матеріального втілення на глибокому рівні до різноманітності класів у зовнішніх рівнях, як наприклад у ієрархії:

{дисипативна структура {організм {тварина {ссавець {гуманоїд {людина {спільнота}}}}}}}

Окремим випадком є ієрархія за інтенсивністю взаємодії. У більшості біологічних і фізичних систем відносно інтенсивна взаємодія передбачає відносно близьку просторову досяжність. У живих та штучних системах за допомогою нервів чи телефонних ліній можливі дуже сильні певні взаємодії на великих відстанях. При цьому, в обох випадках здатність об’єктів маленького масштабу передавати інформацію на великі відстані забезпечується тим, що вони є частиною оточуючої їх великомасштабної системи. В межах, де взаємодії направлені через спеціалізовані комунікації і транспортні системи, просторова досяжність стає менш визначальною рисою їх структури. Концепція просторової досяжності важлива при визначенні захищених границь дії телекомунікаційних пристроїв, оскільки потенційний ризик набагато більший.

Ієрархія специфікацій еволюціонує в природних системах завдяки процесам, що класифікуються як самоорганізація. В штучних системах ієрархія розвивається як завдяки організованим процесам, так і завдяки процесам самоорганізації. Процеси самоорганізації в складних динамічних суттєво нелінійних нерівноважних нестаціонарних відкритих системах, до яких відноситься більшість реальних систем, вивчаються синергетикою [16]. Самоорганізація представляється як емерджентна, тобто та, яка раптово виникає. При однакових приростах впливу на нелінійну систему вона може давати різні реакції залежно від початкового стану системи на відміну від лінійних систем, де інтенсивність реакції залежить лише від величини вхідного впливу. Найбільш цікаві явища виникають при взаємодії на рівні множини нелінійних динамічних систем. У цьому випадку спостерігаються кооперативні процеси, які приводять до виникнення принципово нових властивостей системи взаємодіючих динамічних підсистем. Одна з таких властивостей – *самоорганізація*, проявляється у самоузгодженості (когерентності) взаємодії підсистем, що дає можливість говорити про виникнення упорядкованої структури (так званих *патернів*), чи навіть нової системи, яка не є простою сумою підсистем. Виникнення самоузгодженості пов’язано з прагненням системи до певного стійкого стану, що називають атрактором.

Основні принципи самоорганізації складних відкритих систем розглянуті вище. Поява нової системи пов’язана із втратою стійкості і біфуркацією – переходом початкової системи у новий стійкий стан. Проходить зміна структури системи. Зміни, які проходять близько до точок нестійкості, залежать від низки відносно не багатьох факторів, які називаються параметрами порядку (ПП) і визначають поведінку підсистем динамічної системи, ніби «підпорядковуючи» її деякій єдиній структурі поведінки. У свою чергу, самі підсистеми формують ПП і, таким чином, виникає, свого роду зворотний зв’язок, а точніше круговий причинний зв’язок. Зміни ПП проходять значно повільніше, ніж зміни «підпорядкованих» їм підсистем. Виникнення ПП пов’язано із взаємодією чи конкуренцією підсистем. ПП відрізняються від управляючих параметрів тим, що останні є зовнішніми впливами, які змінюють ПП. В ієрархії підсистем ПП, які формуються у системі більш високого рівня ієрархії, стають управляючими параметрами для підсистем більш низького рівня. Таким чином, ПП відіграють вирішальну роль при поясненні процесів самоорганізації на всіх рівнях ієрархічних систем. Впливи на параметри управління в моменти біфуркації можуть приводити до суттєвих змін у структурі систем. Процеси *еволюції* можна розглядати як необмежену послідовність процесів самоорганізації. Загальна послідовність процесу еволюції може бути представлена наступними фазами: 1) відносно стабільний стан втрачає стійкість внаслідок, приміром,

зміни внутрішнього стану чи зовнішніх обмежень; 2) біфуркація, яка зумовлена новим елементом у системі або впливом на управляючий параметр, запускає динамічний процес, що приводить до подальшої самоорганізації системи; 3) по завершенню процесу самоорганізації еволюціонуюча система переходить у новий відносно стабільний стан.

У природних системах процес еволюції при випадкових впливах у точках біфуркації породжує розгалужену низку можливостей, з яких потім життя обирає різними способами одну, найбільш життєздатну. Нежиттєздатні чи енергетично невигідні системи не витримують конкуренції і гинуть чи руйнуються. В штучних системах аналогічний процес проходить на інформаційному рівні ще на етапі проектування, коли з безлічі варіантів винахідник чи проектувальник обирає оптимальний, за певними критеріями, варіант. Після створення системи її оптимальність перевіряється на практиці. Еволюція штучних систем забезпечується не тільки за рахунок конкурентного природного відбору, а й за рахунок оптимізації параметрів системи на інформаційному рівні на фазі проектування системи. В реальному інформаційному об'єкті, який підлягає захисту, можуть проходити одночасно обидва процеси, сприяючи чи протидіючи один одному. У зіткнення можуть прийти, з одної сторони, цілі, ідеали, планові організаційні начала, вимоги до технічних, ергономічних, економічних параметрів та вимоги до безпеки, і, з іншої сторони, саморганізація системи, мимовільні процеси на різних рівнях системи, які самостійно, мимовільно формуються національними, соціальними, технічними, психологічними, язиковими та іншими структурами [17].

Синергетика будує математичні моделі складних систем, що розвиваються. Це дає можливість створити синергетичні моделі системи інформаційної безпеки відкритого інформаційного об'єкту. *Несанкціонований вплив може здійснюватись як через параметри управління, так і через параметри порядку. Синергетичне моделювання дозволяє виявити небезпечні атрактори та найбільш важливі ПП й параметри управління. Синергетичний аналіз об'єкта має передувати етапу категорювання інформаційних ресурсів, що підлягають захисту. Класифікація інформації має проводитись як у класі оброблюваної інформації управління, так і у класі параметрів порядку системи. При синергетичному аналізі можливих каналів витоку інформації та каналів впливу на систему має розглядатись міжрівнева взаємодія як з верхнім, командним рівнем системи, так і з нижнім, впливаючим на системоутворення, рівнем.* Синергетичний підхід не відміняє традиційних підходів, заснованих в основному на лінійних закономірностях. Особливістю синергетичного підходу є те, що він досліджує емерджентні явища, які виникають внаслідок взаємодії нелінійних систем, застосування невідповідних масштабів тощо.

На завершення цього розділу дамо особливості ієрархії сучасних інформаційних систем. Інтенсивний розвиток мікро-, а сьогодні й наноелектроніки приводить до того, що апаратний спосіб реалізації функцій, на відміну від програмного, охоплює все вищі класичні ієрархічні рівні: логічних елементів, функціональних блоків, багатофункціональних агрегатів, станцій тощо. Елементарним об'єктом стає вже не лише мікропроцесор чи мікро-ЕОМ, а, наприклад, станція комутації, маршрутизатор тощо. З іншого боку, інкапсуляція (зникнення) нижніх рівнів ієрархії в апаратній реалізації систем компенсується створенням нових верхніх рівнів при розвитку інформаційних систем до національних, глобальних і далі космічних масштабів. Усталеною ієрархією сучасних інформаційних систем є ієрархія рівнів:

{апаратний {мікропрограмний (BIOS) {асемблерний (драйверний) {програмний (комп'ютерний) {мережний (колективу обчислювачів) {національної мережі {глобальної мережі …}}}}}}}

Ієрархічність систем має враховуватись у системі інформаційної безпеки. Захисту в тій чи іншій мінімально необхідній мірі підлягають всі рівні системи. Треба виходити з того, що загрози можуть реалізуватись при несанкціонованому доступі на будь-якому рівні. Зміни на нижніх рівня можуть впливати на функціонування верхніх рівнів і навпаки, зміни на верхніх рівнях управляють змінами на нижніх.

У відкритих системах, порівняно з закритими системами, виникають ряд нових загроз, які пов'язані з не закритістю систем, гомеостатичністю, ієрархічністю та наявністю процесів самоорганізації. Відкрита система більш вразлива до віддаленого несанкціонованого доступу та несанкціонованому впливу на її поведінку.

V Кардинальні вимоги до системи інформаційної безпеки відкритих систем

Принципи формування кардинальних вимог до системи інформаційної безпеки відкритих систем мають включати у себе наступне.

Деструктивні події на будь-якому даному рівні стосуються організацій на інших рівнях. Для системи інформаційної безпеки принцип підпорядкованості відіграє суттєву роль. Нажаль, він справедливий не завжди і порушується. Нижні рівні можуть управляти верхніми і управління може оминати сусідні рівні, порушуючи ієрархію управління. Основна властивість системи інформаційної безпеки полягає в тому, що

рівень захищеності системи визначається рівнем захищеності найменш захищеної ланки (блоку), яка знаходиться на найменш захищеному рівні ієрархії. Характерні для ієрархічних систем загрози приводять до необхідності формування спеціальних вимог до системи інформаційної безпеки як на кожному з рівнів, так і до безпеки міжрівневої взаємодії з нижнім і верхнім суміжними рівнями.

Ієрархія системи інформаційної безпеки, успадкована від системи, що захищається, тісно зв'язана з принципом безперервності захисту: захист інформаційних ресурсів відкритої системи має забезпечуватись на всіх етапах життєвого циклу системи та на всіх її ієрархічних рівнях. У ефективно захищених ієрархічних відкритих системах кожна елементарна міжрівнева взаємодія має контролюватись та ідентифікуватись, а будь-яка взаємодія з несуміжними рівнями повинна бути заблокована. Перш за все контроль та ідентифікація мають бути реалізовані у мінімальній діалоговій структурі (MIS). Серед функцій MIS має бути реалізована функція інформаційної та фізичної безпеки. Для стійких об'єктів зміни структури мають бути обмежені таким способом, що MIS зберігається (консервується). При категоріюванні інформаційного об'єкту має бути проведене синергетичне моделювання об'єкта, щоб виявити небезпечні атрактори та найбільш важливі параметрів порядку й параметри управління. Класифікація інформації має приводитись як у класі оброблюваної управляючої інформації, так і у класі параметрів порядку системи. При аналізі можливих каналів витоку інформації та каналів впливу на систему чи цьому має розглядатись міжрівнева взаємодія як з верхнім, командним рівнем системи, так із нижнім, який впливає на процес системоутворення, рівнем.

Результати та висновки

У цій частині роботи вирішені задачі, об'єднані поставленою метою вироблення науково-методичних основ системи інформаційної безпеки відкритих систем: проаналізовані властивості ієрархічності відкритих систем та процеси самоорганізації в них; сформульовано принципи формулювання кардинальних вимог до системи інформаційної безпеки. Напрямом подальшої роботи може бути розробка функціональних послуг та механізмів безпеки мінімальної діалогової структури й контролю міжрівневих взаємодій.

Література: ***1.*** *Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих систем. 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.*** *Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих систем. 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* ***3.*** *Таненбаум Э. Многоуровневая организация ЭВМ. – Пер. с англ. – М.: Мир, 1979, - С. 547.* ***4.*** *Гради Буч. "Объектно-ориентированный анализ и проектирование с примерами приложений на С++",* ***1998,*** *"BINOM, Невский диалект". (http://www.helloworld.ru/texts/comp/other/oop/index.htm)* ***5.*** *Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications. Geneva, 1991; Стандарт ISO 7498-1:1984. Базова модель ВВС. – С. 31.* ***6.*** *Чернышев М. К., Гаджиев М. Ю. Математическое моделирование иерархических систем с приложениями к биологии и экономике. – М.: Наука, 1983. – С. 192.* ***7.*** *Данилов Ю. А., Кадомцев Б. Б. Что такое синергетика? (http://spkurdyumov.narod.ru/KADOMCEV.htm).* ***8.*** *Кадомцев Б. Б. Динамика и информация. – М.:УФН, Т. 164, № 5, 1994. – С. 82.* ***9.*** *Буданов В. Г. Трансдисциплинарное образование, технологии и принципы синергетики. Синергетическая парадигма. – М.: Прогресс-традиция, 2000. – 285 – 305 с.* ***10.*** *Андрианов И. В., Баранцев Р. Г., Малевич Л. И. Асимптотическая математика и синергетика: путь к целостной простоте. – М.: Едиториал УРСС, 2004. – С. 304.* ***11.*** *Тардаскін М, Ф., Кононович В. Г., Вараксін О. О., Тардаскіна Т. М. Механізми забезпечення інформаційної безпеки телекомунікаційних мереж загального користування. // Зв'язок. – 2005. № 7. – С. 30 – 35, № 8. – С. 24 – 28.* ***12.*** *Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС).* ***13.*** *ITU-T Recommendation X.1081. The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics. – С. 22.* ***14.*** *Kolasa, Jerzy and Picket, (S.T.A.): Ecological systems and the concept of biological organization, Proc. Natl. Acad. Sci. USA, Vol. 86, pp. 8837-8841, November 1989.* ***15.*** *Feibleman, (J. K.): Theory of integrative levels, British Journal for the Philosophy of Science, Vol. 5, pp. 59-66, 1954.* ***16.*** *Большой психологический словарь / под ред. Б. Г. Мещерякова, В. П. Зинченко - 3-е изд., доп. и перераб. - СПб.: ПРАЙМ-ЕВРОЗНАК, 2006. - 672 с.* ***17.*** *Венгерок А. Б. Синергетика и политика // «Общественные науки и современность», № 4, 1993. – С. 55 – 69.*