УДК 681.35
DOI: 10.31673/2409-7292.2019.030614

Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук

КОНЦЕПЦІЯ ПОБУДОВИ ЗАХИЩЕНОЇ СИСТЕМИ УПРАВЛІННЯ ІТ ЦЕНТРУ

В статті висвітлено шляхи створення ІТ центру, як технологічної системи, що реалізує з необхідною якістю ефективне надання інформаційних послуг, їх захист від несанкціонованого доступу, засекречення потоку даних, що забезпечує захищеність інформації, цілісність з'єднання з відновленням, попередження відмов тощо. Запропоновано до застосування відомий інформаційно-ентропійний метод для визначення одного із основних параметрів системи управління мережами ІТ центру - кількість управляючої інформації, яка забезпечує необхідну точність параметрів мережі, що управляється.

Ключові слова: система управління мережами ІТ центру, інформаційно-ентропійний метод, кількість управляючої інформації, захист інформації, служба безпеки.

Вступ

ІТ центр – це технологічна система, яка реалізує з необхідною якістю ефективне надання інформаційних послуг, їх захист від несанкціонованого доступу, засекречення потоку даних, що забезпечує захищеність інформації, цілісність з'єднання з відновленням, захист від відмов тощо. Базові функціональні складові ІТ центру: транспортна мережа та інтелектуальна надбудова.

Побудова захищеної системи управління (СУ) мережею ІТ центру призначена для забезпечення ефективного використання наявного обладнання мережі у будь-яких ситуаціях при дотриманні норм якості обслуговування користувачів.

Виклад основного матеріалу

Проаналізуємо способи досягнення основних завдань, визначених функцій та принципи організації захищеної СУ мережами ІТ центру. [1] Відповідно визначених вимог, ІТ центр охоплює всю діяльність, мета функціонування якого є зменшення негативного впливу на роботу мережі, зокрема:

запланові відключення систем передавання;

зростання вимог обміну як передбаченими, так і непрогнозованими подіями;

перевантаження;

ускладнення в реалізації вимог обміну.

Завдання СУ мережею ІТ центру:

пріоритетне обслуговування викликів при мінімальній довжині шляху;

використання всіх наявних та доступних шляхів для обслуговування навантаження, за умови найуспішнішого обслуговування;

зменшення перевантаження комутаційних систем та відключення при збільшенні.

Переваги у СУ мережею ІТ центру:

покращення обслуговування контрольованих об'єктів (КО);

ефективна експлуатація мережі ІТ центру;

повна інформація про якість роботи мереж і її стан;

захищеність важливих КО, зокрема, при виникненні у мережі екстремальних ситуацій.

При проведенні аналізу стану мережі, необхідно порівнювати контрольовані значення параметрів з пороговими. Відомо, що активно розробляються і проходять випробування методи управління, засновані на використанні "штучного інтелекту". При цьому зауважується: децентралізоване управління потребує менше кваліфікованого персоналу; централізоване управління забезпечує кращий огляд стану, більший обсяг інформації, прийняття кращих рішень. З розгляду організації структури управління контрольованими об'єктами необхідно врахувати наступні три елементи: планування та взаємодію елементів для СУ мережею ІТ центру;контроль за якістю роботи і стану мережі, прийняття необхідних заходів; розвиток СУ мережею ІТ центру.

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

Як зазначалось вище, концепція захищеної СУ мережею ІТ центру передбачає систему управління у вигляді функціональних підсистем: підсистема управління транспортною мережею і підсистема управління "інтелектуальною надбудовою" [2, 3].

Проаналізуємо ці підсистеми. Завданнями управління транспортною мережею є:

організаційно-технічне управління (планування мереж) забезпечує: адаптацію структури мереж та схем спрямованих потоків до прогнозованих ситуацій, підтримку пропускної спроможності мереж на максимально можливому рівні;

оперативно-технічне управління забезпечує у реальному часі адаптацію структури мереж і схем спрямованих потоків до змін станів контрольованих об'єктів та обсягів надходжуваного навантаження;

Для реалізації цих завдань підсистемі управління транспортною мережею ІТ центру необхідно виконувати такі функції:

контролювати технічний стан контрольованих об'єктів (КО), локалізацію несправностей;

контролювати трафік та якість обслуговування КО;

проводити збір, обробку, зберігання та відображення інформації стану мережі;

тестування обладнання і КО;

здійснювати управління трафіком та схемами спрямованих потоків навантаження;

здійснювати управління функціонуванням КО мережі та зміною структури мережі;

проводити перерозподіл технічних засобів між мережами відповідно до ситуації;

планувати заходи з прогнозування ситуацій(зокрема, планування графіків обходів та замін);

забезпечити введення в експлуатацію обладнання;

взаємодію зі службами технічної експлуатації;

проводити збір та аналіз статистичних даних про роботу мереж технічної експлуатації та удосконалення методів технічної експлуатації;

вивчати потоки навантаження;

експертизу проектів зміни технічних або кількісних характеристик мереж та їх елементів у частині відповідності існуючого та запланованого навантаження;

проводити розробку перспективних алгоритмів управління мережею.

Підсистема управління "інтелектуальною надбудовою" – це важлива мережна служба, призначення якої є для забезпечення функціонування мережі, планування та облік роботи усіх компонентів. Служба утворюється з сукупності технічних та програмних засобів мережі, а також інформаційних ресурсів, розміщених у всіх системах мережі.

Служба управління мережею описується відомою моделлю взаємодії відкритих систем (ВВС), у відповідності до якої управління мережею є розподіленим і забезпечується функціонуванням всіх систем, що входять. Логічну структуру служби управління представлено на рис.1. Базою структури є підтримка високої продуктивності мережі; прикладні процеси, що забезпечують: усунення виникаючих пошкоджень; керування конфігурацією мережі; захищення від несанкціонованого доступу до інформації, що передається.

Прикладні процеси для виконання функцій управління мережею, або її частиною, отримують інформацію про роботу взаємодії як своєї, так і інших систем мережі.[3] Необхідні їм відомості передає адміністративний персонал "Прикладні об'єкти системного керування" (SMAE) та "Об'єкти адміністративного керування рівнями" (ОАК). В свою чергу керуючі прикладні процеси пов'язані з роботою "Прикладних об'єктів системного керування " та "Об'єктів керування рівнями". З цією метою керуючі повідомлення передаються на відповідні рівні системи.

Прикладні процеси адміністративного управління підтримуються елементами мережі рівнів. Рівні від фізичного до представницького є звичайними для системи, а рівень "Прикладні об'єкти системного керування" володіє необхідною специфікою – у верхній

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

частині прикладного рівня розміщено функціональний блок – SMAE. Робочий режим "Прикладного об'єкту системного керування" підтримується "Сервісним елементом керування асоціації" (ASCE). "Прикладний об'єкт системного керування" визначає набір протоколів та види послуг, які необхідні для потреб адміністративного управління, у тому числі і для передавання управляючої інформації між системами мереж [3].

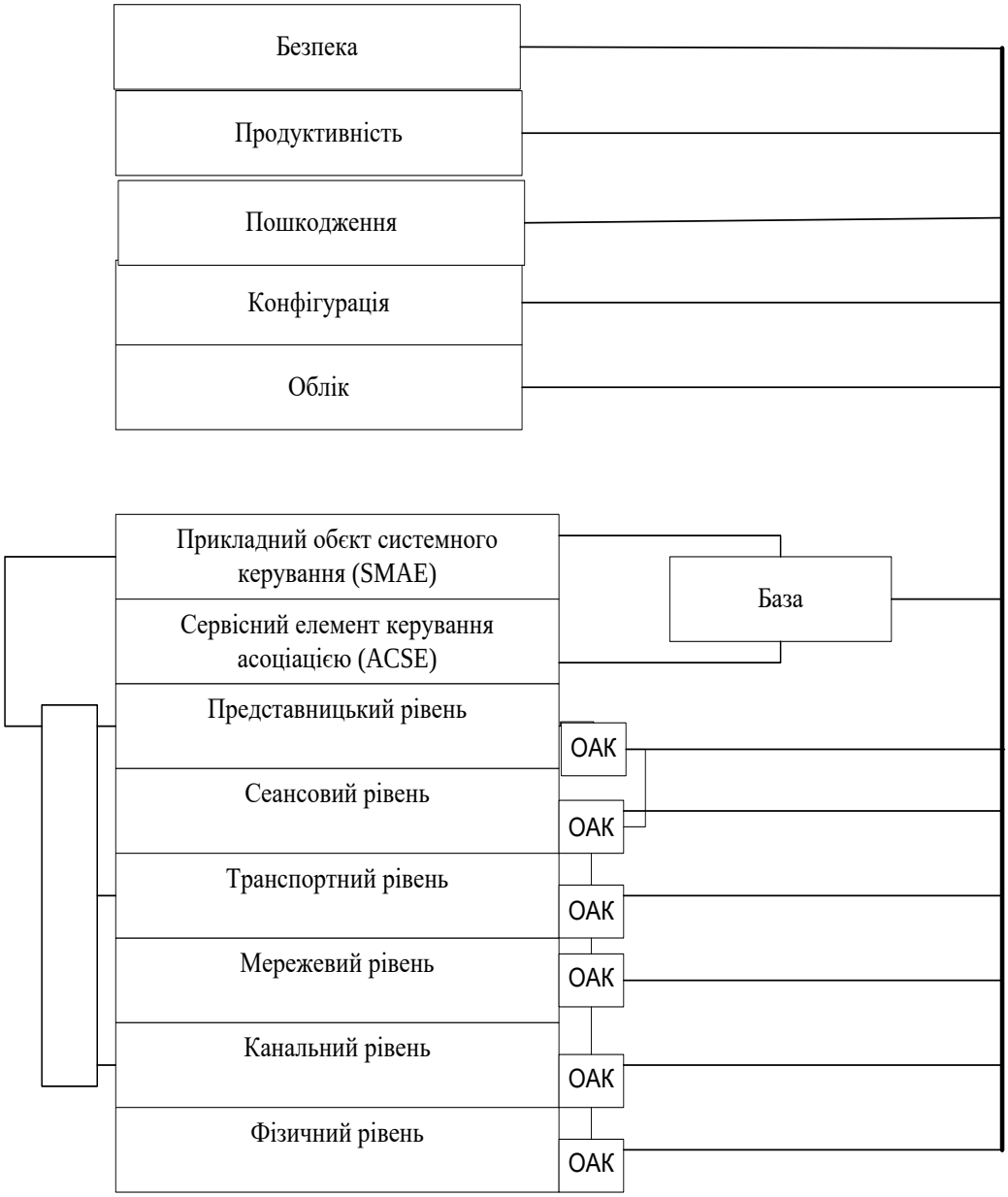

Рис. 1. Структура служби управління

Зокрема, для адміністративного управління необхідна інформація про роботу усіх рівнів системи. Тому у системі створюється база даних, для забезпечення керуючих прикладних процесів усією необхідною інформацією. База у кожній системі складається з основної частини (рис. 1.) та розподілених частин Б на всіх її рівнях.

Завданням кожної з рівневих частин є збір відомостей про роботу рівня, вплив на його об'єкти зі сторони керуючих прикладних процесів. Керуюча інформаційна база кожного

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

рівня з'єднана із відповідним об'єктом адміністративного управління (ОАК). Останній в свою чергу взаємодіє з керуючими прикладними процесами та базою.

В об'єкті адміністративного керування надходить інформація про роботу відповідного рівня: спостереження за функціонуванням протоколу, передаванням повідомлень про виникаючі помилки, зміну станів, потоки даних. ОАК здійснює також загрузку програм рівня, керує зміною протокольних параметрів та ресурсів.

Важливе значення процесами керування відводиться безпеці - захисту інформації від несанкціонованого доступу. [4] Виконання цього завдання забезпечується (рис.1.) рівневими компонентами безпеки та прикладним процесом "Безпека". Керування протоколами пов'язано з виконанням операцій "всередині" кожного протоколу. Вони здійснюють зміну його характеристик та параметрів, наприклад, встановлення визначеної кількості блоків даних, спрямованих до партнера на транспортному рівні після отримання від нього дозволу.

У межах СУ мережею ІТ центру виокремлюють такі основні функції керування: при відмовах; обліком; конфігурацією та іменами; ефективністю функціонування; безпекою.

Керування при відмовах – сукупність засобів, ініційованих у результаті нестабільної роботи функціонального середовища ІТ центру. Відмови проявляються у вигляді збоїв при функціонуванні мережі. Керування відмовами надають засоби обслуговування з аналізу фактів реєстрації збоїв, прийому та обробки повідомлень про виявлення збоїв, адміністративного супроводження збоїв, виконання послідовностей тестів, виправлення відмов.

Керування обліком – це сукупність засобів для визначення вартості ресурсів та сплату за їх використання.

Керування конфігурацією за іменами – сукупність засобів управління, ідентифікації, збору та надання даних, які забезпечують безперервне функціонування служб взаємодії та містить засоби установки параметрів відкритих систем, ініціювання та закриття ресурсів ІТ центру, збору даних про стан відкритих систем, забезпечення конкретними даними за запитом.

Керування ефективністю функціонування – це сукупність засобів, необхідних для оцінки поведінки ресурсів мережі ІТ центру та ефективності діяльності взаємодії.

Однією з основних функцій СУ мережею ІТ центру є керування безпекою. Засоби захисту ресурсів мережі ІТ центру: санкціонування, шифрування та управління ключами, контроль доступу, аутентифікації, аналіз і обслуговування реєстраційних файлів безпеки. [4]

Проаналізуємо такі важливі категорії обміну інформацією СУ мережею ІТ центру: керуючі впливи; повідомлення про подію; передавання інформації.

Обмін інформацією управління - це двостороння взаємодія, у якій сторони виконують функції ініціатора або відповідача для кожного одиничного акту обміну. Ініціатор формує керуючу взаємодію, тобто видає запит на визначену функцію управління. КО формує відповідь на керуючий запит. Реакція на передану інформацію реалізується у запитах на визначену інформацію, яка видається ініціатором та у відповідях, що формуються відповідачем. Повідомлення про події формуються і надсилаються ініціатором. Якщо необхідне підтвердження про прийом такого повідомлення, то воно формується відповідачем у вигляді відповіді.

Процеси, що забезпечують СУ мережею ІТ центру, отримують керуючі впливи: від контрольованого об'єкту і (або) програмного забезпечення, які функціонують як адміністративні агенти, локальні для цього процесу управління; від віддалених систем через їхні прикладні об'єкти управління системами.

Гарантування безпеки інформації в СУ мережею ІТ центру є складним завданням [4]. Відповідно до міжнародних стандартів проблеми захисту інформації вирішуються комплексно одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі зв'язку. Це дає можливість забезпечити захищення систем ІТ центру на всіх етапах їх

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

функціонування – від проектування до технічної експлуатації. Захищеність процесів функціонування усієї системи визначається ступенем захищеності найслабшої частини системи.

Архітектура забезпечення захисту збільшує область застосування еталонної моделі взаємодії відкритих систем при передаванні даних між системами. Визначаються служби безпеки та механізми, забезпечувані моделлю ВВС; розміщення цих служб та механізмів у вузлах мережі.

Проведемо аналіз служб захищення СУ мережі ІТ центру.

Служба аутентифікації однорівневих об'єктів забезпечує підтвердження функціонування об'єктів при періодичному передаванні або при встановленні з'єднання. Служба аутентифікації джерела даних *N*-рівня забезпечує підтвердження *N+1*-рівневі про те, що відправником даних є об'єкт *N+1*-рівня.

Контроль доступу гарантує захищення від несанкціонованого використання ресурсів. Такими можуть бути як ресурси ІТ центру, так і інші ресурси, зокрема, доступні через протоколи мережі ІТ центру. Служби захисту даних забезпечують захист від несанкціонованого доступу:

служба криптозахисту з'єднання забезпечує дотримання таємності усіх даних *N*-об'єкта при передаванні *N*-з'єднанням. Служба криптозахисту без з'єднання гарантує таємність усіх даних *N*-об'єкта, що передаються одним блоком даних служби *N*-рівня без встановлення з'єднання;

служба криптозахисту вибіркових полів забезпечує захист вибіркових полів даних *N*-об'єкта при передаванні *N*-з'єднанням або в одному блоці даних служби *N*-рівня без встановлення з'єднання;

служба криптозахисту потоку даних забезпечує таємність інформації, яку отримують з аналізу потоків даних (, обсяг, наявність або відсутність, інтенсивність потоків);

служба цілісності з'єднання з відновленням гарантує забезпечення цілісності усіх даних *N*-об'єкта при передаванні *N*-з'єднанням з виявленням будь-якого змінення та здатністю відновлення;

служба цілісності з'єднання без відновлення аналогічна службі цілісності з'єднання з відновленням, але не містить процедури відновлення;

служба цілісності вибіркових полів з'єднання забезпечує цілісність вибіркових полів даних *N*-об'єкта у блоці даних *N*-служби при передаванні *N*-з'єднанням та приймає форму визначення факту змінення;

служба цілісності без з'єднання забезпечує цілісність одного блоку даних *N*-служби без встановлення з'єднання та приймає форму визначення факту змінення прийнятого блоку даних служби. Додатково можуть забезпечуватись обмежені форми виявлення вставок та повторів.

Служба попередження відмов приймає одну чи обидві форми:

служба попередження відмов з підтвердженням джерела забезпечує підконтрольному об'єкту необхідні докази про походження даних, які захищають проти спроби відправника помилково відмовитись від факту надсилання даних або від їх вмісту;

служба попередження відмов з підтвердженням доставки забезпечує підконтрольному об'єкту докази даних, які захищають від спроби отримувача помилково відмовитись від факту прийому даних або від їх вмісту.

Отже, для побудови захищеної системи управління мережею ІТ центру необхідно визначити один з найважливіших параметрів – це мінімальну кількість управляючої інформації, що забезпечує необхідну точність параметрів контрольованих об'єктів [2].

Такими вимогами володіє більш «гнучка» архітектура СУ мережами ІТ центру. Системи управління характеризуються такими ознаками: складністю; розосередженістю; жорсткими вимогами до захисту інформації; функціональними можливостями; надійністю, точністю. В статті запропоновано відомий інформаційно-ентропійний метод для розрахунку

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

кількості інформації, а як наслідок, і необхідної пропускної спроможності каналів системи управління мережею ІТ центру з акцентуванням вимог до безпеки. За допомогою інформаційно-ентропійного методу визначимо необхідний мінімум керуючої інформації. За умови, що параметри мережі повинні забезпечувати задану точність, володіти як інваріантністю до випадкових збурюючих факторів, так і якістю адаптивності до плинних прогнозованих діянь [3]. Одним з основних завдань управління функціонуванням СУ ІТ центру є зменшення відхилення певного процесу від бажаного та визначення мінімально необхідної кількості управляючої інформації для забезпечення необхідної точності параметрів на керуючій мережі. Вимога до точності керування при цьому значно підвищується.

Інформаційно-ентропійний метод дає змогу знайти кількість управляючої інформації, що визначається як різниця ентропій мережі перед ввімкненням СУ і після встановлення режиму нормальної роботи. При цьому враховується необхідна кількість управляючої інформації, яка необхідна для підтримки режиму нормальної роботи. Режим нормальної роботи мережі визначається середньо-квадратичним відхиленням контрольованих параметрів від допустимих значень. Кількість каналів та їх параметри залежать від обсягу управляючої інформації.

Вимоги до точності керування мережею часто поєднуються з вимогами швидкості перебігу процесу. [3] У термінах теорії інформації процес «керування мережею» вважається процесом зменшення невизначеності її стану, що чисельно характеризує зміни відповідної ентропії в процесі керування, оскільки ентропія визначає відхилення параметрів мережі за кожний фіксований момент часу. Вихідними даними для розрахунку є відомості про: об`єкт управління; параметри об`єктів управління; відхилення параметрів вказаних об`єктів. У кожному конкретному випадку при виборі об`єктів управління та їх параметрів виходять з необхідної точності розрахунків та потреб системи управління. За прогнозом, кількість управляючої інформації в таких системах різко зростає з наданням послуг, внаслідок чого система управління може поглинути основну мережу. Одним з головних завдань для СУ мережами ІТ центру є визначення мінімально необхідної кількості управляючої інформації, яка повинна повністю забезпечити управляючу мережу з належною точністю параметрів.

СУ мережею ІТ центру повинна володіти як здатністю адаптації до стійких плинних змін режиму, так і властивістю інваріантності, що дозволяє системі бути нечутливою до випадкових діянь. При дослідженні систем управління найефективнішою виявилась система управління, яка має комбіновану структуру, тобто об’єднує властивості адаптивності (замкнена) та інваріантності (розімкнена). Структура комбінованої системи керування подана на рис.2.

Процес функціонування мережі в кожний момент часу t характеризується вектором змінних станів $\{x_1(t), x_2(t),..., x_n(t)\}$ або функціоналом $\Phi\{x_1(t), x_2(t),..., x_n(t)\}$. Вказані змінні станів є випадковими величинами зі своїми законами розподілу $P(x_i)$. Управління мережею - процес приведення змінних стану мережі за заданий час з початкового стану до усталеного. Наприклад, x_i – термін часу доставки інформації між двома вузлами мережі. Якість функціонування мережі характеризується середньою затримкою повідомлень, яка обчислюється середньою величиною затримки на всіх вузлах. Завдання управління мережею має на меті мінімізацію і підтримку на рівні, не більше за задане середнє очікування і зменшення дисперсії середньої затримки повідомлень у мережі. Вимоги до точності управління мережею часто поєднуються з вимогами збільшення швидкодії. У термінах теорії інформації є визначення: процес управління мережею – це процес зменшення невизначеності стану мережі, що може бути чисельно представлено, як зміна ентропії мережі в процесі управління, оскільки ентропія визначає відхилення параметрів мережі за даний проміжок часу.

Відомо, що середня кількість інформації при передаванні сигналу дорівнює різниці ентропії розподілу ймовірностей цієї величини до і після отримання сигналу [3,4].

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

Таким чином, визначивши зміну ентропії керованого процесу функціонування мережі в процесі управління, можна визначити кількість інформації, необхідну для отримання заданого відхилення ймовірності змінних стану мережі.

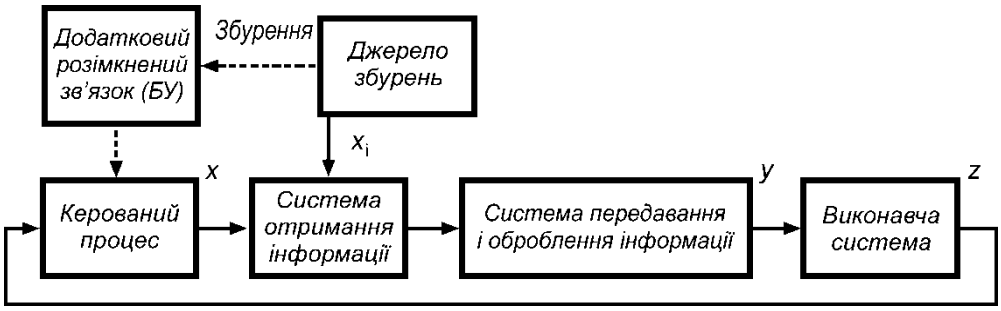

Рис. 2. Структура комбінованої системи керування

Кожну сукупність значень параметрів мережі ІТ центру можна розглядати, як певний стан мережі. У теорії ймовірності та теорії інформації поняття ентропії було поширене на розподіл імовірностей будь-яких змінних. Ентропією безперервного розподілу ймовірностей змінних $x_1, x_2, \ldots x_n$ прийнято величину:

$$B = -\int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} p(x_1, x_2, \ldots, x_n) \cdot \log p(x_1, x_2, \ldots, x_n) dx_1, \ldots, dx_n, \qquad (1)$$

де $p(x_1, x_2, \ldots, x_n)$ –щільність імовірностей.

Теорія інформації розглядає ентропію розподілу ймовірностей в системах отримання і передачі інформації. При цьому вважається, що після отримання інформації про яку-небудь величину, розподіл імовірності цієї величини, отже, ентропія може суттєво змінитися. В теорії інформації поняттю ентропії надається значення «суб'єктивної» або відносної характеристики. Подібну ентропію вважаємо інформаційною ентропією. Крім інформаційної ентропії для опису управління взаємодії елементів мережі, запропоновано застосовувати інше поняття ентропії, що характеризуються не координатами безлічі елементів мережі, а обмеженим числом різних величин - координат. Цей вид ентропії - розподіл імовірностей координат керованого процесу або просто ентропія процесу.

Приріст (зменшення) ентропії буде визначатися як:

$$B(t) - B(t\text{-}1) = \log \frac{\delta_1(t)}{\delta_1(t-1)} + \ldots \log \frac{\delta_n(t)}{\delta_n(t-1)}, , \qquad (2)$$

де $\delta_i(t)$ – середньоквадратичні відхилення параметрів мережі в момент часу t;

$\delta_i(t\text{-}1)$– середньоквадратичні відхилення параметрів мережі в момент часу t-1.

Для оцінки кількості інформації, яка передається в системі управління мережею ІТ центру, необхідно оцінити відношення дисперсій відхилення параметрів повідомлень, що досліджуються в мережі в різних ситуаціях, а така оцінка може бути зроблена за вимогами до параметрів основної мережі [3].

Технічна реалізація абсолютно інваріантних систем складна. Їх потрібно розглядати як граничні характеристики, до яких прагнуть, але досягнути важко. Тому в ряді систем досягається інваріантність не повна, а часткова, або система інваріантна до ε, де під ε вважаємо похибку системи. Система, інваріантна до ε - це така система, в якій зберігаються межі абсолютно інваріантної системи і існує динамічна похибка δ, що характеризує міру інваріантності. Користуючись основними визначеннями, згідно з теорією інформації, можна

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

вказати таку абсолютно інваріантну систему, яка буде відрізнятися від вихідної наявністю динамічної похибки (при максимально необхідній кількості інформації *ΔH*). Порівняння таких систем для однієї множини вхідних сигналів дозволить отримати оцінку інваріантності. Використовуючи оцінки інваріантності до ε (міра ε-інваріантності), отримаємо вираз, що визначає необхідну кількість інформації *ΔH*:

$$\Delta B = K\left(\log\frac{\delta_1}{\bar{\delta}_1} + \log\frac{\delta_2}{\bar{\delta}_2} + ... + \log\frac{\delta_n}{\bar{\delta}_n} \right), \quad (3)$$

де δ_i – можливі середньоквадратичні відхилення контрольованих параметрів інформаційної мережі від необхідних значень;

$\bar{\delta}_i$ – середньоквадратична допустима похибка контрольованих параметрів інформаційної мережі від необхідних значень; $i = \overline{1,2,...n}$;

K – коефіцієнт, який залежить від типу каналу зв'язку.

Тоді, середня кількість інформації, яку необхідно передати в системі управління, повинна дорівнювати сумі виразів (2) і (3), при цьому буде забезпечено як властивість адаптивності, так і інваріантності.

Запропонований підхід дозволяє знайти необхідний мінімум інформації, при якому параметри мережі матимуть задану точність. З точки зору теорії інформації і динамічної точності необхідно, щоб система управління забезпечувала задану точність параметрів мережі при мінімальному обсязі управляючої інформації.

Тому інформаційно-ентропійний метод дозволяє визначити запропонованим методом кількість управляючої інформації у системі управління будь-якої мережі ІТ центру. Таку оцінку за допомогою інших практичних методів майже неможливо отримати, так як обмежена кількість вихідних даних, особливо для мереж, на яких застосовуються різні технології. Практична цінність забезпечується можливістю врахування обсягу керуючої інформації з переліком вимог до точності параметрів основної мережі. Така оцінка визначається дисперсією відхилення від математичного очікування. Чим більші вимоги до точності параметрів управляючої мережі, тим потрібний більший обсяг управляючої інформації.

Запропоновано комбіновану структуру системи управління (рис.2), яка дозволяє керувати мережею ІТ центру у двох режимах одночасно, поєднуючи як властивості інваріантності, так і адаптивності параметрів мережі.

Інформаційно-ентропійний метод не залежить від характеру і кількості об`єктів управління та їх параметрів, є універсальним. Для розрахунку обсягу управляючої інформації за вказаним методом розроблено алгоритм головної процедури рис.3.

Висновок

В статті висвітлено шляхи створення системи управління мережами ІТ центру, як технологічної системи, що реалізує з необхідною якістю ефективне надання інформаційних послуг, їх захист від несанкціонованого доступу, засекречення потоку даних, що забезпечує захищеність інформації, цілісність з'єднання з відновленням, попередження від відмов тощо.

Розглянуто принципи побудови захищеної системи управління мережами ІТ центру.

Запропоновано до застосування інформаційно-ентропійний метод для визначення одного із основних параметрів СУ мережами ІТ центру - кількість управляючої інформації. Іінформаційно-ентропійний метод не залежить від характеру і кількості об`єктів управління та їх параметрів, є універсальним.

Наведено комбіновану структуру системи керування, яка забезпечує систему управління мережами ІТ центру в двох режимах.

Для розрахунку обсягу управляючої інформації розроблено алгоритм головної процедури.

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019

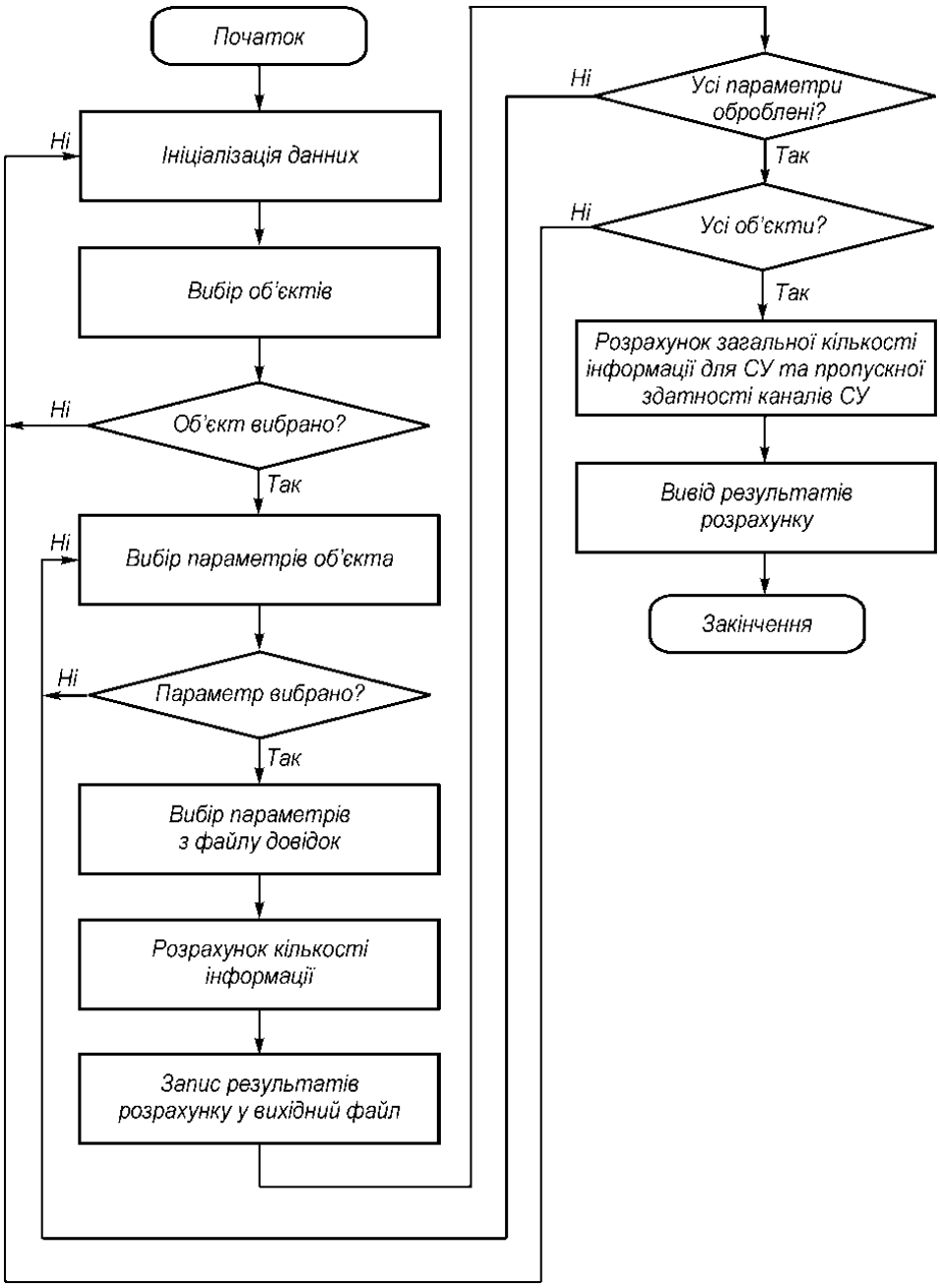

Рис.3. Алгоритм головної процедури

Перелік посилань

1. Методи оптимізації: Підручник для вищих навчальних закладів за напрямом «Телекомунікації»/ В.Б. Толубко, Л.Н. Беркман – ДУТ, 2016. – 442 с.

2.Стеклов В. К., Беркман Л. Н. Проектування телекомунікаційних мереж. - К.: Техніка,2002.- 792 с.

3.Сучасні системи управління в телекомунікаціях. Монографія/ В.К.Стеклов, Л.Н. Беркман, Б.Я.Костік - К.: Техніка, 2005. – 400 с. .

4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": Закон України від 05.10.94 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286 зі змінами від 27.03.14 № 1170-VII // ВВР –2014 –№22 – ст. 816.

Надійшла: 20.07.2019 Рецензент: д.т.н., проф. Савченко В.А.

© Л.Н. Беркман, Я.О. Прийма, Н.С. Чумак, В.Є. Дмітрієв, О.О. Щедрова, А.А. Ярчук, 2019