УДК 004.5

А. В. Бойченко
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Вимоги до систем моніторингу факторів впливу на живучість

Визначено фактори впливу на живучість і розглянуто існуючі засоби моніторингу розподілених комп'ютерних мереж. Сформовано вимоги до систем моніторингу факторів впливу на живучість. Запропоновано узагальнену архітектуру комплексної системи моніторингу.

Ключові слова: *живучість, система моніторингу, вимоги до програмного забезпечення.*

Опис факторів впливу на живучість

В умовах неперервного зростання кількості та якості інформаційних систем як у сфері державного управління, так і в економіці проблема моніторингу факторів впливу на живучість набуває особливого значення. Це підтверджується великою кількістю публікацій, присвячених дослідженню живучості як в Україні, так і за кордоном. Головними напрямками досліджень є ефективність використання різних методів підвищення живучості: динамічна зміна конфігурації, метод ізоляції тощо. У випадку розподілених комп'ютерних мереж багато уваги приділяється впливу на живучість різних комунікаційних протоколів [11], а також вимог до програмного забезпечення [4, 5, 10]. При цьому, недостатньо уваги приділено питанням моніторингу факторів впливу на живучість та інтеграції окремих програмних модулів до системи забезпечення живучості.

Під живучістю системи розуміють її здатність зберігати повну або часткову працездатність в умовах впливу несприятливих факторів (виведення з ладу елементів системи, відмови, критичне збільшення робочого навантаження тощо). Зокрема, живучість, як властивість розподіленої комп'ютерної системи (РКС), характеризує її здатність обирати оптимальний режим функціонування за рахунок власних внутрішніх ресурсів, перебудови структури, зміни функцій та поведінки окремих підсистем у зв'язку зі зміною зовнішніх умов і відповідно до цілі її функціонування [1–3, 12].

Під живучою розподіленою комп'ютерною системою (далі — ЖРКС) будемо розуміти таку, однією із системних характеристик якої є живучість.

Під фактором впливу на живучість (далі — ФВЖ) будемо розуміти зміну умов роботи ЖРКС, яка призводить до підвищення або зниження її живучості.

Під системою моніторингу факторів впливу на живучість (далі — СМФ) будемо розуміти програмно-апаратну систему, яка виконує моніторинг ФВЖ.

Під вимогою до системи моніторингу будемо розуміти можливість, яка очікується розробниками від СМФ.

Виділимо основні етапи створення системи моніторингу живучості:

1) визначення цілей, стратегії й загальної політики щодо моніторингу живучості;

2) аналіз і розробка вимог;

3) визначення методики проектування — крок, призначенням якого є вибір методів розпізнавання та аналізу ФВЖ і способу їхнього застосування для наступних кроків, яка задовольнятиме вимогам, сформульованим у п. 2;

4) проектування СМФ на основі систематичного застосування обраних на попередньому кроці методів аналізу ФВЖ;

5) реалізація системи та інтеграція її з іншими підсистемами ЖРКС. Даний крок має бути підтриманий підготовкою програм із навчання співробітників, адміністраторів і персоналу служб керування інформаційною безпекою;

6) функціонування СМФ, що охоплює сукупність процедур і дій, таких як: перевірка погодженості засобів системи і їхньої відповідності сформованим вимогам, контроль за коректністю роботи СМФ, перегляд проектних і експлуатаційних рішень за результатами експлуатації, супровід (триваюча розробка) засобів СМФ, відстеження позаштатних ситуацій і реакція на них.

Живучість забезпечується досконалістю підсистеми комунікації ЖРКС (як у технічному, так і в організаційному аспектах), прогнозуванням негативних явищ і вжиттям превентивних заходів з їхнього відвернення, розробкою сценаріїв дій у надзвичайних ситуаціях, наявністю резервних ресурсів, а також рівнем підготовки, самовідданістю та професіоналізмом персоналу [8].

Показником живучості для ЖРКС прийнято вважати мінімальну кількість елементів системи (вершинна зв’язність) або зв’язків між ними (реберна зв’язність) [13, 14], вихід котрих із ладу веде до порушення зв’язності структури системи.

Особливості процесу моніторингу

Моніторинг факторів впливу на живучість, є чинником, який дозволяє досліджувати поточний рівень живучості системи та прогнозувати майбутній.

Інформація СМФ потребує щоденного аналізу з боку системного адміністратора. В іншому випадку реакція на ФВЖ виявиться спізнілою.

Моніторинг передбачає:

— збір даних із різних джерел;

— визначення кореляцій;

— виявлення ознак ФВЖ.

Стан живучості системи у будь-який момент часу характеризується параметрами, сукупність яких дає змогу оцінити його функціональну відповідність завданням, що розв’язуються ЖРКС. У той же час оцінка цих параметрів вміщує

оцінку відповідних параметрів складових ЖРКС. Таким чином, характеристику живучості, можна записати [7]:

$$S = f\,(S_{O1}, S_{O2}, ..., S_{ON}),$$

де S_{ON} — характеристика стану N-го об'єкта ЖРКС, визначена як

$$S_{0N} = f\,(S_{ON1}, S_{ON2}, ..., S_{ONM}, P_{O1}, P_{O2}, ..., P_{OL}\,),$$

де S_{ONM} — характеристика стану M-го об'єкта ЖРКС, підпорядкованого N-му об'єктові, у загальному випадку визначається як

$$S_{ONK} = f_O\,(P_{O1}, P_{O2}\,, ..., P_{OL}\,),$$

де P_{OL} — L-й параметр оцінки стану об'єкта контрольованої системи. Оцінка стану контрольованої системи є основним призначенням моніторингу, що реалізується через:

— організацію семантично й технологічно узгодженої актуалізації інформації про стан складових ЖРКС як записів територіально-розподільної бази даних;

— надійне зберігання цієї інформації в стандартизованій формі;

— забезпечення необхідних умов для оперативного застосування поточної інформації об'єктів ЖРКС шляхом використання захищених протоколів передачі даних.

Для виявлення ФВЖ може використовуватися модель, яка є розширенням «Моделі виявлення порушення безпеки» [9]. Модель включає 6 основних компонентів:

S — суб'єкти, що ініціюють діяльність у системі (користувачі чи процеси);

O — об'єкти, що складають ресурси системи — файли, мережеві пакети, обладнання;

R — записи, які генеруються внаслідок певних дій суб'єктів чи зміни стану об'єктів;

P — профілі — структури, які характеризують поводження суб'єктів чи стан об'єктів у термінах статистичних і поведінкових моделей;

A — аномальні дані, що характеризують виявлені випадки ненормального поводження чи ненормального стану;

L — правила функціонування СМФ при обробці інформації.

Основною метою моделі є формулювання характеристик нормального поводження системи для наступного виявлення ФВЖ.

R — сукупність записів, кожна з яких у моделі представляє 6-мірний вектор, компоненти якого містять наступну інформацію:

<суб'єкт; дія; об'єкт; умови для надання виключення;
лист використання ресурсів; час>,

де зміст компонентів наступний.

Дія — операція, яку здійснює суб'єкт і об'єкт.

Умови для надання виключення визначають, що додатково необхідно зробити суб'єктові, щоб одержати необхідний доступ.

Лист використання ресурсів може містити, наприклад, час зайнятості CPU (центрального процесора).

Час — унікальна мітка часу та дати, коли відбулася дія.

Системні визначення передбачають формування образу ЖРКС. Визначення основних можливостей передбачає формування переліку функцій ЖРКС, припинення яких призведе до зниження заданого рівня живучості, а визначення другорядних можливостей передбачає формування переліку функцій ЖРКС, припинення яких, навпаки, не призведе до зниження такого рівня. Аналіз живучості передбачає аналіз можливості збереження та відновлення системи.

Життєвий цикл моніторингу складається з 4-х фаз (рис. 1):

1) ідентифікації ресурсів і проблем;

2) визначення основних можливостей (істотні, несуттєві; проблемні області, способи їхнього усунення й ін.);

3) визначення другорядних можливостей (істотні, несуттєві; проблемні області, способи їхнього усунення й ін.);

4) аналізу живучості (виявлення тенденцій із використання ресурсів, визначення динаміки росту, вироблення політики).

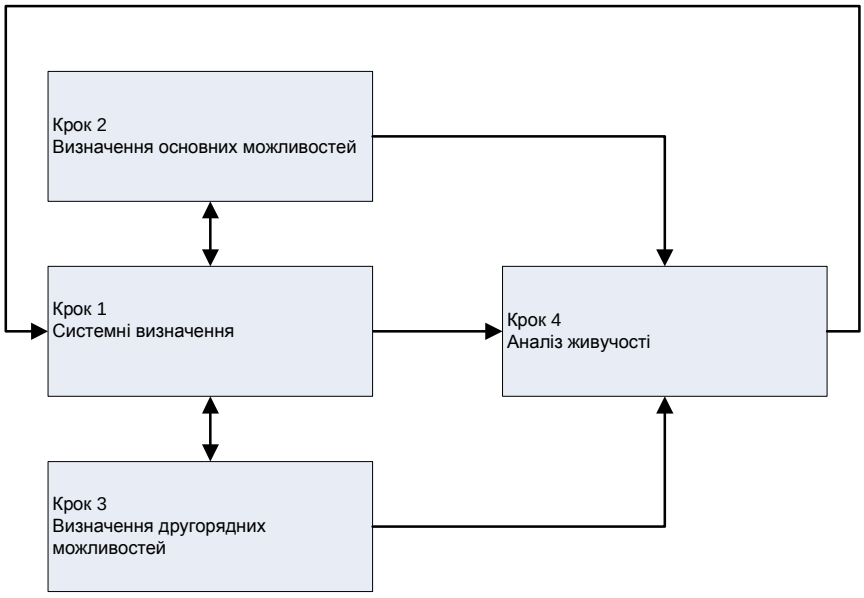

Рис. 1. Етапи моніторингу живучості

Аналіз пов’язаний із вибором однієї з можливих альтернатив серед усіх можливих станів ЖРКС, за допомогою переходу до якої можливе досягнення потрібного рівня живучості.

При цьому, звичайно, потрібно враховувати, що ФВЖ можуть суттєво відрізнятися один від одного (за небезпечністю даного ФВЖ, за частотою виникнення, складністю розпізнавання тощо), крім того, вони можуть мати різний закон розподілу. Тому при формуванні переліку вимог потрібно враховувати коефіцієнт складності розпізнавання ФВЖ, і враховувати його для обчислення планової продуктивності СМФ.

Методичну основу моніторингу живучості складають методи аналізу ризиків, які передбачають аналіз вхідних даних, (інформаційні об'єкти ЖРКС, типи ФВЖ й ін.).

Формування вимог до системи моніторингу

Сформулюємо основні вимоги до СМФ, зображеної на рис. 2.

На рис. 2. показані джерела формування вимог до системи моніторингу: вимоги користувачів, системні вимоги, проектна специфікація [6].

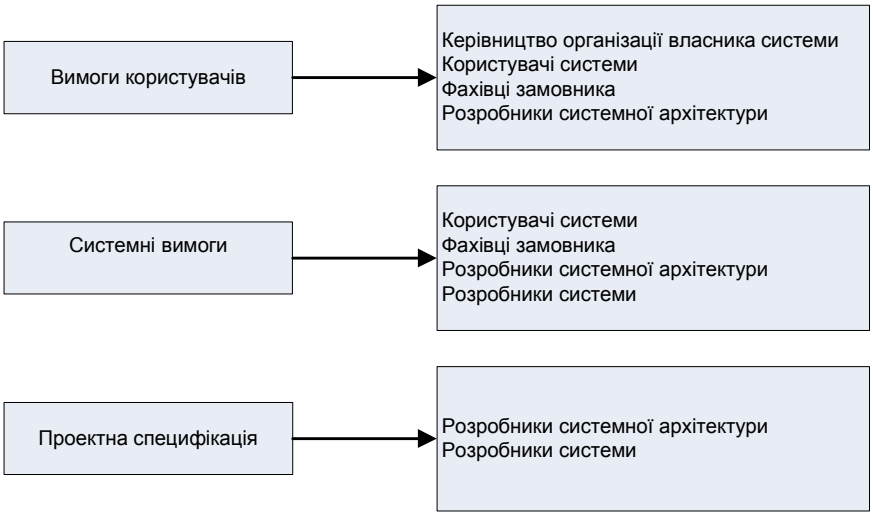

Рис. 2. Джерела формування вимог до СМФ

Результатом формування є документ, у якому сформульовано всі типи вимог, у відповідності з обраними стандартами проектування [6], згруповані наступним чином:

— функціональні;
— інтерфейсні;
— до продуктивності;
— специфічні;
— характеристики якості;
— інші.

Функціональні вимоги:

— збір даних: система моніторигу повинна забезпечувати безперервне отримання даних щодо ФВЖ, як у середині ЖРКС, так і за її межами;

— визначення кореляцій: СМФ повинна забезпечувати автоматичне виявлення залежностей між окремими ФВЖ;

— виявлення ознак ФВЖ: СМФ повинна забезпечувати введення ознак ФВЖ до БД та їхнє автоматичне розпізнавання;

— інформування користувачів: СМФ повинна забезпечувати надсилання повідомлень до визначених користувачів електронною поштою (протокол SMTP) чи

шляхом надсилання мережевих повідомлень (для користувачів, які знаходяться в локальній мережі);

— інформування системи керування: СМФ повинна забезпечувати передачу до системи керування повідомлень при виникненні ФВЖ;

— збереження даних: СМФ повинна мати механізми для збереження інформації до БД та наступного її отримання.

Інтерфейсні вимоги:

— вимоги до інтерфейсів користувачів;

— вимоги до апаратних інтерфейсів;

— вимоги до програмних інтерфейсів;

— вимоги до комунікаційних інтерфейсів.

Вимоги до продуктивності:

— кількість і характеристики об'єктів моніторингу;

— максимальна кількість користувачів СМФ;

— максимальна кількість одночасно відкритих файлів.

Специфічні вимоги залежать від особливостей комп'ютерної системи, у якій здійснюється моніторинг. Їх можна згрупувати наступним чином:

— відповідність стандартам, за якими створюється комп'ютерна система;

— особливості апаратного забезпечення ЖРКС.

Основними характеристиками якості СМФ будемо вважати:

— коректність реалізації;

— ефективність;

— гнучкість;

— захищеність;

— здатність до взаємодії;

— переносність;

— достовірність;

— здатність повторного використання;

— здатність до тестування;

— простоту використання.

Додатково доцільно визначити ще ряд вимог:

— вимоги до БД СМФ (граничний обсяг, кількість записів);

— вимоги до адаптації та інсталяції СМФ.

Для забезпечення аналізу живучості система моніторингу повинна надавати можливість опису:

— інформаційних процесів ЖРКС;

— користувачів і їхніх функцій, підметів автоматизації в прив'язці до структури ЖРКС;

— інформаційних і фізичних об'єктів мережі;

— сценаріїв виконання інформаційних функцій;

— станів системи;

— матрицю взаємозв'язків між ФВЖ.

Виконання моніторингу живучості й виявлення ФВЖ вимагає наявності в складі СМФ підсистеми формування звітності, необхідної для діагностики мережі й одержання статистичного представлення про її живучість. Звіти формуються на основі записів про виявлені фактори, містять обов'язково часові мітки та характе-

ристики ФВЖ. Звіти мають відображатися в текстовій та графічній формі, і бути пристосованими до легкого експорту в інший формат. До складу звітів, які формуються СМФ, повинні входити:

1) звіт про виявлені ФВЖ — має показувати докладну статистику про розпізнані системою факторів впливу на живучість за заданий проміжок часу, включаючи такі параметри, як тривалість фактору та інші статистичні дані;

2) звіт контролю живучості —має показувати статистику інтегрального показника живучості за заданий період часу;

3) звіт про відновлення живучості — має включати інформацію про заходи, які були ініційовані в системі, з метою подолання негативних ФВЖ і відновлення живучості системи;

4) звіт про поточний стан живучості — має показувати всі активні на даний момент часу фактори;

5) загальний звіт — має показувати загальну тривалість факторів впливу на живучість і загальну кількість повністю чи частково нейтралізованих, виявлених із запізненням ФВЖ. Звіт має бути доступним у графічній і текстовій формі.

Конкретизація факторів, які відслідковуються СМФ

Основними ФВЖ, які мають відслідковуватися СМФ, доцільно визначити ті фактори, які призводять до порушення цілісності інформаційного ресурсу ЖРКС:

— порушення цілісності окремих компонентів ЖРКС (пристроїв, обладнання);

— порушення цілісності, у тому числі умисна модифікація інформаційних ресурсів (програмного забезпечення також);

— переривання передачі потоку даних (трафіка);

— виконання ініціації фіктивного з'єднання;

— неправомірна зміна режимів роботи ЖРКС (її окремих компонентів, обладнання, програмних засобів тощо), ініціювання технологічних чи тестувальних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації).

Причинами таких ФВЖ можуть бути:

— зміна умов фізичного середовища (стихійні лиха: землетрус, повінь, пожежа й аварії або інші випадкові події);

— збої та відмови в роботі обладнання та технічних засобів ЖРКС;

— наслідки помилок під час проектування та розробки компонентів ЖРКС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

— впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання та т.п.).

Показники роботи живучої розподіленої комп'ютерної системи, які відслідковуються СМФ

Основними показниками роботи ЖРКС, які мають відслідковуватися СМФ доцільно визначити показники цілісності та доступності інформаційного ресурсу:

— доступність елемента ЖРКС;

— доступність інформаційного ресурсу;

— час реакції, який визначається як час між виникненням запиту до якого-небудь мережевого сервісу й отриманням відповіді на нього;

— пропускна спроможність, яка відображає об'єм даних, переданих мережею за одиницю часу;

— затримка передачі, яка рівна інтервалу між моментом надходження пакета на вхід якого-небудь мережевого пристрою й моментом його появи на виході цього пристрою;

— доступність, передбачених у ТЗ мережевих сервісів.

Архітектура системи моніторингу

На основі сформованих вище вимог можна запропонувати архітектуру системи моніторингу факторів впливу на живучість. Оскільки ЖРКС представляє собою класичну територіально розподілену комп'ютерну мережу, яка взаємодіє з іншими мережами, наприклад, Internet (рис. 3), і має розвинені засоби адміністрування та зберігання даних, доцільно будувати СМФ, базуючись на доступних засобах моніторингу.

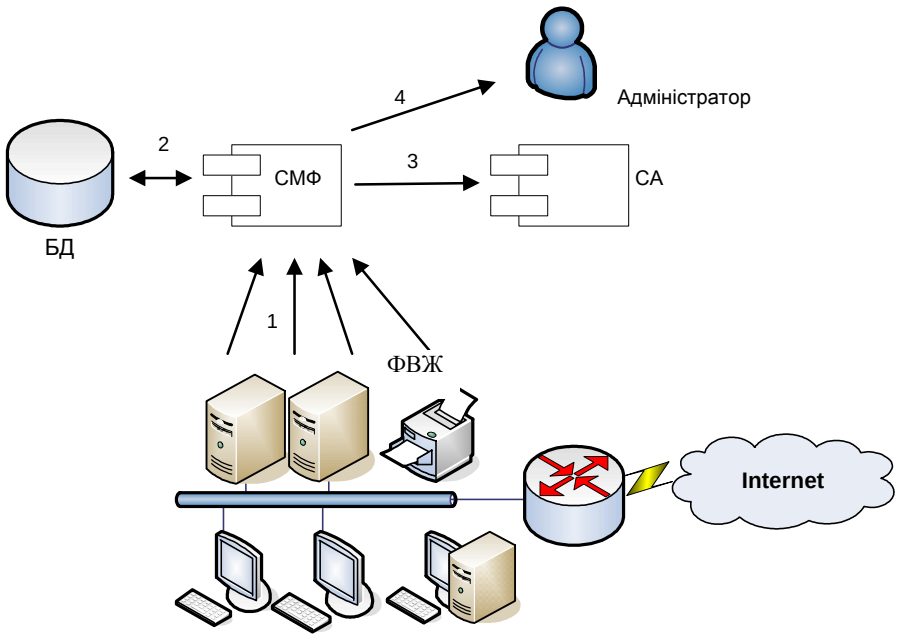

Рис. 3. Інформаційна взаємодія СМФ: 1 — СМФ отримує дані з різних джерел; 2 — СМФ використовує БД для зберігання інформації; 3 — СМФ надає інформацію щодо ФВЖ до СА; 4 — СМФ надає інформацію щодо ФВЖ адміністратору системи

ЖРКС належать до класу великих організаційно-технічних систем, які характеризуються великою розмірністю та розподіленістю в просторі, великими обсягами інформації, що передається та обробляється, паралельністю виконання процесів обробки інформації, функціонування та управління. Для сучасних ЖРКС характерна проблемна (функціональна) орієнтація програмного забезпечення та банків даних різних рівнів ієрархії. Необхідною ознакою ЖРКС є обов'язкова на-

явність функції обміну даними як основи для забезпечення інформаційної взаємодії між територіально-розподіленими обчислювальними комплексами різних підсистем.

СМФ включає програмні та апаратні засоби, необхідні для виконання її основної функції — моніторингу ЖРКС. Інформаційна взаємодія СМФ із ЖРКС, СА, адміністратором та БД представлена на рис. 3.

При дослідженні ЖРКС доцільно виділяти фізичний та логічний рівень. Фізична архітектура ЖРКС описує структуру, призначення та взаємодію протоколів фізичного, канального, мережевого, транспортного та сеансового рівнів семирівневої еталонної моделі мережевої взаємодії.

Логічна архітектура описує структуру та взаємодію програмних засобів мережі, що представляється прикладним і представницьким рівнями семирівневої еталонної моделі мережевої взаємодії.

Огляд засобів моніторингу

Основні властивості існуючих засобів моніторингу приведені в таблиці.

Характеристики засобів моніторингу

Система моніторингу	Основні властивості
Remstats	СМФ для РКС, які включають багато серверів і маршрутизаторів. Основу системи складають додатки трьох категорій: — сервери (збір інформації безпосередньо на вилучених машинах (дані від df, uptime, netstat, uname, ps), аналіз лог-файлів)); — колектори (збір даних від програм-серверів, по SNMP, перевірка сервісів і досяжності); — програми монітори (відстеження критичних ситуацій (алертів) і оповіщення про проблеми). Дані про поточний стан усієї РКС і її підсистем представлені у вигляді таблиць і графіків, побудованих із використанням програми RRDtool.
Alertmon	СМФ для моніторингу групи рознесених по мережі UNIX серверів, дозволяє визначати позаштатні ситуації, про які автоматично повідомляється адміністраторові, ведеться журнал проблем, і автоматично починаються спроби відновити нормальний режим роботи. На кожному із серверів з alertmon здійснюються функції спостереження за роботою «сусідів», що дозволяє створити розподілену систему моніторингу з можливістю централізованого спостереження за станом кожної ЕОМ в ЖРКС.
Nagios (стара назва — NetSaint) Network Monitor	Програма моніторингу працездатності хостів і сервісів РКС (SMTP, POP3, HTTP, NNTP, PING). Моніторинг виконується через набір зовнішніх компонент. Має зручний web-інтерфейс. Звіт про виявлені проблеми направляється на e-mail чи на мобільний пристрій. Є русифікована версія.
NCM — Network Complex Monitor	Система комплексного моніторингу ЖРКС і її компонентів. На даний момент дозволяє моніторити: BGP, VOIP, хости, сервіси. У розробці використовується MySQL і PHP.

Продовження таблиці

Netinfo — система керування та моніторингу мережі	Netinfo — багатофункціональний універсальний засіб керування РКС, що дозволяє гнучко набудовувати параметри ЛОМ, контролювати роботу мережних сервісів, окремих сегментів мережі, машин і спеціалізованого устаткування. Для роботи потрібно PHP і PostgreSQL.
NetMon — NETwork MONitoring system	СМФ для IP-мережі. NETMON дозволяє контролювати в реальному часі працездатність РКС, яка складається з багатьох різнотипних об'єктів — маршрутизаторів, інтерфейсів, BGP-шлюзів, хостів і їхніх сервісів. За допомогою NETMON можна відслідковувати стан таких об'єктів, збирати значення всіляких лічильників, визначати події і реакцію на них, зберігати історію роботи РКС.
NetMon (NETwork MONitoring Dealer)	Програма, що виконує роль посередника між низькорівневим моніторингом мережі й інтерфейсом оператора або базою даних. Концентрує дані про стан РКС, періодично опитуючи різними способами всілякі мережні об'єкти, формалізує отримані дані й забезпечує уніфікований інтерфейс доступу до їхніх значень. Може використовуватися як первинне джерело даних й одночасно як підсистема оповіщення про події, що відбуваються, у загальній СМФ ЖРКС.
hqmon	СМФ розроблена для моніторингу працездатності ресурсів РКС, таких як: продукція Cisco Systems, канали зв'язку між Cisco, bgp-сесії, сервіси. Інформація від пристроїв збирається по SNMPv1.
NetXMS	Система моніторингу ФВЖ, розроблена для роботи у великих ЖРКС. Особливості даної СМФ: — трирівнева архітектура; — збір інформації через SNMP і власних агентів (на більшості UNIX систем, включаючи комерційні, а також Windows і IPSO); — централізоване відновлення агентів; — гнучка система розмежування доступу; — гнучка система обробки подій; — можливість збору інформації (включаючи SNMP) з мереж, що знаходяться за NAT-ом через проксі-агента; — шифровані комунікації; — підтримка кластерів (міграція ресурсів між нодами і т.п.); — ядро системи й агенти можуть переноситися між POSIX-сумісними системами. Модульна архітектура дає можливість легкого розширення функціональності.
Zenoss — Open Source Network/Systems Monitoring	Розповсюджується під ліцензією GPL система моніторингу інфраструктури РКС. При створенні ЖРКС може використовуватися в якості відкритої альтернативи продуктам IBM Tivoli, HP OpenView, BMC Patrol. Програма написана мовою Python із використанням Zope, у якості СУБД використовується MySQL 5.0.x. У web-інтерфейсі активно використовуються Ajax технології. У програмі можна використовувати модулі моніторингу від системи Nagios, а також одержання інформації про стан об'єктів використовуючи SNMP, SNMP Trap, Ping/ICMP, SSH/Telnet, Syslog, WMI, XML/RPC інтерфейс.

Продовження таблиці

WifiScanner	Сканер безпровідної мережі для виявлення точок доступу й активних кінцевих клієнтів. Працює під Linux, з більшістю драйверів безпровідних пристроїв (Cisco, Hermes/Orinoco, Atheros, Centrino, PrismII і т.п.). Результат може бути представлений як в інтерактивному режимі, так і у вигляді звіту чи графіка.
Munin	Пакет для моніторингу змін характеристик ЖРКС у вигляді графіків. Складається із клієнтської частини, установлюваної на машинах, для яких потрібно будувати графіки, і серверної, яка збирає інформацію з клієнтів і представляє дані у вигляді графіків з доступом через web-інтерфейс. Написана на perl, графіки будуються за допомогою RRDTool.
Netwhistler	Програма по заданій масці, сканує всі адреси мережі й малює за отриманими даними структуру взаємодії хостів у вигляді карти, на якій відбиває статус пристроїв. Програма здійснює перевірку досяжності хоста, роботи типових сервісів, аналізує дані, які можна одержати по SNMP. Написана на Java.
Bandwidth	Програма для контролю за трафіком кінцевих користувачів. Будує зведені таблиці (html) і графіки по кожному користувачеві (як по IP, так і по підмережі) з розбивкою за днями, тижнями й місяцями. На кожному графіку деталізований вид трафіка: HTTP, TCP, UDP, P2P і т.д.
Big Sister	Система моніторингу та контролю за станом машин у мережі. Контроль здійснюється через web-інтерфейс, є присутнім система нотифікації у випадку виникнення збою.
Zabbix	GPL система моніторингу роботи додатків і хостів у РКС. Стан мережі й сервісів відображається на графіку у вигляді динаміки зміни. Дані з хостів передаються або шляхом запиту із сервера моніторингу, або через посилку SNMP trap. Присутня гнучка система оповіщення.
RANCID	Призначена для віддаленого моніторингу конфігурації маршрутизаторів Cisco, Alteon, Bay Networks, Juniper і т.д. Конфігурація періодично забирається з віддалених пристроїв, зміни відслідковуються й містяться в CVS-репозиторії.
SysOrb	Система моніторингу складається з 3-х частин: — сервер для перевірки віддалених хостів (статистика через SNMP, активність HTTP, ICMP, SMTP, Generic TCP); — клієнти для збору локальної статистики (Uptime,Load Average, Free space, Free memory, Process presence); — скрипт для представлення накопичених і поточних даних за допомогою web-інтерфейсу.
Net Matrix	Система для моніторингу роботи маршрутизаторів CISCO на php.
Autostatus	Невелика програма для моніторингу працездатності ЕОМ у мережі і перевірки активності наданих ними видів сервісу.
Scotty	Система керування та спостереження за станом різних компонентів ЖРКС. Складається з 2-х частин: TnmTcl Extension — доступ до інформації з SNMP, ICMP, DNS, HTTP, RPC, NTP, UDP і Tkined — система мережного керування та контролю.

Продовження таблиці

BigBrother	Багатофункціональна система мережевого моніторингу.
NOCOL/SNIPS	Система моніторингу функціонування DNS-серверів, TCP-портів, продуктивності, журналів ОС, Radius-серверів, BGP, ICMP, RPC, NTP, джерел безперебійного живлення, SNMP у складі РКС.
SecureNet	Система діагностики та керування станом РКС.
MON	Стежить за працездатністю РКС і при збоях оповіщає адміністратора. Види підконтрольних служб: ping, telnet, ftp, smtp, http, nntp, pop3, imap, disk space, SNMP.
Netdisco	Засіб для контролю топології мережі через автоматизоване визначення структури, використовуючи SNMP. Дозволяє визначати по заданому IP або MAC адресу і номер порту на комутаторі, вмикати/вимикати порти, будувати карту РКС і т.д.

Кожен із приведених засобів дозволяє виконувати ту чи іншу задачу моніторингу та формування звітності, виявляти певні фактори впливу на живучість. Але жоден із них не є комплексною системою моніторингу ФВЖ, яка б задовольняла сформульованим вище вимогам.

Висновки

Моніторинг факторів впливу на живучість відіграє надзвичайно важливу роль в удосконаленні методів організації інформаційної взаємодії в розподілених комп'ютерних системах. Одним із головних етапів створення будь-якої системи моніторингу факторів впливу на живучість є формування вимог до неї. Враховуючи особливості функцій, які реалізуються СМФ, складність сучасного апаратного та програмного забезпечення та особливості задачі моніторингу можна виділити наступні групи вимог:

— функціональні;
— інтерфейсні;
— вимоги щодо продуктивності;
— специфічні;
— характеристики якості;
— інші.

Однією з головних функцій систем моніторингу факторів впливу на живучість є аналіз даних системного аудиту, формування розширеної звітності про стан живучості та функціонування в режимі реального масштабу часу.

Існуючі засоби моніторингу розподілених комп'ютерних систем не відповідають повністю сформульованим вимогам, і можуть бути інтегровані до СМФ у якості окремих підсистем. Коректна реалізація вимог до систем моніторингу факторів впливу на живучість дозволить створити ефективний механізм підвищення живучості в розподілених комп'ютерних системах.

1. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С.* Введение в теорию живучести вычислительных систем. — К.: Наук. думка, 1990. — 184 с.

2. *Кузнєцова М.Г.* Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 8, № 3. — С. 40–47.

3. *Mead N., Ellison R., Linger R., Longstaff T., Mc Hugh J.* Survivable Network Analysis Method. TECHNICAL REPORT. CMU/SEI-2000-TR-013. ESC-2000-TR-013. 2000. 00tr013.pdf

4. *Varner P., Knight J.* Security Monitoring, Visualization and System Survivability // Department of Computer Science University of Virginia, 2001. — Varner-10-09.pdf.

5. *Lipson H.* Evolutionary Systems Design: Recognizing Changes in Security and Survivability Risks. — CERT, 2006. — 06tn027.pdf

6. *Соммервил И.* Инженерия программного обеспечения. 6-е изд. / Пер. с англ. — М.: Издательский дом «Вільямс», 2002. — 624 с.

7. *Андрейчук Н.Д., Бурков Ю.Ю.* Застосування технологій Internet для моніторингу стану складних систем шляхом використання розподільних баз даних // Стратегічна Панорама. — 1999. — № 3. — С 151–154.

8. *Дудко С.* Параметричний підхід до аналізу системи управління // Вісник державної служби. — 2002. — № 3. — С. 69–73.

9. *Denning D.* An Intrusion Detection Model // IEEE Transactions on Software Engineering. — 1987, Feb. — Vol. SE-13, N 2. — P. 222–232.

10. *Nancy R.* Mead, Requirements Engineering for Survivable System. Technical Note CMU/SEI-2003-TN-013 // Carnegie Mellon University, 2003.

11. *Abdur Chowdhury, Ophir Frieder, Peng-Jun*. On the Design, Development, Deployment,and Network Survivability Analysis of the Dynamic Routing System Protocol. Department of Computer Science. Illinois Institute of Technology. — http://www.ir.iit.edu/publications/downloads/DRS-NSA-SUPE.pdf.

12. *Громов Ю.Ю., Винокуров Д.Е., Самхарадзе Т.Г., Пасечников И.И.* Анализ живучести информационных сетей информационные процессы и управление. — Тамбов: Тамбовский государственный технический университет, 2006. — № 1.

13. *Рябинин И.А*. Надежность и безопасность структурно-сложных систем. — СПб.: Политехника, 2000.

14. Моделирование живучести систем энергетики: методология, модель, реализация. Сообщения по прикладной математике. — М.: ВЦ АН СССР, 1986.

Надійшла до редакції 12.12.2007