ІНФОРМАЦІЙНІ СИСТЕМИ, МЕРЕЖІ ТА ТЕХНОЛОГІЇ

УДК 004.7, 658.012.324

І. І. Пастернак
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ДІАГНОСТИКА ТА НАЛАГОДЖЕННЯ ВУЗЛІВ КОРПОРАТИВНОЇ МЕРЕЖІ КІБЕРФІЗИЧНИХ СИСТЕМ

Розглянуто переваги та недоліки сучасних засобів реалізації середовищ діагностики. Запропоновано спеціалізоване середовище діагностики та налагодження вузлів корпоративної мережі. Програмно реалізовано модулі, які в короткі терміни дають змогу діагностувати проблему та усунути її без участі людини. Розроблено чіткий механізм виявлення відхилень у роботі корпоративної мережі та сповіщення про них системного адміністратора. Створено базу даних, в яку записують стан вузлів корпоративної мережі та дані про них. Досягнуто стабільної роботи завдяки простій структурі середовища та зв'язку з його модулями. Створено веб-інтерфейс для зручного огляду вузлів корпоративної мережі та з можливістю їх групування за категоріями.

Ключові слова: корпоративна мережа, клієнт, сервер, кіберфізична система.

The advantages and disadvantages of existing means to date of implementation environments diagnosis. A specialized diagnostic and debugging environment node corporate network. Program implemented modules that allow to quickly diagnose the problem and fix it without human intervention. Developed a clear mechanism of abnormalities in the corporate network and notifies you about your system administrator. Established database, which recorded the state of the corporate network nodes and data about them. Reached a stable operation with a simple structure and environment because of its modules. A web interface for easy inspection units and the corporate network with the possibility of grouping them by category.

Key words: corporate network, client, server, cyber physics system.

Вступ

Діагностика корпоративної мережі – процес (безперервний) аналізу стану інформаційної мережі. У разі виникнення несправності мережевих пристроїв фіксується факт несправності, визначається її місце і вид. Повідомлення про несправності передається, пристрій чи вузол відключається і замінюється резервним або налагоджується. Постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної комп'ютерної мережі, необхідний для підтримки її в працездатному стані. Контроль – це необхідний перший етап, який повинен виконуватися під час управління мережею. Зважаючи на важливість цієї функції, її часто відокремлюють від інших функцій і реалізують спеціальними засобами. Такий поділ функцій контролю корисний для невеликих і середніх мереж. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки й пристрої мережі, а їх вимкнення або реконфігурацію він може виконувати у такому разі вручну. Також у деяких випадках автономний засіб може діагностувати проблему та виправити її.

Процес контролю роботи мережі зазвичай поділяють на два етапи – моніторинг і діагностика. На етапі моніторингу виконується простіша процедура – процедура збирання первинних даних про роботу мережі: статистики про кількість кадрів і пакетів різних протоколів, що циркулюють у

мережі , стан портів концентраторів, комутаторів і маршрутизаторів тощо. Далі виконується етап діагностики, під яким розуміють складніший й інтелектуальніший процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі. Завдання моніторингу вирішуються програмними і апаратними вимірниками, тестерами, мережевими аналізаторами, вбудованими засобами моніторингу комунікаційних пристроїв, а також агентами систем управління. Завдання діагностики потребує активнішої участі людини і використання таких складних засобів, як експертні системи, що акумулюють практичний досвід багатьох мережевих фахівців.

Очевидно, куди простіше запобігти неполадкам у мережі, ніж виправляти проблеми, які вже виникли. Діагностика серверів і мережевих пристроїв допоможе завчасно дізнатися про потенційні неполадки і запобігати їх виникненню. Відстежуючи функціонування мережі та зберігаючи передісторію її роботи, адміністратор до того ж може надати точну інформацію користувачам, у яких іноді складається неправильне уявлення про частоту появи різних несправностей. Не менш важливо, що мережева діагностика дозволяє отримувати точні відомості про події в мережі, а також час і джерела звернень у мережу. Отже, існує два типи діагностики. Першу з них будемо називати оперативною діагностикою, а другу – діагностикою безпеки. Великі підприємства іноді розділяють ці два типи діагностики на два окремі процеси, які виконують працівники виробничих підрозділів та IT-безпеки, але малі та середні компанії з певних причин частіше організовують загальний процес діагностики. Незалежно від розміру бюджету та кількості співробітників, мережі малих і середніх компаній зазвичай не потребують такого ж рівня поточної оперативної діагностики, як у великих корпораціях. Мережі малих підприємств завантажені не настільки інтенсивно, як корпоративні, й обслуговувати їх не так складно. Крім того, технічні проекти малих компаній простіші, вони не потребують детального аналізу тенденцій і звітів, необхідних в установах з повільнішими процедурами прийняття рішень [17].

Аналіз останніх джерел та публікацій

Кіберфізична система (англ. *Cyber-physical system*) – інформаційно-технологічна концепція, що припускає інтеграцію обчислювальних ресурсів у фізичні процеси. У такій системі сенсори, обладнання та IT-системи з'єднані між собою комунікаційною мережею в одну систему, яка може виходити за межі одного підприємства чи бізнесу. Ці системи взаємодіють одна з одною за допомогою стандартних інтернет-протоколів для прогнозування, самоналаштування і адаптації до змін. Комунікаційні мережі відіграють важливу роль у кіберфізичних системах, оскільки саме через ці мережі відбувається контроль і моніторинг, розподілення навантаження у системі. Для проектування мережі можна використовувати різні технології проектування комп'ютерних мереж, метод проектування мережі насамперед залежить від сфери застосування, вимог і розмірів кіберфізичної системи. А щоб зручно було керувати вузлами мережі, потрібно розробити доступну клієнт-серверну концепцію [1, 3].

Всі засоби моніторингу та діагностики мереж КФС (кіберфізичних систем) можна розділити на кілька великих класів:

– системи управління мережею (Network Management Systems) – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік у мережі;

– засоби управління системою (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне устаткування [1, 2, 4];

– вбудовані системи діагностики й управління (Embedded Systems). Ці системи виконують у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи;

– аналізатори протоколів (Protocol analyzers). Це програмні або апаратно-програмні системи, які обмежуються, на відміну від систем управління, лише функціями моніторингу й аналізу трафіку

в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах;

– зазвичай кілька десятків. Аналізатори протоколів дають змогу встановити деякі логічні умови для захоплення окремих пакетів і виконувати повне декодування захоплених пакетів, тобто показувати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів один в одного з розшифруванням змісту окремих полів кожного пакета;

– обладнання для діагностики і сертифікації кабельних систем. Умовно це устаткування можна поділити на чотири основні групи: мережеві монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри);

– експертні системи. Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі у працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Найпростішим варіантом експертної системи є контекстозалежна help-система. Складніші експертні системи є базами знань, з елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron [5, 8];

– багатофункціональні пристрої аналізу та діагностики. У зв'язку з поширеністю локальних мереж виникла необхідність розроблення недорогих портативних приладів, які суміщають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів, і навіть деяких можливостей програмного забезпечення мережевого управління. Приклади таких пристроїв – Compas компанії MicrotestInc або 675 LANMeter компанії FlukeCorp.

Постановка завдання

Розглянути переваги та недоліки сучасних засобів реалізації середовищ діагностики КФС. Програмно реалізовано модулі, які в короткі терміни дають змогу діагностувати проблему та усунути її без участі людини. Розробити чіткий механізм знаходження відхилень у роботі корпоративної мережі та сповіщення про них системного адміністратора. Створити веб-інтерфейс для зручної діагностики вузлів корпоративної мережі та з можливістю їх групування за категоріями.

Основні результати досліджень

Проектування загальної структури корпоративної мережі КФС

Розроблювана схема комп'ютерної мережі КФС складається з вузлів, які зображені на рис. 1, а саме: інтернет; фаєрвол; інтернет-сервер; роутер; свіч; хаб; Wi-Fi міст; поштовий сервер; мультиплексор; NAS; клієнтські комп'ютери; суперкомп'ютер; термінальний сервер; принтер; МФУ; Wi-Fi роутер; ноутбук; КПК; планшет; проектор; сканер; факс.

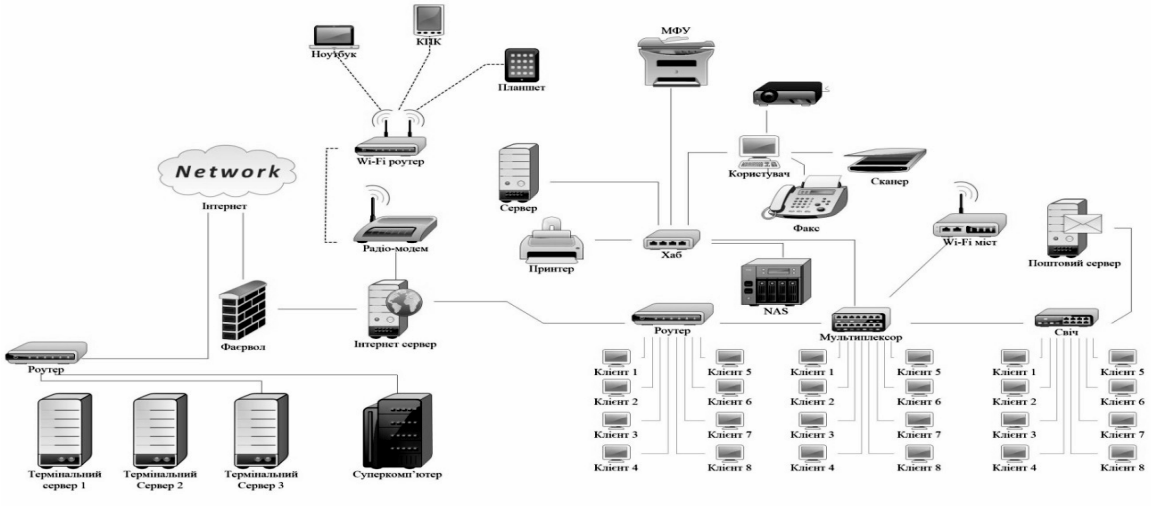

Рис. 1. Структурна схема комп'ютерної мережі КФС

Властивості мережевого концентратора у КФС дають змогу істотно підвищити загальний рівень надійності та відмовостійкості мережі. Тим більше, що вирішення всіх колізій та забезпечення загального контролю за станом приєднаних каналів покладено безпосередньо на сам пристрій без залучення додаткових потужностей, як програмних, так і апаратних. Хаби можна об'єднувати один з одним, що дозволяє будувати мережі абсолютно будь-яких топологій і розмірів, а також здійснювати магістральні з'єднання, забезпечуючи тим самим реалізацію топології "шина". Важлива причина мультиплексування сигналів – висока вартість каналів зв'язку і їх обслуговування, а наявні системи зв'язку часто не повністю використовують пропускну здатність каналу. Встановлення мультиплексора, як правило, набагато дешевше і займає менше часу, ніж організація нових каналів зв'язку. Це стосується як провідних, так і безпровідних каналів передавання інформації.

Структура середовища діагностики КФС

Спеціалізоване середовище діагностики вузлів корпоративної комп'ютерної мережі КФС працюватиме за алгоритмом, який показаний на рис. 2. Перед розгорненням спеціалізованої системи моніторингу корпоративної мережі нам потрібно підготувати середовище для цього. Середовищем КФС буде операційна система сім'ї Linux, а саме CentOS 7. Цю операційну систему вибрано через високу надійність, швидкодію та всі необхідні функції.

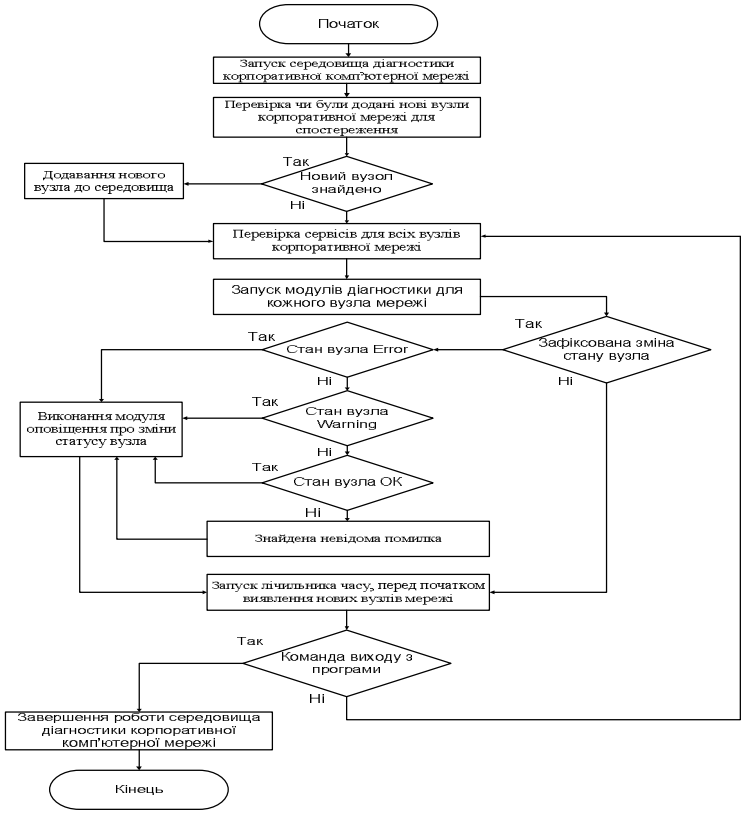

Рис. 2. Схема алгоритму роботи спеціалізованого середовища діагностики КФС

Red Hat Enterprise Linux складений переважно з вільного та відкритого програмного забезпечення, але наявний у доступній для вживання двійковій формі (наприклад, на CD або DVD дисках) лише для передплатних користувачів. Дотримуючись вимог, Red Hat випускає усі вихідні тексти своїх продуктів під GNU General Public Licensета іншими вільними ліцензіями. Розробники CentOS використовують цей вихідний код для створення кінцевого продукту, дуже подібного до Red Hat Enterprise Linux і вільного для завантаження та використання, однак без відповідної технічної підтримки з боку компанії Red Hat.

Засоби інтеграції додаткових функцій у спеціалізоване середовище діагностики КФС

Середовище діагностики Nagios є модульним, а тому всі модулі, які ми розробляємо, працюють незалежно один від одного, що збільшує гнучкість системи та безперебійність її роботи загалом. Кожен модуль незалежний, відповідає за окремі функції, що зображено на рис. 3.

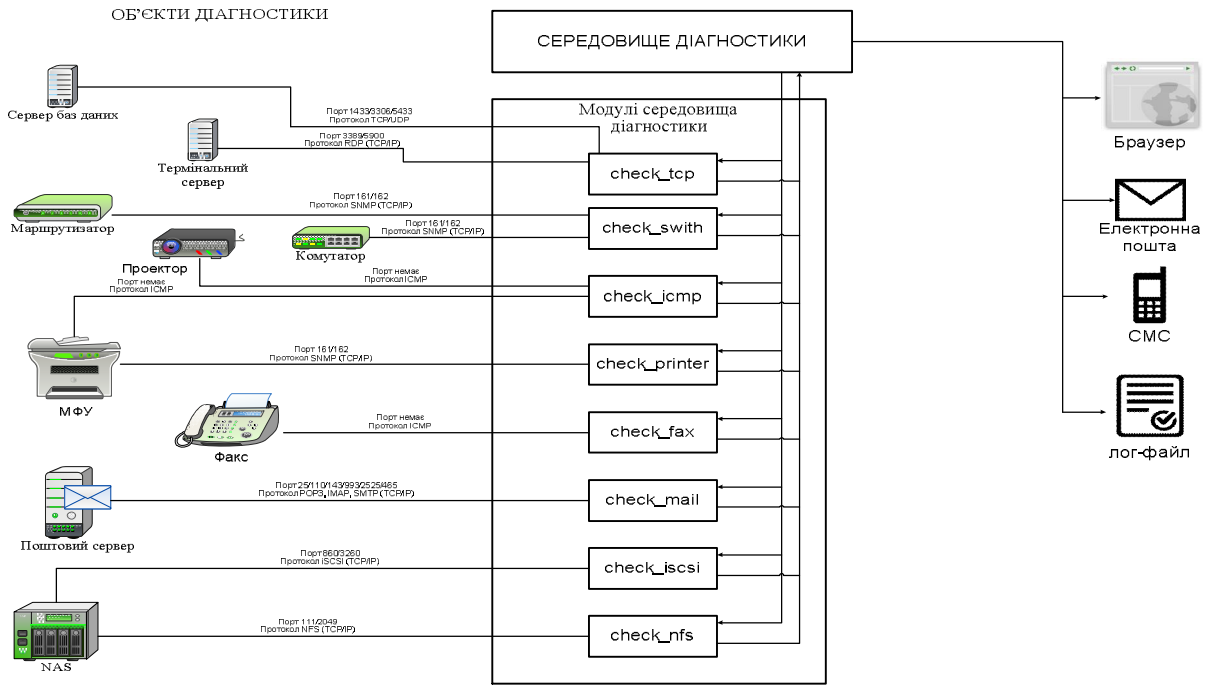

Рис. 3. Взаємодія модулів середовища діагностування КФС з мережею

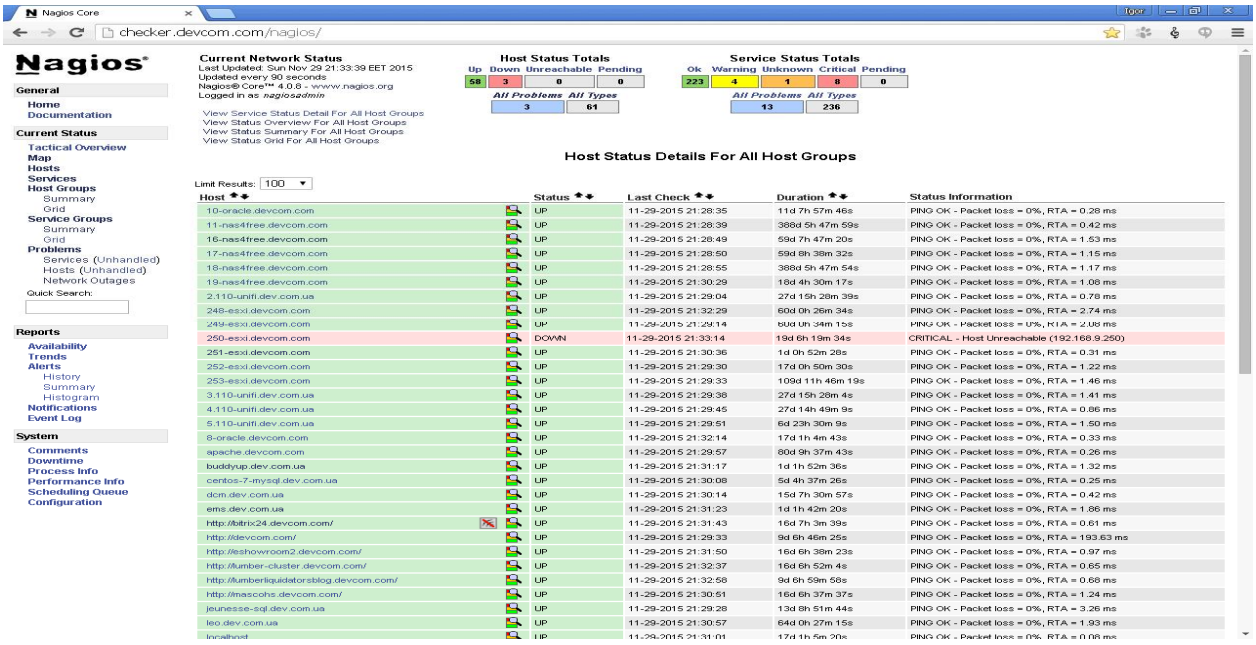

Рис. 4. Веб-інтерфейс середовища Nagios зі створеними вузлами корпоративної комп'ютерної мережі КФС

Усі розроблені модулі були поміщені за директорією /usr/local/nagios/libexec. Модулі ми викликаємо, описавши їх перед тим у конфігураційному модулі commands.cfg, де вказано спосіб виклику модуля та передавання йому необхідних параметрів. За допомогою опису модуля можемо передати йому такі параметри, як ім'я сервера, статус, адреса, дата та час, контакти, тип нотифікацій, аліас сервера, ім'я сервісу тощо.

Маючи уявлення про самі модулі середовища діагностики корпоративної комп'ютерної мережі КФС, можна розпочати їх написання під різні сервіси. Деякі модулі вже існують як готове рішення в середовищі діагностики мережі Nagios, а деякі нам довелося дописувати під певні сервіси, за якими потрібно спостерігати. Усі модулі середовища розроблено за допомогою інтерпретатора bash та perl в операційній системі сім'ї Linux.

Перевірка працездатності спеціалізованого середовища діагностики КФС

Після розгортання середовища діагностики КФС та створення конфігураційних файлів для усіх вузлів корпоративної комп'ютерної мережі та підключення до них модулів, які було розроблено, це все бачимо у веб-інтерфейсі нашої системи, який показаний на рис. 4.

Також на скріншоті бачимо, що один вузол корпоративної мережі, а саме 250-esxi.devcom.com, вимкнений більш ніж 19 днів (колонка Duration) та на іншому вузлі комп'ютерної мережі. Відключені й нотифікації про статус вузла, про що свідчить відповідне позначення.

Якщо нас цікавить детальніша інформація про вузол, можна її отримати, клацнувши на назву відповідного сервера чи вузла корпоративної мережі, який нас цікавить.

Навантажувальне тестування середовища діагностики КФС

Перевіривши роботу середовища діагностики корпоративної комп'ютерної мережі КФС, потрібно протестувати його роботу в реальних умовах. Для цього створюємо конфігураційні файли для перевірки великої кількості вузлів корпоративної мережі. Також ми цим самим перевіримо стабільність роботи середовища за великої кількості вузлів, які ми моніторимо [6, 7]. Після конфігурації вузлів, за якими спостерігатимемо за допомогою середовища, їх нараховано понад п'ятсот. Навантаження на момент роботи нашого середовища становило близько 19 %. Звідси ми можемо зробити висновок, що система без проблем може діагностувати до 500 вузлів корпоративної комп'ютерної мережі, будучи майже не навантаженою. Це дає змогу з'ясувати, яку кількість вузлів мережі може перевіряти це середовище, маючи у своєму розпорядженні необхідні для цього модулі, написані під час розроблення спеціалізованого середовища діагностики. Разом з тим, на виході маємо доволі потужне середовище діагностики корпоративної комп'ютерної мережі.

Для ще наочнішої демонстрації залежності часу діагностики одного сервісу, п'яти та десяти сервісів вузла від кількості вузлів корпоративної мережі було змодельовано таку ситуацію. Поступово до середовища ми додавали кількість діагностувальних вузлів і заміряли час, протягом якого оброблялись дані перевірки сервісів вузлів корпоративної мережі. У результаті тестування досягнуто показників, які наведено в табл. 1.

Таблиця 1

Залежність часу оброблення одного запиту від кількості діагностувальних вузлів

Кількість вузлів корпоративної мережі КФС	Час оброблення 1 сервісу, с	Час оброблення 5 сервісів, с	Час оброблення 10 сервісів, с
100	до 1	до 5	до 7
200	до 2	6–7	7–9
300	до 4	7–8	8–12
400	3-4	8–10	13–18
500	4–5	9–12	15–19

Результати вимірювань можна вважати прийнятними для будь-яких компаній, оскільки час оброблення 500 вузлів, на кожному з яких діагностуються по десять сервісів, не перевищує 20 секунд. Щоб об'єктивно оцінити, ми розгорнули аналог цього спеціалізованого середовища діагностики корпоративної мережі та виконали заміри на ньому, вибравши аналогом систему

діагностики Zabbix, доволі популярну серед корпоративного сегмента. Результати порівняння подано в табл. 2.

Таблиця 2

Порівняння з аналогом

Середовище діагностики	Кількість вузлів корпоративної мережі	Час оброблення 10 сервісів на кожному з вузлів, с	Час реакції середовища діагностики, с	Навантаження на середовище, %
Zabbix	500	до 34	до 14	57
Спеціалізоване середовище діагностики	500	до 19	до 5	19

Маючи об'єктивні дані, можна зробити висновок, що наше спеціалізоване середовище діагностики корпоративної мережі КФС продуктивніше. Оскільки навантаження на сервер є значно меншим за тієї самої кількості вузлів, які діагностуються, та меншим час відгуку системи за меншого часу оброблення всіх сервісів вузлів мережі, то це середовище можуть використовувати великі компанії для поліпшення якості діагностики своєї мережі.

Висновки

Описано принципи побудови корпоративних мереж КФС та їх розподіленість. Розроблено спеціалізоване середовище діагностики КФС та змодельовано корпоративну комп'ютерну мережу середнього підприємства. Одночасно описано процес діагностики вузлів мережі та варіанти відхилень у їх роботі. Здійснено діагностику мережі – об'єкта дослідження та змодельовано роботу системи в реальних умовах. Проведено первинну перевірку функціонування системи загалом. Розроблено модулі для перевірки багатьох сервісів вузлів корпоративної комп'ютерної мережі КФС, які повідомляють про роботу мережі загалом та використовуються для діагностики майбутніх неполадок у мережі КФС. Налаштовано функцію сповіщення про вихід з ладу одного чи певної кількості вузлів корпоративної комп'ютерної мережі, системного адміністратора за допомогою пошти. Наведено алгоритм тестування комп'ютерної мережі в спеціалізованому середовищі діагностики вузлів корпоративної мережі КФС.

1. Chris Giametta. Pro Flex on Spring, 2009. – p.445. 2. Оберг Роберт Дж. Технология COM + Основы и программирование = Understanding and Programming COM+: A Practical Guide to Windows 2000 First Edition. – М.: Вильямс, 2000. – С. 480. 3. Липаев В. В. Обеспечение качества программных средств. Методы и стандарты. – М.: Синтег, 2001. – С. 246. 4. Макгрегор Дж., Сайкс Д. Тестирование объектно-ориентированного программного обеспечения. – К.: Диасофт, 2002. – С. 432. 5. Тамре Л. Введение в тестирование программного обеспечения. – М.: Вильямс, 2003. – С. 368. 6. Татарчук М. І. Корпоративні інформаційні системи: навч. посіб. – 2005. – С. 245. 7. Мухамедзянов Н. Java. Server applications. – М.: Издательство СОЛОН-Р, 2003. – С. 267. 8. Орфалі Роберт, Ден Харкі JAVA and CORBA in client server applications.