ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

ПАРИЖСЬКИЙ Артур Владиславович

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ ДЛЯ КОНТРОЛЮ УЧБОВОЇ ДІЯЛЬНОСТІ

Спеціалізація – Комп'ютерні системи та мережі

Спеціальності – 123 - Комп`ютерна інженерія

Керівник: Мартинюк О.М.

К.т.н, доцент

Одеса – 2021

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

ПАРИЖСЬКИЙ Артур Владиславович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Дослідження технологій моніторингу для контролю учбової діяльності

керівник проекту (роботи) Мартинюк О.М.,к.т.н, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ректора ОНПУ від "_10_"___11_____2021_ року № 405-в

2. Строк подання студентом проекту (роботи) 01.12.2021

3. Вихідні дані до проекту (роботи) завдання на дослідження

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1 Аналіз технологій автоматизації в системах моніторингу

2 Дослідження систем моніторингу

3 Моделі моніторингу учбової діяльності

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Мета та задачі дослідження, Модель контролю учбових завдань, Структурна модель активності студентів, Модель контролю подій, Формування проекту та його системи контролю, Модель послідовності відповідної активності студентом, Структура контролю звітності, Модель даних контролю учбової діяльності, Модель контролю використання ресурсів, Стурктурна модель контролю ресурсів

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	1 Аналіз технологій автоматизації в системах		
	моніторингу		
2	Дослідження систем моніторингу		
3	Моделі моніторингу учбової діяльності		
	Ілюстративний матеріал		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи магістра

№	Найменування	Кільк.	Примітка
1	Пояснювальна записка	65	
2	Мета та задачі дослідження	1	
3	Модель контролю учбових завдань	1	
4	Структурна модель активності студентів	1	
5	Модель контролю подій	1	
6	Формування проекту та його системи контролю	1	
7	Модель послідовності відповідної активності студентом	1	
8	Структура контролю звітності	1	
9	Модель даних контролю учбової діяльності	1	
10	Модель контролю використання ресурсів	1	
11	Стурктурна модель контролю ресурсів	1	
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

				АМДП.ЗАМ151.0303		
Зм. Лист	№ докум.	Підпис	Дата			
Розробив	*Парижський*			*Дослідження технологій моніторингу для контролю учбової діяльності*	Літ.	Лист 1 / Листів 1
Перевірив	*МартинюкО.М*					
Реценз.					*«Одеська політехніка»*	
Н. Контр.					*ІКС КІСМ ЗАМ151*	
Затвердив						

АНОТАЦІЯ

Парижський А.В. Дослідження технологій моніторингу для контролю учбової діяльності — кваліфікаційна робота магістра. Одеса, 2021.: 65 стор., 7 рисунків, 8 джерел.

Об’єкт дослідження - процес контролю використання ресурсів лабораторій з віддаленим доступом.

Предмет дослідження - системи моніторингу комп’ютерних ресурсів та діяльності користувачів інформаційних систем.

Мета дослідження полягає в розробці та дослідженні моделей моніторингу учбової діяльності за рахунок використання систем контролю діяльності об’єктів та суб’єктів віддалених лабораторій, що дозволить скоротити час процесів оцінювання роботи студентів та керування ресурсами учбових лабораторій.

В роботі проведено аналіз сучасних систем моніторингу інформаційних систем та можливість їх використання в учбовому процесі для контролю виконання учбових активностей. Було обрано систему моніторингу та проведено розробку моделей, які розширюють її можливості та дозволяють використовувати її в рамках учбового процесу для контроля відвідування занять, визначення активності студентів в учбовому процесі та здійсненні моніторингу оцінювання завдань, які студенти виконують.

ВІДДАЛЕНИЙ ДОСТУП, МОНІТОРИНГ СИСТЕМ, МОДЕЛІ КОНТРОЛЮ СИСТЕМ, ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

ABSTRACT

Paryzhskyi A.V. Research of monitoring technologies for control of educational activity - master's qualification work. Odessa, 2021.: 65 pages., 7 pic, 8 sources.

The object of research is the process of controlling the use of remote access laboratories.

The subject of research - systems for monitoring computer resources and activities of users of information systems.

The purpose of the study is to develop and study models for monitoring educational activities through the use of control systems for facilities and entities of remote laboratories, which will reduce the time of assessment of student performance and resource management of educational laboratories.

The paper analyzes the modern systems of monitoring information systems and the possibility of their use in the educational process to monitor the implementation of educational activities. A monitoring system was selected and models were developed that expand its capabilities and allow it to be used in the educational process to control attendance, determine student activity in the learning process and monitor the evaluation of tasks performed by students.

REMOTE ACCESS, SYSTEM MONITORING, SYSTEM CONTROL MODELS, USE OF INFORMATION RESOURCES

ЗМІСТ

Вступ	5
1 Аналіз технологій автоматизації в системах моніторингу	7
1.1 Основні поняття і визначення	8
1.2 Аналіз мережевих технології та стандарти	9
1.3 Архітектура, компоненти мережі та стандарти	10
1.4 Можливості автоматизації та диспетчеризації	12
1.5 Мультиагентні системи	17
1.6 Управління розподіленими динамічними системами	19
1.7 Висновки до розділу	20
2 Дослідження систем моніторингу	21
2.1 Визначення засобів систем моніторингу	22
2.2 Визначення засобів управління мережею	23
2.3 Дослідження протоколів та стандартів управління мережою	24
2.4 Дослідження агентів	30
2.4.1 Реалізація агентів SNMP для управління мережами зв'язку	30
2.4.2 Агенти типу RMON	32
2.4.3 Аналізатори протоколів	33
2.5 Аналіз сучасних систем моніторингу	37
2.6 Висновки до розділу	40
3 Моделі моніторингу учбової діяльності	44
3.1 Контроль присутності	45
3.2 Контроль подій	48
3.3 Контроль виконання задач	51
3.4 Контроль звітності	54

3.5 Контроль використання ресурсів 57
3.6 Висновки до розділу 60
Висновки 62
Перелік джерел посилань 64

ВСТУП

Актуальність. Використання інформаційних систем суттєво розширило можливості учбових закладів. Комп'ютерні мережі і системи дозволили використовувати більш широкий спектр активностей для студентів будь-якої спеціальності, зокрема:

- вивчати комп'ютерні технології, не маючи спеціалізованого обладнання;
- проводити експерименти з природничих наук на основі програмних симуляцій;
- проводити вивчення небезпечних процесів у безпечному середовищі;
- проводити автоматичне тестування засвоєння знань студентів;
- проводити контроль завдань на основі есе, рефератів та інших самостійних робіт студентів;
- інші учбові активності, передбачені програмою навчання.

Для реалізації подібних активностей створено велику кількість інструментальних засобів, які дозволяють розгортати віддалені або хмарні платформи навчання, такі як Moodle, Canvas та інші. Основною перевагою таких платформ є можливість організації віддаленого навчання для студентів, яке дозволяє проводити ряд стандартних учбових активностей, таких як проведення лекцій, практичних занять, тестування, надання учбового контенту та певна кількість інших можливостей.

Однак, на сьогоднішній день, на рівні с LMS, інтенсивно розвиваються лабораторії з віддаленим доступом, які розширюють можливості практичного навчання студентів та слухачів.

Проте, організація таких систем вимагає ретельної підготовки як програмної складової лабораторії, так і апаратних ресурсів, що призводить до

необхідності здійснення контролю як самих ресурсів інформаційної навчальной системи, так і діяльності студентів в неї. Для цього необхідно використовувати системи моніторингу, які дозволяють здійснювати спостереження за такими ресурсами комп'ютерних системи, як сервіси, утилізація апаратних можливостей, якість комунікаційної системи та інше. Такі системи широко використовуються в будь-яких системах різного масштабу, проте, вони не адаптовані для реалізації моніторингу учбової діяльності, що призводить до необхідності розробки методів, моделей, засобів та підходів до розробки нових систем, або адаптації існуючих для задач контролю учбової діяльності, зокрема в системах з віддаленим доступом.

Мета дослідження полягає в розробці та дослідженні моделей моніторингу учбової діяльності за рахунок використання систем контролю діяльності об'єктів та суб'єктів віддалених лабораторій, що дозволить скоротити час процесів оцінювання роботи студентів та керування ресурсами учбових лабораторій.

Об'єкт дослідження - процес контролю використання ресурсів лабораторій з віддаленим доступом.

Предмет дослідження - системи моніторингу комп'ютерних ресурсів та діяльності користувачів інформаційних систем.

Методи дослідження полягають у використанні таких засобів, як теорія систем, теорія множин, теорія графів.

Наукова новизна дослідження полягає в розробці нових та вдосконалені існуючих моделей контролю ресурсів комп'ютерних мереж, аудиту діяльності користувачів інформаційних систем та адаптації сучасних інформаційних систем для використання в умовах віддаленого доступу.

Практичне значення дослідження полягає в розробці структурованих описів об'єктів учбового процесу та розробці складових систем моніторингу, які дозволяють визначати активність цих об'єктів із розмежуванням на основі контексту виконуваних задач.

1 АНАЛІЗ ТЕХНОЛОГІЙ АВТОМАТИЗАЦІЇ В СИСТЕМАХ МОНІТОРИНГУ

Контроль та прогнозування процесів – дуже складний процес. Моніторинг – це неперервний процес нагляду та реєстрації параметрів об’єктів в порівнянні із зазначеними показниками. Створюється багато технологій, пристроїв, що дозволяють проводити моніторинг будь яких об’єктів в реальному часі та попереджають о різноманітних випадках. Це організовано на зборі даних із вимірювальних приборів – сенсорів, та ці дані передаються до бази даних та оброблюються.

Для керування такими датчиками та сенсорами на великі дистанції використовуються системи автоматизованого моніторингу. Такі системи дозволяють усім підсистемам працювати автоматично та виконувати швидко вимірювання, виключати помилки, що могли бути пов’язані з людиним фактором. Людина проводить аналіз результатів та вибір необхідних засобів спостереження та управління.

Загальні переваги використання систем автоматизованого моніторингу:

- контроль даних в реальному часі;
- безперервний моніторинг за мережею;
- збір даних, попередній аналіз інформації та відправка її в будь-яке місце через мережу інтернет;
- автоматичне повідомлення діючих осіб;
- економія фінансів;
- виключення помилок адміністраторів.

Моніторинг або спостереження - це система постійного спостереження за явищами і процесами, що проходять в мережі[1].

1.1 Основні поняття і визначення

В якості основних понять прийняті наступні:

Система автоматизації - це сукупність елементів і пристроїв для створення конструктивного і функціонального цілого, призначеного для виконання певних функцій в галузі спостереження та захисту мереж [2].

Елемент системи автоматизації - це самостійний в конструктивному відношенні прилад (або пристрій), який використовується в системі [2].

Управління - це процес завдання, підтримки режиму роботи об'єкта на основі аналізу інформації про його стан. Всі види управління можуть бути безпосередніми (місцевими) або дистанційними. У системах дистанційного автоматизованого управління (ДАУ) повинна бути забезпечена можливість задати дистанційно одним органом керування необхідні режими роботи при автоматичному виконанні проміжних операцій за заданою програмою і виключена можливість одночасного управління з різних постів.

Автоматизований механізм - системний об'єкт або інший механізм, оснащений системами і пристроями автоматичного регулювання, управління, контролю і захисту [3].

Дистанційне автоматизоване управління - це засіб управління, за допомогою якого можна регулювати бажаний режим роботи механізму, впливаючи на елемент управління (наприклад, який регулює важіль або рукоятку). Потім система управління самостійно виконує всі проміжні дії.

Система аварійно-попереджувальної сигналізації (АПС) - система, що забезпечує сигналізацію про досягнення контрольованих параметрів заданих меж і зміні нормальних режимів роботи механізмів і пристроїв.

1.2 Аналіз мережевих технології та стандарти

Ethernet - стандарт локальних мереж. Під Ethernet розуміється будь-який Ethernet, Fast Ethernet, Gigabit Ethernet. Будь який Ethernet використовує метод поділу середовища передачі даних - метод CSMA/CD - метод колективного доступу з розпізнаванням несучої та виявлення колізій.

Fast Ethernet - загальний термін для позначення стандартів, що використовують як середовище передачі даних виту пару. Довжина сегмента до 100 метрів на швидкості 100 Мбіт/с [8].

Gigabit Ethernet – швидкість складає до 1 Гбіт/с, Використовується метод кодування PAM5, частота основної гармоніки 62,5 МГц. Відстань до 100 метрів.

Бездротові локальні мережі WLAN. Основні призначення бездротових локальних мереж (WLAN) - організація доступу до інформаційних ресурсів усередині будівлі [8]. Друга за значущістю сфера застосування - це організація громадських комерційних точок доступу в людних місцях - готелях, аеропортах, кафе, а також організація тимчасових мереж на період проведення заходів (виставок, семінарів).

Бездротові локальні мережі створюються на основі сімейства стандартів IEEE 802.11. Ці мережі відомі також як Wi-Fi, і хоча сам термін Wi-Fi, в стандартах явним чином не прописаний, бренд Wi-Fi одержав у світі саме широке поширення.

Основні стандарти 802.11. В даний час широко використовується переважно три стандарти групи IEEE 802.11 [8].

Стандарт IEEE 802.11g, розвитком стандарту 802.11b і передбачає передачу даних в тому ж частотному діапазоні, але з більш високими швидкостями.

Стандарт IEEE 802.11n за швидкістю передачі порівнянна з провідними стандартами. Максимальна швидкість передачі стандарту 802.11n приблизно в 5 разів перевищує продуктивність класичного Wi-Fi.

Можна відзначити наступні основні переваги стандарту 802.11n[8]:

– велика швидкість передачі даних (близько 300 Мбіт/с);

– рівномірний, стійке, надійне і якісне покриття зони дії станції, відсутність непокритих ділянок;

– сумісність з попередніми версіями стандарту Wi-Fi.

Недоліки:

– велика потужність споживання;

– два робочих діапазону (можлива заміна обладнання);

– ускладнена і більше габаритна апаратура.

Мережі стандарту 802.11 можуть будуватися за будь-який з наступних топологій:

– незалежні базові зони обслуговування (Independent Basic Service Sets, IBSSs);

– базові зони обслуговування (Basic Service Sets, BSSs);

– розширені зони обслуговування (Extended Service Sets, ESSs).

– незалежні базові зони обслуговування (IBSS)

– IBSS являє собою групу працюючих відповідно до стандарту 802.11 станцій, що зв'язуються безпосередньо одна з іншою.

Ядром бездротової мережі Wi-Fi являє собою точка доступу, яку підключають до наземної мережевої інфраструктури і забезпечує передачу радіосигналу [8].

Максимальна швидкість передачі даних на фізичному рівні в бездротовій Мережі стандарту 802.11n складає 600 М/біт в секунду, на практиці це означає швидкість в 150-200 М/біт в секунду. У попередній версії стандарту (802.11g) максимальна технічна швидкість дорівнювала 54 М/біт в секунду.

1.3 Архітектура, компоненти мережі та стандарти

Мережі, поділяються по територіальній поширеності:

– персональна мережа (PAN) для взаємодії різних приватних пристроїв, що належать одному власникові.

– локальна мережа (LAN) від маленької офісної мережі до мережі рівня великого підприємства.

– Мережі, що об’єднує кілька локальних мереж (CAN)

– Мережі городу (MAN) між установами в межах одного або кількох міст та зв'язують багато локальних мереж.

– Глобальні мережі – (WAN) покривають великі географічні регіони, що включають в себе як локальні мережі, так і інші телекомунікаційні мережі і пристрої.

В кожному типі мережі різне функціональне значення, наприклад, змішана мережа, багато-рангова мережа, клієнт-серверна мережа.

Поділяються мережі на топології з'єднання вузлів мережі, згідно використовуваним технологіям. Є різниця між фізичною топологією та логічною. Фізична – це визначені правила з’єднання вузлів, а логічна – визначає напрямки потоків даних між вузлами мережі. Тому дуже важливо при проектуванні це враховувати та розробляти ці структури.

При проектуванні мережі потрібно враховувати середовище передачі даних та особливості. Можливе підключення як провідне, за допомогою кабелів, так і бездротове з передачею інформації по радіохвилях в певному частотному діапазоні. Список мережевих технологій які будуть використовуватися на об'єкті. Враховуючи специфіку об'єкта, будуть використані більшість найпоширеніших технологій, що використовуються для побудови комп'ютерної мережі такого масштабу.

Конкретніше можна відзначити те, що для реалізації локальної мережі буде використовуватися технологія Ethernet.

Системи моніторингу будуються на двох основних принципах - автоматизації та диспетчеризації. Автоматизація знижує роль людського фактора під час керування інженерними системами і підвищує їх швидкодію. Диспетчеризація дає можливість прямого управління обладнанням з

диспетчерського пункту на основі візуальної інформації, що надійшла оператору.

Ці два принципи забезпечуються такими компонентами системи, як[2]:

– вимірювальні прилади, засоби автоматизації та виконавчі механізми;
– багатофункціональна кабельна система;
– провідні і бездротові мережі передачі даних;
– автоматизоване диспетчерське управління;
– сертифіковане програмне забезпечення;
– адміністративні ресурси.

1.4 Можливості автоматизації та диспетчеризації

Сучасні технічні засоби дозволяють робити роботу систем моніторингу не тільки ефективною, але і комфортною, а також підвищувати надійність мереж без збільшення штату співробітників. Значиму роль в системах автоматизації і диспетчеризації грає програмне забезпечення, яке дає можливість[3]:

– формувати аналітичні звіти;
– здійснювати резервне копіювання інформації;
– оперативно передавати дані по смс, e-mail;
– централізовано керувати всіма інженерними системами на одному або декількох об'єктах;
– здійснювати управління інженерними системами віддалено, з будь-якої точки світу.

Доцільність впровадження систем моніторингу обумовлена не тільки питаннями забезпечення безпеки об'єкта, також слід мати на увазі вимоги конкурентного ринку і необхідність планування ресурсів.

1.5 Засоби прогнозування та прийняття рішень

Використання багатоагентних систем дає ряд переваг над централізованими методами.

Агенти проводять без прямого втручання людини або іншої керуючої суті та можуть оптимізувати значення деякої оціночної функції [8].

Ще однією важливою властивістю агента є те, що він присутній у зовнішньому середовищі, з якого він здатний взаємодіяти. Зазвичай, середовище не контролюється агентом, він лише здатний впливати на неї. Поділ намірів і бажань необхідно, так як агент може мати несумісні бажання або бажання можуть бути недосяжні. Оскільки агент обмежений в ресурсах і не може досягти всіх бажань одночасно, природно вибирати найбільш значущі цілі - наміри. Отже, агент - розумна сутність, вміщена в зовнішнє середовище, здатна взаємодіяти з нею, роблячи автономні раціональні дії для досягнення цілей. Інтелектуальний агент - це агент, що володіє наступними властивостями[8]:

– реактивність - агент відчуває зовнішнє середовище і реагує на зміни в ній, здійснюючи дії, спрямовані на досягнення цілей;

– проактивність - агент показує керовану цілями поведінку, проявляючи ініціативу, здійснюючи дії спрямовані на досягнення цілей;

– соціальність - агент взаємодіє з іншими сутностями зовнішнього середовища (іншими агентами, людьми і т. д.) для досягнення цілей.

При розробці системи кожне з перших двох властивостей досягається досить легко. Найбільшу складність представляє поєднання в системі обох властивостей в потрібних пропорціях. Буде не дуже ефективно, якщо агент жорстко слідкує за сценарієм досягнення мети, не реагуючи на зміни у зовнішньому середовищі і не володіючи здатністю помітити необхідності коригування плану. Але також неефективною буде і поведінка, обмежена лише реакцією.

Соціальність - це не просто обмін даними. Крім комунікації, соціальна поведінка має включати кооперацію з іншими сутностями, яка полягає в поділі цілей між окремими сутностями, спільному плануванні та координації дій, спрямованих на досягнення загальних цілей. Соціальна поведінка, як мінімум, передбачає наявність у агента уявлень про цілі інших сутностей і тому, як вони планують цих цілей досягти.

Адаптивність - здатність автоматично пристосовуватися до невизначених і мінливих умов в динамічному середовищі.

Таким чином, попередниками програмних агентів можна вважати складні адаптивні системи, які вміють підлаштовуватися під ситуацію або обставини і принциповим чином змінювати свою поведінку або характеристики, щоб забезпечити вирішення поставлених перед ними завдань. Однак у випадках, коли агент функціонує в складному, постійно мінливому середовищі, взаємодіючи при цьому з іншими агентами, то така мультіагентна система значно складніше простої адаптивної системи, так як вона швидше навчається і може діяти ефективніше за рахунок перерозподілу функцій або завдань між агентами.

Складні системи часто розглядають як середовище дії агентів. З поняттям складних систем пов'язані такі фундаментальні ідеї, які безпосередньо впливають на функціонування мультіагентних систем[8]:

– в складних системах існують автономні об'єкти, які взаємодіють один з одним при виконанні своїх визначених завдань;

– агенти повинні мати можливість реагувати на мінливі умови середовища, в якій вони функціонують і, можливо, змінювати свою поведінку на основі отриманої інформації;

– складні системи характеризуються виникають структурами - логічно пов'язаними схемами, які формується в результаті взаємодії між агентами;

– складні системи з виникаючими структурами часто існують на межі порядку і хаосу;

– при створенні складних систем на базі агентів має сенс розглядати біологічні аналогії, такі як: паразитизм, симбіоз, репродукцію, генетику, мітоз і природний відбір.

Концепція агентів, розроблена в рамках мультиагентних технологій і мультиагентних систем, передбачає наявність активної поведінки агентів, тобто здатності комп'ютерної програми самостійно реагувати на зовнішні події і вибирати відповідні дії. Сьогодні агентні технології пропонують різні типи агентів, моделі їх поведінки і властивості, сімейство архітектури і бібліотеки компонентів, орієнтовані на сучасні вимоги.

Проста комп'ютерна програма відрізняється від агента тим, що не обтяжує себе цільовою поведінкою і аналізом досягнутих результатів. Навпаки, агент, що представляє інтереси користувача, "зацікавлений" у тому, щоб завдання було виконано. У разі невдачі або якогось збою він повинен повторити спробу пізніше або мати про запас альтернативний варіант вирішення проблеми. Агенти в процесі відпрацювання завдань завжди формують список виконаних дій, результати тестування і верифікації і відсилають його в керуючу систему.

Області знання і технології, за допомогою яких формуються механізми штучного інтелекту і застосування мультиагентних систем[8]:

– алгоритми кластерізації;

– нейроні мережі;

– системи, що засновуються на знаннях;

– нечітка логіка;

– теорема Баєса;

– генетичні алгоритми;

– дерева рішень.

Таким чином, агент - це самостійна програмна система, що [8]:

– має можливість приймати вплив із зовнішнього світу;

– визначати свою реакцію на цей вплив і формувати відповідну дію;

– змінювати свою поведінку з плином часу в залежності від накопиченої інформації і витягнутих з неї знань,

– володіти мотивацією і здатна після делегування повноважень користувачем поставити себе на його місце і прийняти рішення, відповідне ситуації.

Інтелектуальний агент повинен мати наступні властивості:

– автономність - здатність функціонувати без втручання з боку свого власника і здійснювати контроль внутрішнього стану і своїх дій;

– адаптивність - агент має здатність навчатися;

– колаборативність - агент може взаємодіяти з іншими агентами декількома способами, граючи різні ролі;

– здатність до міркувань - агенти можуть володіти частковими знаннями або механізмами виведення, а також спеціалізуватися на конкретну предметну область;

– комунікативність - агенти можуть спілкуватися з іншими агентами;

– мобільність - здатність передачі коду агента з одного сервера на інший;

– соціальна поведінка - можливість взаємодії і комунікації з іншими агентами;

– реактивність - адекватне сприйняття середовища і відповідні реакції на її зміни;

– активність - здатність генерувати цілі і діяти раціонально для їх досягнення;

– наявність базових знань - знання агента про себе, навколишньому середовищу, включаючи інших агентів, які не змінюються в рамках життєвого циклу агента;

– наявність переконань - змінна частина базових знань, які можуть змінюватися в часі;

– наявність мети - сукупність станів, на досягнення яких спрямована поточна поведінка агента;

– наявність бажань - стану і/або ситуації, досягнення яких для агента важливо;

– наявність зобов'язань - завдання, які бере на себе агент на прохання і/або дорученням інших агентів;

– наявність намірів - те, що агент повинен робити в силу своїх зобов'язань та/або бажань.

1.5 Мультиагентні системи

Система, в якій декілька агентів можуть спілкуватися, передавати один одному деяку інформацію, взаємодіяти між собою і вирішувати поставлену задачу називається мультиагентной (МАС). У МАС завдання або підзадачі розподілені між агентами, кожен з яких розглядається як член групи або організації[8].

МАС зазвичай складається з наступних основних компонентів:

– безліч організаційних одиниць, в яких виділяються: підмножина агентів, які маніпулюють підмножиною об'єктів;

– безліч завдань;

– простір, в якому існують агенти і об'єкти;

– безліч відносин між агентами;

– безліч дій агентів.

Основною формою організації взаємодії між агентами, що характеризуються об'єднанням зусиль для досягнення спільної мети при одночасному поділі між ними функцій, ролей і обов'язків, є кооперація. У загальному випадку це поняття можна визначити формулою: кооперація = співпраця + координація дій + вирішення конфліктів.

Під координацією зазвичай розуміється управління залежностями між діями. Комунікація між штучними агентами залежить від обраного протоколу, який представляє собою безліч правил, що визначають, як синтезувати значущі і правильні повідомлення. Фундаментальними особливостями групи, складеної з агентів, які співпрацюють для досягнення спільної мети, є соціальна структура і розподіл ролей між агентами[8].

Основою архітектури агента є контекст, або серверна середовище, в якому він виконується. Кожен агент має постійний ідентифікатор - ім'я. У серверному середовищі може виконуватися не тільки вихідний агент, а й його копія. Агенти здатні самостійно створювати свої копії, розсилаючи їх по різним серверам для виконання роботи. Після прибуття агента на наступний сервер його код і дані переносяться в новий контекст і стираються на попередньому місцезнаходженні. У новому контексті агент може робити все, що там не заборонено. Після закінчення роботи в контексті агент може переслати себе в інший контекст або по вихідному адресу відправника. Агенти здатні також вимикатися самі або за командою сервера, який переносить їх після цього з контексту в місце, призначене для зберігання.

В архітектурі МАС основну частину складає предметно-незалежне ядро, в складі якого виділяються наступні базові компоненти[8]:

– служба прямого доступу забезпечує безпосередній доступ до атрибутів агентів;

– служба повідомлень відповідає за передачу повідомлень між самим агентами, а також між агентами і додатковими системами ядра;

– бібліотека класів агентів (частина бази знань) містить інформацію про класифікацію агентів в даній МАС.

– співтовариство агентів - серверне "місце", де розміщуються агенти; цей блок, крім життєдіяльності агентів, забезпечує ще функції щодо завантаження / запису агентів і їх властивостей і за оптимізацію роботи агентів з ресурсами.

– онтологія - предметна база знань, яка містить конкретні знання про об'єкти і середовищі функціонування, що подаються у вигляді відповідної семантичної мережі.

1.6 Управління розподіленими динамічними системами

Синхронізація - збіг або зближення змінних стану двох або кількох систем, або узгоджена зміна деяких кількісних характеристик систем[7].

Завдання синхронізації відрізняється від завдання управління з еталонною моделлю, оскільки в ній допускається збіг різних змінних, взятих в різні моменти часу. Тимчасові зрушення можуть або бути постійними, або прагнути до постійних. Крім того, у багатьох задачах синхронізації зв'язку між системами є двосторонніми. Це означає, що граничний режим в системі (синхронне рішення) заздалегідь не відомий. Спільною особливістю завдань управління синхронізацією є те, що бажана поведінка однозначно не фіксована, а його характеристики задаються лише частково. У завданнях синхронізації часто основною вимогою є збіг або узгодженість коливань всіх підсистем, в той час як характеристики руху кожної підсистеми можуть варіюватися в широких межах. У контексті мультиагентного управління (МАУ) під синхронізацією розуміють узгоджену поведінку агентів, наприклад, повне або часткове зближення з часом станів агентів або їх можна побачити виходів[7].

У МАУ така мета управління частіше формулюється як завдання досягнення консенсусу або узгодження характеристик, в яких кожен агент прагне зменшити відхилення своєї цільової змінної від відповідних змінних

своїх сусідів. Якщо мова йде про відхилення від середнього арифметичного станів сусідів, то ставиться завдання досягнення усередненого консенсусу.

Ще один клас задач МАУ є розподілене управління формаціями - керування локально взаємодіючими агентами, що утворюють деякі геометричні конфігурації.

Окремий клас задач МАУ - розподіл ресурсів між різними можливими завданнями, завдання диспетчеризації, які зводяться до задачі досягнення консенсусу.

1.7 Висновки до розділу

В першому розділі проведений аналіз загальних параметрів автоматизації для визначення основних технологій. Визначені основні мережеві технології, необхідні архітектура та компоненти мереж. Другим кроком – потрібно було визначити засоби прогнозування та прийняття рішень, провести аналіз мультиагентних систем та їх типів, визначити особливості управління розподіленими динамічними системами.

2 ДОСЛІДЖЕННЯ СИСТЕМ МОНІТОРИНГУ

Постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної мережі, необхідний для підтримки її в працездатному стані. Контроль - це необхідний перший етап, який повинен виконуватися при управлінні мережею. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки і влаштування мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи - моніторинг і аналіз. На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і т. п.

Далі виконується етап аналізу, під яким розуміється більш складний і інтелектуальний 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 аналізу вимагає більш активної участі людини і використання таких складних засобів, як експертні системи, що акумулюють практичний досвід багатьох мережевих фахівців.

2.1 Визначення засобів систем моніторингу

Всі засоби моніторингу та аналізу мереж, 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 в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею - включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п.

– 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

– Вбудовані системи діагностики і управління (Embedded Systems). Ці системи виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління.

– Аналізатори протоколів (Protocolanalyzers). Представляють собою програмні або апаратно-програмні системи, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах - зазвичай кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують 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. Мережеві монітори призначені для тестування кабелів різних категорій. Слід розрізняти мережеві монітори і аналізатори протоколів. Мережеві монітори збирають дані лише про статистичні показники трафіку - середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки і т.п.

– 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.

2.2 Визначення засобів управління мережею

Системи управління виконують не тільки функції моніторингу та аналізу роботи мережі, необхідні для отримання вихідних даних для налаштування мережі, але і включають функції активного впливу на мережу - управління конфігурацією і безпекою, які потрібні для відпрацювання виробленого плану настройки та оптимізації мережі.

Загальна класифікація засобів управляння мережею:

– Управління конфігурацією мережі - полягає в конфігурації компонентів мережі, включаючи їх місце розташування, мережні адреси і ідентифікатори, управління параметрами мережевих операційних систем, підтримку схеми мережі: також ці функції використовуються для іменування об'єктів.

– Обробка помилок - це виявлення і усунення наслідків збоїв у роботі мережі.

– Аналіз продуктивності - допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи і величину трафіка, а також планувати розвиток мережі.

– Управління безпекою - включає в себе контроль доступу та збереження цілісності даних. У функції входить процедура аутентифікації, перевірки привілеїв, підтримка ключів шифрування, управління правами. До цієї ж групи можна віднести важливі механізми управління паролями, зовнішнім доступом, з'єднання з іншими мережами.

– Облік роботи мережі - включає реєстрацію і управління використовуваними ресурсами і пристроями. Ця функція оперує такими поняттями як час використання і плата за ресурси.

2.3 Дослідження протоколів та стандартів управління мережою

Найбільш поширеним протоколом управління мережами є протокол SNMP (SimpleNetworkManagementProtocol. Головні переваги протоколу SNMP - простота, доступність, незалежність від виробників. Протокол SNMP розроблений для управління маршрутизаторами в мережі Internet і є частиною стека TCP/IP.

SNMP - це протокол, що використовується для отримання від мережевих пристроїв інформації про їх статус, продуктивність та характеристики, які зберігаються в спеціальній базі даних мережевих пристроїв, що називається MIB (ManagementInformationBase). Існують стандарти, що визначають структуру MIB, в тому числі набір типів її змінних (об'єктів в термінології ISO), їх імена і допустимі операції цими змінними (наприклад, читати). У MIB, поряд з іншою інформацією, можуть зберігатися мережеві та / або MAC-адреси пристроїв, значення лічильників оброблених пакетів і помилок, номери, пріоритети та інформація про стан портів. Деревоподібна структура MIB містить обов'язкові (стандартні) піддерева, а також в ній можуть знаходитися приватні (private) піддерева, що дозволяють

виробнику інтелектуальних пристроїв реалізувати будь-які специфічні функції на основі його специфічних змінних.

Агент в протоколі SNMP - це елемент, який надає менеджерам, розміщеним на керуючих станціях мережі, доступ до значень змінних MIB, і тим самим дає їм можливість реалізовувати функції з управління та спостереження за пристроєм. Типова структура системи управління зображена на наступному малюнку:

Визначення функцій агентів і менеджерів в стандартах OSI досить добре узгоджуються з визначеннями систем SNMP. Повідомлення, які агент посилає менеджеру за своєю ініціативою, називаються повідомленнями - notifications.

Менеджер не тільки збирає і порівнює дані, одержувані від агентів, на основі цих даних він може також виконувати адміністративні функції, керуючи операціями віддалених агентів.

У стандартах OSI різниця між менеджерами та агентами не дуже чітка. Суб'єкт SMAE, що виконує в одній взаємодії роль менеджера, може в іншій взаємодії виконувати роль агента, і навпаки. Стандарти OSI не визначають способів взаємодії агента з керованими об'єктами. Стандарти OSI також не говорять про те, як агент взаємодіє з керованими об'єктами, які перебувають за межами керованої системи, тобто об'єктами, з якими потрібно взаємодіяти через мережу. У таких випадках може знадобитися, наприклад, щоб один агент запросив дані про деякий об'єкт від іншого агента. Порядок такого роду взаємодії також не визначається стандартами OSI.

Щоб менеджер і агент змогли взаємодіяти, кожен повинен мати певні відомості про один одного. Ці відомості модель OSI називає контекстом додатку (Application Context, AC). AC описує елементи прикладного рівня стека OSI, які використовуються агентами і менеджерами.

Прикладний рівень стека OSI включає кілька допоміжних служб загального призначення, які використовуються прикладними протоколами і клієнтськими програмами (в тому числі і додатками управління) для

автоматизації найбільш часто виконуваних дій. Це не закінчені протоколи прикладного рівня, подібні протоколах ftp, telnet або NCP, за допомогою яких користувач мережі може виконати якусь корисну дію, а допоміжні системні функції, які допомагають розробнику прикладного протоколу або програми написати її компактно і ефективно. На прикладному рівні стека OSI існують наступні допоміжних служби:

– ACSE (Association Control Service Element). Відповідає за встановлення з'єднань між додатками різних систем. З'єднання (сесія, сеанс) на прикладному рівні OSI носить назву асоціації. Асоціації бувають індивідуальними та груповими (shared).

– RTSE (Reliable Transfer Service Element). Займається підтримкою відновлення діалогу, викликаного розривом нижчележащих комунікаційних служб, в рамках асоціації.

– ROSE (Remote Operations Service Element). Організовує виконання програмних функцій на віддалених машинах (аналог служби виклику віддалених процедур RPC).

Основна модель управління OSI включає: управління системами, управління N-рівнем і операції N-рівня. Це розбиття на три області зроблено для того, щоб врахувати всі можливі ситуації, що виникають при управлінні.

Основна модель управління системами передбачає виконання керуючих операцій і передачу повідомлень між одноранговими системами, що означає необов'язковість жорсткого розподілу ролей на керуючі та керовані системи. Ця модель полегшує реалізацію розподілених аспектів управління. З іншого боку, допускається реалізація однорангових систем як керуючих і керованих.

Керований об'єкт - це представлення OSI про ресурс з метою управління. Ресурс може бути описаний як керований об'єкт. Конкретний керований об'єкт - це екземпляр (instance) деякого класу керованих об'єктів. Модель управління OSI широко використовує об'єктно-орієнтований підхід. Клас керованих об'єктів - це набір властивостей, які можуть бути

обов'язковими або умовними. За допомогою опису одного класу керованих об'єктів, наприклад комутаторів, можна створити інший клас керованих об'єктів, наприклад комутаторів, що підтримують техніку VLAN, успадкувавши всі властивості класу комутаторів, але додавши нові атрибути.

Для управління ресурсами менеджер і агент повинні бути обізнані про деталі цих ресурсів. Деталізація представлення керованих об'єктів, які потрібні для виконання функцій управління, зберігається в репозиторії, відомому як Management Information Base (MIB). Бази MIB OSI зберігають не тільки описи класів керованих об'єктів, але й характеристики мережі та її елементів. Бази MIB містять характеристики кожної частини керованого обладнання і ресурсів. MIB також включає опис дій, які можуть виконуватися на основі зібраних даних або ж викликані зовнішніми командами. Бази MIB дозволяють зовнішнім системам опитувати, змінювати, створювати і видаляти керовані об'єкти (реальні ресурси мережі при цьому, природно, продовжують працювати). Протокол CMIP і локальні інтерфейси управління забезпечують доступ до цих можливостей.

MIB - це концептуальна модель, і вона не має ніякого зв'язку зі способом фізичного або логічного зберігання даних в ресурсі. Стандарти не визначають аспекти власне зберігання даних. Протоколи OSI визначають синтаксис інформації, що зберігається в MIB, і семантику обміну даними.

Доступ до керуючої інформації, що зберігається в керованих об'єктах, забезпечується за допомогою елемента системи управління, званого службою CMSIE (Common Management Information Service Element). Служба CMSIE побудована в архітектурі розподіленого додатку, де частину функцій виконує менеджер, а частина - агент. Взаємодія між менеджером і агентом здійснюється по протоколу CMIP. Послуги, що надаються службою CMSIE, називаються послугами CMIS (Common Management Information Services). Протокол CMIP та послуги CMIS визначені в стандартах X.710 і X.711 ITU-T. Послуги CMIS поділяються на дві групи - послуги, що ініціюються менеджером (запити), та послуги, що ініціюються агентом (повідомлення).

Відмінність послуг CMIS від аналогічних послуг SNMP полягає в більшій гнучкості. Якщо запити GET і SET протоколу SNMP застосовні тільки до одного атрибуту одного об'єкта, то запити M-GET, M-SET, M-ACTION і M-DELETE можуть застосовуватися до більш ніж одного об'єкту. Для цього стандарти CMIP / CMIS вводять такі поняття, як огляд (scoping), фільтрація (filtering) і синхронізація (synchronization).

Керуюча інформація від менеджера до агента, що передається по протоколу CMIP кодується відповідно до правил ASN.1 і BER . Для кожної операції визначено формат блоку даних, які переносяться по мережі від менеджера агенту, і навпаки. Формат протокольних блоків даних CMIP описується нотацією ASN.1 і має набагато складнішу структуру , ніж блоки SNMP. Наприклад , блок даних операції M- GET має поля для завдання імен атрибутів, значення яких запрошувати менеджер, а також поля завдання параметрів огляду і фільтрації. Є також поля для завдання параметрів прав доступу до об'єкта. Застосування протоколу CMIP визначає досить високий початковий рівень складності системи управління, так як для його роботи необхідно реалізувати ряд допоміжних служб, об'єктів і баз даних об'єктів . Сповіщення агента CMIP завжди передаються за допомогою надійного транспортного протоколу і в разі втрати будуть передані повторно. Протокол CMIP розрахований на агентів, які можуть з однієї простої команді від менеджера виконати складну послідовність дій. Протокол CMIP істотно краще масштабується , так як може впливати відразу на декілька об'єктів , а відповіді від агентів проходять через фільтри, які обмежують передачу керуючої інформації тільки певним агентам і менеджерам . Протокол CMIP, який є протоколом взаємодії між агентами і менеджерами системи управління OSI, дозволяє за допомогою однієї команди впливати відразу на групу агентів, застосувавши такі опції, як огляд і фільтрація. MIB для протоколу CMIP не мають єдиного стандарту і розробляються кожним виробником телекомунікаційного обладнання тільки для свого власного обладнання.

Content Management Interoperability Services (CMIS, сервіси взаємодії при управлінні контентом) - пропонований провідними виробниками пакет стандартів, що складається з набору веб -сервісів для спільного використання інформації, що зберігається в незв'язаних між собою сховищах контенту [1].

Переваги CMIS. Специфікація CMIS містить опис інтерфейсу для веб - сервісів, який :

- розроблений для роботи з існуючими сховищами, дозволяючи користувачам створювати і вдосконалювати додатки, що підтримують одночасну роботу з безліччю сховищ - роблячи доступним контент, який вони вже мають
- відокремлює веб - сервіси та контент від сховища контента, дозволяючи користувачам керувати контентом незалежно
- забезпечує базові веб - сервіси і інтерфейс Web 2.0 , що відчутно спрощує розробку додатків
- є платформою розробки, яка не залежить від мови програмування
- підтримує розробку композитних додатків і мешап (mash - up) бізнес-або IT- аналітиками
- забезпечує зростання співтовариства незалежних розробників програмного забезпечення

Порівняння протоколів SNMP та CMIP

– Застосування протоколу SNMP дозволяє будувати як прості, так і складні системи управління, а застосування протоколу CMIP визначає деякий, досить високий початковий рівень складності системи управління, так як для його роботи необхідно реалізувати ряд допоміжних служб, об'єктів і баз даних об'єктів.

– Агенти CMIP виконують, як правило, більш складні функції, ніж агенти SNMP. Через це операції, які менеджеру можна виконати над агентом SNMP, носять атомарний характер, що призводить до численних обмінів між менеджером і агентом.

– Повідомлення (traps) агента SNMP надсилаються менеджеру без очікування підтвердження, що може привести до того, що важливі мережеві проблеми залишаться непоміченими, оскільки відповідне повідомлення виявиться втраченим, у той час як повідомлення агента CMIP завжди передаються за допомогою надійного транспортного протоколу і в разі втрати будуть передані повторно.

– Вирішення частини проблем SNMP може бути досягнуто за рахунок застосування більш інтелектуальних MIB (до яких відноситься RMON MIB), але для багатьох пристроїв і ситуацій таких MIB немає (або немає стандарту, або немає відповідної MIB в керованому обладнанні).

– Протокол CMIP розрахований на інтелектуальних агентів, які можуть по одній простій команді від менеджера виконати складну послідовність дій.

– Протокол CMIP істотно краще масштабується, тому що може впливати відразу на декілька об'єктів, а відповіді від агентів проходять через фільтри, які обмежують передачу керуючої інформації тільки певним агентам і менеджерам.

2.4 Дослідження агентів

2.4.1 Реалізація агентів SNMP для управління мережами зв'язку

Існують готові комплекси управління та візуалізації контролю за технологічними процесами. Спочатку цей протокол розроблявся для управління обчислювальними мережами, проте завдяки своїй гнучкості і все більш широкому розповсюдженню він може бути з успіхом застосований як базовий протокол управління телекомунікаційними мережами.

Розроблена система призначена для збору та відображення на станції управління інформації про стан контактних датчиків в обладнанні, розміщеному на віддалених об'єктах в мережі зв'язку. В якості станції

управління використовувався встановлений в центральному офісі комп'ютер, на якому була інстальована система HP OpenView, яка виконувала функції SNMP-менеджера. Для менеджера була створена структура MIB, що описує розроблений SNMP-агент.

Структура SNMP - агента уніфікована з метою використання на різних об'єктах мережі зв'язку. Вона складається з проксі-агента з підключеними промисловими контролерами , які виконують функції збору стану контактних датчиків.

В даний час ряд компаній-операторів для прискорення розробки і зниження вартості систем використовують на своїх технологічних серверах відкриту операційну систему Linux. Враховуючи перспективу широкого застосування ОС Linux у системах зв'язку і управління, ми розробили версію проксі-агента для цієї операційної системи. У порівнянні з описаною вище системою контролю на базі ОС Windows дана система забезпечує наступні додаткові можливості:

- Проведення моніторингу каналів збору інформації та термінального обладнання;
- Збір даних з різних типів контролерів станів;
- Можливість зміни станів виходів підключених контролерів;
- Можливості зміни режиму роботи агента, налаштування системи команд для різних типів контролерів станів, зміни умов видачі і змісту trap - повідомлень за допомогою гнучкої системи файлів конфігурації.

Управління маршрутизатором проводиться SNMP - менеджером, встановленим на станції управління. В якості SNMP - агента використовувався комунікаційний модуль. До нього за допомогою інтерфейсу RS- 232 підключається персональний комп'ютер, який використовується в якості консолі для конфігурації термінального обладнання - маршрутизатора. У системі реалізована архітектура мережі управління SNMPv1 і частково SNMPv2. SNMP - менеджер періодично опитує SNMP - агентів про стан контрольованого устаткування і представляє

отримані дані в зручному для оператора вигляді. SNMP - агенти забезпечують прийом інформації з маршрутизатора, відповіді на запити SNMP-менеджера і оповіщення про надзвичайні ситуації. На комунікаційному модулі, виконує функції SNMP - агента, встановлені операційне ядро реального часу RTEMS 4.0.0 (Real Time Executive for Multiprocessor Systems) і модуль BSP (Board Support Package), що забезпечує зв'язок з апаратурою. У завдання останнього входять ініціалізація модуля і запуск системи, реалізація системних годин для планувальника завдань, підключення драйверів.

Програмне забезпечення SNMP - агента являє собою набір завдань і служб, кожна з яких виконується незалежно від інших завдань.

Розроблене програмне забезпечення для реалізації функцій SNMP - агента є базою для створення різних систем управління розподіленими мережами, побудованими на базі процесорів і контролерів Motorola.

2.4.2 Агенти типу RMON

Нововведенням до функціональних можливостей SNMP є специфікація RMON, яка забезпечує віддалену взаємодію з базою MIB. До появи RMON протокол SNMP не міг використовуватися віддалено, він допускав лише локальне управління пристроями. База RMONMIB має поліпшений набір властивостей для віддаленого управління, оскільки містить агреговану інформацію про пристрій, що не вимагає передачі по мережі великих обсягів інформації. Об'єкти RMONMIB включають додаткові лічильники помилок в пакетах, гнучкіші засоби аналізу графічних трендів і статистики, більш потужні засоби фільтрації для захоплення і аналізу окремих пакетів, а також більш складні умови встановлення сигналів попередження. Агенти RMONMIB більш інтелектуальні порівняно з агентами MIB-I або MIB-II і виконують значну частину роботи по обробці інформації про пристрій, яку раніше виконували менеджери. Ці агенти можуть розташовуватися усередині різних комунікаційних пристроїв, а також бути виконані у вигляді окремих програмних модулів, що працюють на універсальних ПК і ноутбуках.

Відмінною рисою стандарту RMONMIB є його незалежність від протоколу мережевого рівня. Тому, його зручно використовувати в гетерогенних середовищах, що використовують різні протоколи мережевого рівня.

Як видно з опису об'єктів, за допомогою агента RMON, вбудованого в повторювач або інше комунікаційне обладнання, можна провести дуже детальний аналіз роботи сегмента Ethernet або Fast Ethernet. Спочатку можна отримати дані про типи помилок в кадрах, що зустрічаються в сегменті, а потім доцільно зібрати за допомогою группи History залежності інтенсивності цих помилок від часу (в тому числі і прив'язавши їх до часу). Після аналізу тимчасових залежностей часто вже можна зробити деякі попередні висновки про джерело помилкових кадрів і на цій підставі сформулювати більш тонкі умови захоплення кадрів зі специфічними ознаками. Після цього можна провести ще більш детальний аналіз за рахунок вивчення захоплених кадрів, витягуючи їх з об'єктів группи Packet Capture.

2.4.3 Аналізатори протоколів

У ході проектування нової або модернізації старої мережі часто виникає необхідність в кількісному вимірі деяких характеристик мережі таких, наприклад, як інтенсивності потоків даних по лініях зв'язку, затримки, що виникають на різних етапах обробки пакетів, часи реакції на запити того чи іншого виду, частота виникнення певних подій та інших характеристик.

Для цих цілей можуть бути використані різні засоби і насамперед - засоби моніторингу в системах управління мережею, які вже обговорювалися в попередніх розділах. Деякі вимірювання мережі можуть бути виконані і вбудованими в операційну систему програмами.

Але найбільш досконалим засобом дослідження мережі є аналізатор протоколів. Аналізатор мережевих протоколів може використовуватися для:

- локалізації складних проблем;
- виявлення та ідентифікації несанкціонованого програмного забезпечення;

- отримання такої інформації, як базові моделі трафіку і метрики утилізації мережі;
- ідентифікації невикористовуваних протоколів для видалення їх з мережі;
- генерації трафіку для випробування на вторгнення з метою перевірки системи захисту;
- роботи з системами виявлення вторгнень Intrusion Detection System (IDS);
- прослуховування трафіку, тобто локалізації несанкціонованого трафіку з використанням Instant Messaging (IM) або бездротових точок доступу Access Points - (AP);
- вивчення роботи мережі.

Аналізатор протоколів є самостійним спеціалізованим пристроєм, або персональним комп'ютером, зазвичай переносним, класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Мережева карта і програмне забезпечення, що використовуються повинні відповідати топології мережі. Аналізатор підключається до мережі точно так, як і звичайний вузол. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, що передаються по мережі, в той час як звичайна станція - лише адресовані їй. Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера і декодує одержувані дані, та додаткового програмного коду, що залежить від типу топології досліджуваної мережі. Крім того, поставляється ряд процедур декодування, орієнтованих на певний протокол. До складу деяких аналізаторів може входити також експертна система, яка може видавати користувачеві рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті чи інші результати вимірювань, як усунути деякі види несправності мережі.

Особливості аналізаторів:

– Буфер захоплення. Буфери різних аналізаторів відрізняються за обсягом. Буфер може розташовуватися на мережевій карті, або для нього може бути відведено місце в оперативній пам'яті одного з комп'ютерів мережі. Якщо буфер розташований на мережевій карті, то управління ним здійснюється апаратно, і за рахунок цього швидкість введення підвищується. Однак це призводить до подорожчання аналізатора. У разі недостатньої продуктивності процедури захоплення, частина інформації буде губитися, і аналіз буде неможливий. Розмір буфера визначає можливості аналізу по більш або менш представницьким вибіркам даних, що захоплюються. Але яким би великим не був буфер захоплення, рано чи пізно він заповниться. У цьому випадку або припиняється захоплення, або заповнення починається з початку буфера.

– Можливість вимірювання середньостатистичних показників трафіку в сегменті локальної мережі, в якому встановлений мережевий адаптер аналізатора.

– Вимірюється коефіцієнт використання сегменту, матриці перехресного трафіку вузлів, кількість хороших і поганих кадрів, що пройшли через сегмент.

– Можливість роботи з декількома агентами, котрі поставляють захоплені пакети з різних сегментів локальної мережі. Ці агенти найчастіше взаємодіють з аналізатором протоколів за власним протоколом прикладного рівня.

– Фільтри. Фільтри дозволяють керувати процесом захоплення даних, і, тим самим, дозволяють економити простір буфера. Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується в буфер захоплення. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає перегляд непотрібних в даний момент пакетів.

– Перемикачі - це деякі умови початку і припинення процесу захоплення даних з мережі, що задаються користувачем. Такими умовами

можуть бути виконання ручних команд запуску і зупинки процесу захоплення, тривалість процесу захоплення, поява певних значень в кадрах даних. Перемикачі можуть використовуватися спільно з фільтрами, дозволяючи більш детально й тонко проводити аналіз, а також продуктивніше використовувати обмежений обсяг буфера захоплення.

– Пошук. Деякі аналізатори протоколів дозволяють автоматизувати перегляд інформації, що знаходиться в буфері, і знаходити в ній дані по заданим критеріям. У той час, як фільтри перевіряють вхідний потік на предмет відповідності умовам фільтрації, функції пошуку застосовуються до вже накопичених в буфері даних.

– Багатоканальність. Деякі аналізатори протоколів дозволяють проводити одночасний запис пакетів від декількох мережевих адаптерів, що зручно для зіставлення процесів, що відбуваються в різних сегментах мережі. Можливості аналізу проблем мережі на фізичному рівні у аналізаторів протоколів мінімальні, оскільки всю інформацію вони отримують від стандартних мережевих адаптерів. Тому вони передають і узагальнюють інформацію фізичного рівня, яку повідомляє їм мережевий адаптер, а вона багато в чому залежить від типу мережного адаптера. Деякі мережні адаптери повідомляють більш детальні дані про помилки кадрів та інтенсивності колізій в сегменті, а деякі взагалі не передають таку інформацію верхнім рівням протоколів, на яких працює аналізатор протоколів.

Методологія проведення аналізу може бути представлена у вигляді послідовності кроків: аналізатор працює на станції хоста. Коли аналізатор запускається в хаотичному режимі, драйвер мережевого адаптера, NIC, перехоплює весь трафік, що проходить через нього. Аналізатор протоколів передає перехоплений трафік декодеру пакетів аналізатора, який ідентифікує і розщеплює пакети по відповідним рівнями ієрархії. Програмне забезпечення протокольного аналізатора вивчає пакети і відображає інформацію про них на екрані хоста у вікні аналізатора. Залежно від

можливостей конкретного продукту, представлена інформація може згодом додатково аналізуватися і фільтруватися.

Мережеві аналізатори. Мережеві аналізатори являють собою еталонні вимірювальні інструменти для діагностики та сертифікації кабелів і кабельних систем. Мережеві аналізатори містять високоточний частотний генератор і вузькосмуговий приймач. Передаючи сигнали різних частот в передавальну пару і вимірюючи сигнал у приймальній парі, можна виміряти затухання і NEXT. Мережеві аналізатори - це великогабаритні і дорогі прилади, призначені для використання в лабораторних умовах спеціально навченим технічним персоналом.

2.5 Аналіз сучасних систем моніторингу

В підрозділі виділені основні системи моніторингу, що є найбільш використовуваними.

Cacti - це програмне забезпечення з відкритим вихідним кодом в області графічного представлення мережі, і він виводить принципи MRTG на новий рівень. Від використання диска до швидкості вентилятора в джерелі живлення, якщо показник можна відстежувати, Cacti зможе відобразити його та зробити ці дані доступними. Входить до LAMP-набору серверного програмного забезпечення, яке надає стандартизовану програмну платформу для побудови графіків на основі практично будь-яких статистичних даних. Якщо будь-який пристрій або сервіс повертає числові дані, вони, швидше за все, можуть бути інтегровані в Cacti.

Незважаючи на те, що стандартним методом збору даних Cacti є протокол SNMP, також для цього можуть бути використані сценарії Perl або PHP. Фреймворк програмної системи вміло поділяє на дискретні екземпляри збір даних та їхнє графічне відображення, що дозволяє з легкістю повторно обробляти та реорганізовувати існуючі дані для різних візуальних уявлень.

Cacti - це інструментарій з широкими можливостями для графічного відображення та аналізу тенденцій продуктивності мережі, який можна використовувати для моніторингу практично будь-якої контрольованої метрики, що представляється у вигляді графіка. Це рішення також підтримує практично безмежні можливості для налаштування, що може зробити його надто складним при певних застосуваннях.

Nagios — це програмна система для моніторингу мережі, дозволяє робити майже все, що може знадобитися системним та мережевим адміністраторам від пакета прикладних програм для моніторингу.

Nagios може стати проблемою для новачків, але досить складна конфігурація також є перевагою цього інструменту, оскільки він може бути адаптований практично до будь-якого завдання моніторингу.

У Nagios програмна платформа пропонує настроюваний механізм повідомлень електронною поштою, через СМС та миттєві повідомлення більшості популярних Інтернет-месенджерів, а також схему ескалації, яка може бути використана для прийняття розумних рішень про те, хто, як і при яких обставин повинен бути повідомлений, що при правильному налаштуванні допоможе вам забезпечити багато годин спокійного сну. А веб-інтерфейс може бути використаний для тимчасового призупинення отримання повідомлень або підтвердження цієї проблеми, а також внесення нотаток адміністраторами. Крім того, функція відображення демонструє всі контрольовані пристрої в логічному представленні їх розміщення в мережі з колірним кодуванням, що дозволяє показати проблеми в міру їх виникнення.

Недоліком Nagios є конфігурація, так як її краще виконувати через командний рядок, що значно ускладнює навчання новачків. Хоча люди, знайомі зі стандартними файлами конфігурації Linux/Unix, особливих проблем не мають.

Icinga повноцінна програмна платформа для моніторингу та системи оповіщення, яка розроблена такою ж відкритою та розширюваною, як і Nagios, але з деякими відмінностями у веб-інтерфейсі. Як і Nagios, Icinga

може бути використана для моніторингу всього, що говорить мовою IP, настільки глибоко, наскільки ви можете використовувати SNMP, а також плагіни і доповнення, що налаштовуються.

NeDi — це програмне забезпечення, що відноситься до LAMP, яке регулярно переглядає MAC-адреси та таблиці ARP у комутаторах вашої мережі, каталогізуючи кожен виявлений пристрій у локальній базі даних. NeDi постійно переглядає мережну інфраструктуру та каталогізує пристрої, відстежуючи все, що виявить. Через веб-інтерфейс NeDi проходить пошук для визначення комутатора, порту комутатора, точки доступу або іншого пристрою за MAC-адресою, IP-адресою або DNS-іменем. NeDi збирає всю інформацію з кожного мережевого пристрою, з яким стикається, витягуючи з них серійні номери, версії прошивки та програмного забезпечення, поточні часові параметри, конфігурації модулів, відзначення MAC- адреси пристроїв, які були втрачені або вкрадені. Якщо вони знову з'являться в мережі, NeDi повідомить про це.

Ntop — інструмент для аналізу пакетів з легким веб-інтерфейсом, який показує дані в реальному часі про мережний трафік. Інформація про поток даних через хост і про з'єднання з хостом також доступні в режимі реального часу. Ntop надає графіки та таблиці, що показують поточний та минулий мережевий трафік, включаючи протокол, джерело, призначення та історію конкретних транзакцій, а також хости з обох кінців. Одним із найкорисніших застосувань Ntop є контроль трафіку у конкретному місці.

Zabbix – це інструмент для мережного та системного моніторингу мережі, який поєднує кілька функцій в одній веб-консолі. Він може бути налаштований для моніторингу і збору даних з різних серверів і мережевих пристроїв, забезпечуючи обслуговування і моніторинг продуктивності кожного об'єкта.

Zabbix дозволяє проводити моніторинг серверів та мереж за допомогою широкого набору інструментів, включаючи моніторинг гіпервізорів віртуалізації та стеків веб-додатків.

В основному, Zabbix працює із програмними агентами, запущеними на контрольованих системах. Але це рішення також може працювати без агентів, використовуючи протокол SNMP або інші можливості для моніторингу. Zabbix підтримує VMware та інші гіпервізори віртуалізації, надаючи докладні дані про продуктивність гіпервізора та його активність. Особлива увага також приділяється моніторингу серверів програм Java, веб-сервісів і баз даних.

Observium - це програма для моніторингу мережного обладнання та серверів, яке має величезний список пристроїв, що підтримуються, що використовують протокол SNMP. Як програмне забезпечення, що відноситься до LAMP, Observium відносно легко встановлюється та налаштовується, вимагаючи звичайних установок Apache, PHP та MySQL, створення бази даних, конфігурації Apache тощо. Він встановлюється як власний сервер із виділеною URL-адресою.

Observium поєднує у собі моніторинг систем та мереж з аналізом тенденцій продуктивності. Він може бути налаштований для відстеження будь-яких показників.

2.6 Висновки до розділу

Моніторинг є одним з найважливіших завдань, необхідних організації повноцінного управління обчислювальної мережею. Процес виявлення самих несправностей та формування комплексу заходів може зайняти значний час та суттєво вплинути на функціонування системи автоматизації підприємства загалом. Часті відмови або тривалі періоди непрацездатного стану мережі можуть призвести до повної втрати працездатності системи автоматизації підприємства. Для підвищення оперативності вжиття заходів, здатних повернути обчислювальну мережу в режим штатного функціонування, необхідно проведення моніторингу мережі, який переважно залежить від людського фактора. Професійного досвіду спеціаліста, що експлуатує великі

обчислювальні мережі, часто не вистачає для оперативної діагностики мережі та прийняття рішення під час усунення збоїв у роботі.

В роботі були досліджені різноманітні засоби моніторингу.

Системи управління мережею (Network Management Systems). Централізовані програмні системи, які збирають дані про стан вузлів та комунікаційних пристроїв мережі, а також про трафік, що циркулює у мережі. Ці системи не тільки здійснюють моніторинг та аналіз мережі, але й виконують в автоматичному або напівавтоматичному режимі дії з управління мережею – включення та відключення портів пристроїв, зміна параметрів мостів адресних таблиць, комутаторів та маршрутизаторів тощо. Прикладами систем управління можуть бути популярні системи HP OpenView, SunNet Manager, IBM NetView та ін.

Засоби управління системою (System Management). Часто виконують функції, аналогічні функцій систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне та апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне обладнання. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад засоби управління системою можуть виконувати найпростіший аналіз мережного трафіку.

Вбудовані системи діагностики та управління (Embedded Systems). Ці системи виконані у вигляді програмно-апаратних модулів, що встановлюються у комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики та управління тільки одним пристроєм, і в цьому їхня основна відмінність від централізованих систем управління.

Аналізатори протоколів (Protocol Analyzers). Є програмними або апаратно-програмними системами, які обмежуються, на відміну від систем управління, лише функціями моніторингу та аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах – зазвичай кілька

десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто в зручній для спеціаліста формі вкладеність пакетів протоколів різних рівнів один в одного з розшифровкою змісту окремих полів кожного пакета.

Експертні системи. Акумулюють людські знання про виявлення причин аномальної роботи мереж та 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

Багатофункціональні пристрої аналізу та діагностики. В останні роки у зв'язку з поширенням обчислювальних мереж виникла необхідність розробки недорогих портативних приладів, що поєднують функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів і навіть деяких можливостей програмного забезпечення мережного управління.

Одним із важливих завдань моніторингу є контроль за безпекою обчислювальної мережі. Всі перераховані засоби та продукти моніторингу контролюють роботу елементів обчислювальної мережі, але не контролюють безпеку трафіку, що проходить, і ступінь захищеності елементів мережі та всієї мережі в цілому.

Безпека комп'ютерної мережі (у сенсі захищеності від шкідливих дій) забезпечується двома методами: аудитом і контролем. Аудит безпеки – перевірка налаштування мережі (відкритих портів, доступності "внутрішніх" програм ззовні, надійності автентифікації користувачів).

Сутність контролю безпеки полягає у виявленні аномальних подій у функціонуванні мережі та контролює:

– навантаження на серверне ПЗ та залізо: аномально високі рівні завантаження процесора, раптове скорочення вільного місця на дисках, різке збільшення мережного трафіку найчастіше є ознаками мережевої атаки;

– журнали та звіти на наявність помилок: окремі повідомлення про помилки в лог-файлах програм-серверів або журнал подій серверної операційної системи допустимі, але накопичення та аналіз таких повідомлень допомагає виявити несподівано часті або систематичні відмови;

– стан потенційно вразливих об'єктів – наприклад, тих, захищеність яких важко проконтролювати безпосередньо (ненадійне стороннє ПЗ, зміна/неперевірена конфігурація мережі): небажані зміни прав доступу до деякого ресурсу або вмісту файлу можуть свідчити про проникнення "ворога".

Існуючі системи моніторингу обчислювальної мережі є вузькоспрямованими, які вирішують певні завдання, не здатні бачити всю проблему загалом. Універсальна система моніторингу повинна забезпечити контроль за безпекою мережі, працездатністю мережі передачі даних, каналоутворювального обладнання та кінцевого обладнання користувачів, у тому числі, контроль наявності або відсутності технічного обслуговування всіх елементів. Все зазначене дозволить забезпечити своєчасне реагування на всі несправності, що виникають, в деяких випадках навіть до їх виникнення, скоротить тимчасові і трудові витрати на відновлення мережі після виникнення несправностей.

3 МОДЕЛІ МОНІТОРИНГУ УЧБОВОЇ ДІЯЛЬНОСТІ

Використання різноманітних технологій дистанційного навчання призводить до необхідності використання комплексних підходів до контролю учбової діяльності. Необхідно контролювати усі аспекти, які стосуються проведення он-лайн занять:

- контроль лабораторного обладнання;
- контроль присутності студентів у системі;
- контроль використання лабораторних ресурсів;
- контроль звітності студентів про виконання завдань.

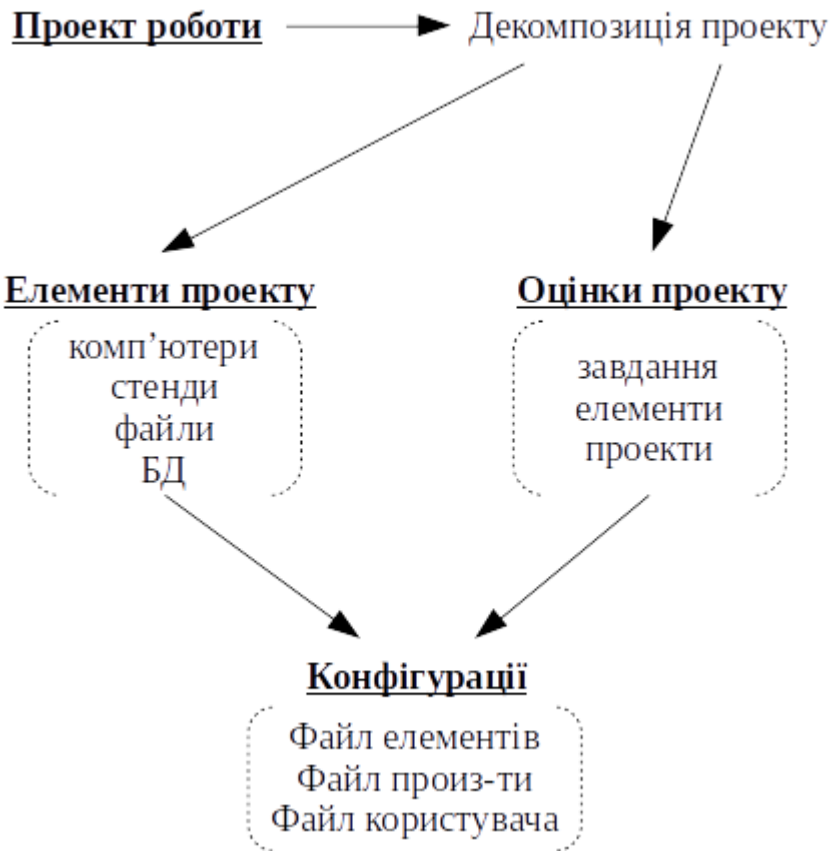

Рисунок 3.1 - Модель контролю учбових завдань

Для реалізації даних функцій необхідна система моніторингу, яка дозволяє встановлювати тригери, засновані на складних моделях об’єктів контролю. Також, система моніторингу повинна підтримувати відносно простий формат даних опису сутностей, які підлягають контролю, для запобігання утворення складних конфігураційних файлів та структур баз даних.

Основні складові такої системи визначаються програмно-апаратними підсистемами, які використовуються віддаленими або локальними лабораторіями та іншими учбовими системами.

Надання сервісів з даного контролю, дозволяє викладачу оперативно втручатись в проблемні ситуацій, такі як збій сервісів, відмова апаратних складових тощо. Але основною задачею розгортання моніторингу в даному дослідженні є контроль виконання студентами завдань з ціллю автоматизації частини процесів викладача.

3.1 Контроль присутності

Контроль присутності дозволяє отримувати інформацію про наявність студентів в системі дистанційної освіти або учбової лабораторії, а також тривалість цієї присутності. При цьому, викладача, як правило, цікавлять наступні характеристики:

- визначення типу активності;
- часові маркери присутності;
- доступ до ресурсів.

Для організації даного типу контролю, необхідно використовувати структуровану інформацію про систему та її користувачів, яку можна описати наступною моделлю

Для контролю в системі необхідно використання наступних сутностей:

- activity;
- students;

- folder;
- action

Сутність “activity” визначає найменування роботи, яка виконується та підлягає контролю. Ідентифікація системою виконується за рахунок унікального ідентифікатора з бази даних, користувачами - назвою проекту, відповідно до учбового плану або методичних вказівок. Назва проекту чи активності використовується як корень дерева подій в панелі моніторингу для відображення.

Сутність “students” визначає перелік студентів, які повинні виконати відповідне завдання. Ідентифікатор бази даних дозволяє унікально визначати учасника, навіть при повному співпадінні ФІО студента. Додатково використовується зв’язка із академічною групою студента. Також, використовуються аутентифікаційні дані, які користувач задіює при вході в систему навчання.

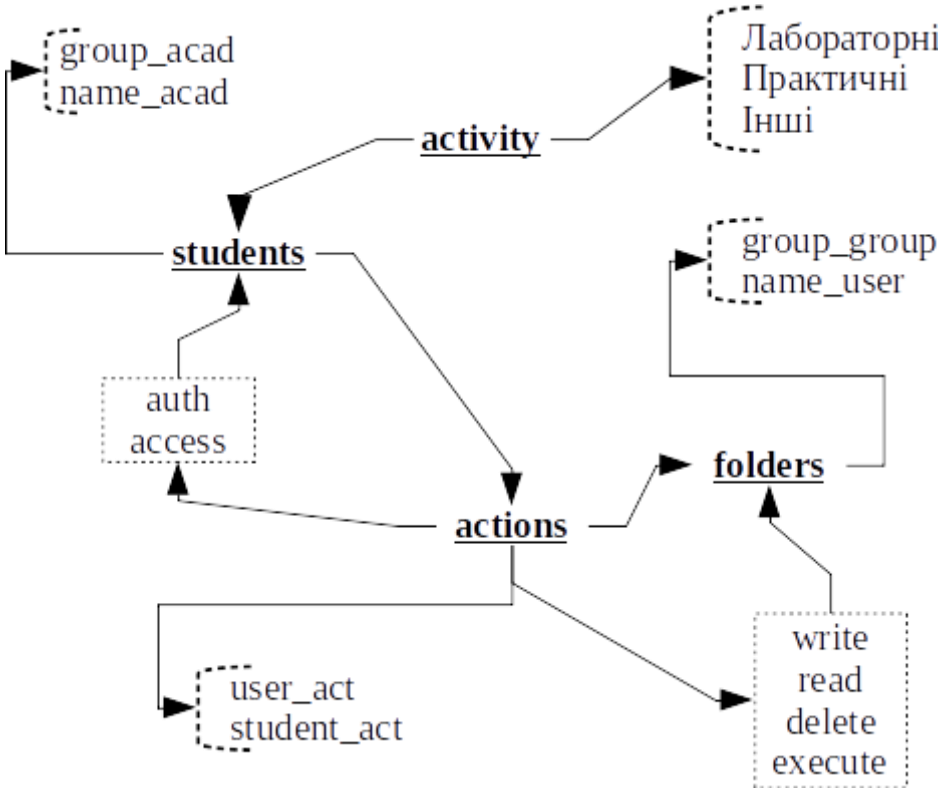

Рисунок 3.2 - Структурна модель активності студентів

Сутність “folder” визначає шлях для ресурсів, які необхідні для виконання відповідної активності. За кожним проектом закріплено відокремлений каталог, в якому здійснюється зберігання файлів проекту. До каталогу визначаються права доступу:

- власник каталогу, викладач, який створив проект. Має повні права на каталог та його файли;
- група, яка має доступ до каталогу. Группа студентів, не обов’язково з однієї академічної групи, які прив’язані викладачем до проекту;
- інші особи не мають ніякого доступу до цих файлів.

Спроба доступу не авторизованими особами визиває виключення та повідомлення адміністратору активності. Студенти, які створюють файли у відповідному каталозі активності, стають власниками такого файлу і інші користувачі не мають на нього прав. Будь-яка спроба неавторизованого доступу визиває виключення та повідомлення адміністратора активності (викладача).

Взаємодія між елементами моделі описується діями, які відповідають логіці відносин для відповідного елементу. Для сутності студентів визначаються основні дії, такі як авторизація та доступ до каталогу.

В першому випадку, контролю підлягають маніпуляція, які стосуються прав доступу до ресурсів системи, такі як зміна паролю, факт входу в систему, аудит час знаходження в системі та інше.

В другому випадку контролю підлягають дії студентів під час виконання учбових активностей, зокрема, доступ до файлів, звернення до баз даних тощо.

Опис структури контролю активностей студентів доцільно здійснювати, використовуючи інструменти структурованого ієрархічного опису сутностей. Зокрема, в рамках дослідження, використовувалася мова розмітки XML, яка дозволяє надати структуру кожного об’єкту системи, її взаємозв’язків, а також підтримується обраною системою моніторингу Zabbix.

3.2 Контроль подій

В ході виконання студентами ті викладачами активностей, необхідно контролювати події, які виникають в ході виконання завдань.

Для здійснення контролю проведення активностей, необхідно відслідковувати наступні події, які пов’язані зі студентами та викладачами відповідної активності:

- доступність та цілісність файлів активності;
- доступність та цілісність БД активності;
- доступність вузлів;
- доступність сервісів;
- несанкціонований доступ до ресурсів;
- вхід/вихід студентів з проекту;
- запит на консультацію;
- відсутність активності студентів.

Кожна нестандартна подія (з перелічених вище) підсвічується в окремій секції інтерфейсу системи моніторингу для запобігання перетинання із відображенням учбових активностей студентів.

Події поділені на чотири секції:

- контроль доступності та цілісності даних;
- контроль доступності вузлів та сервісів;
- контроль доступу та присутності користувачів;
- запити на консультацію.

Перша секція відповідає за контроль цілісності інформаційних ресурсів учбової лабораторії, зокрема, файлові ресурси та бази даних. В даному контексті контролю підлягає файлова структура каталогів та розгорнуті бази даних та їх таблиці.

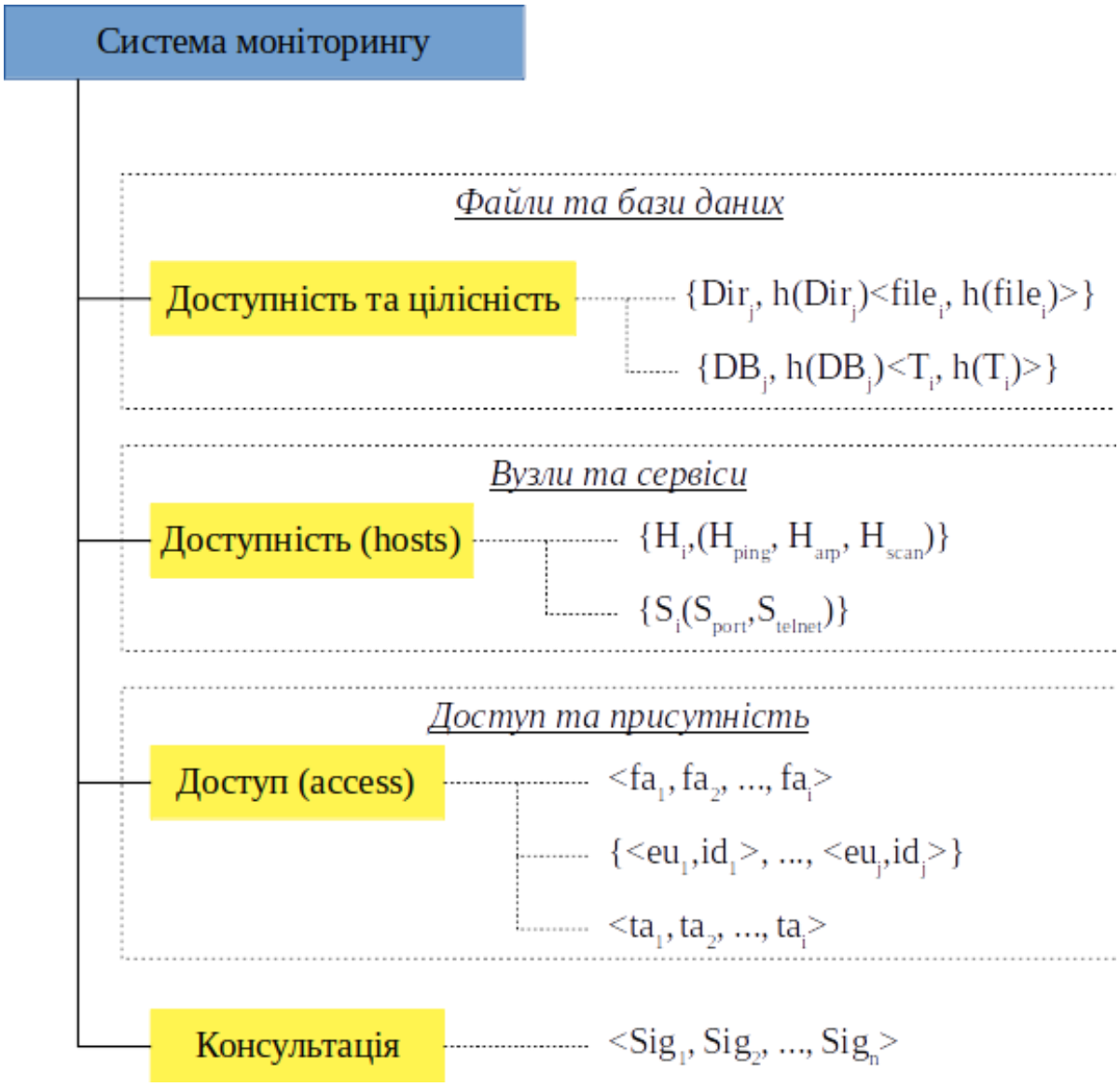

Рисунок 3.3 - Модель контролю подій

Доступність визначається наявністю відповідних ресурсів в системі за рахунок періодичних опитувань, а також контролю видалення ресурсів. Контроль цілісності визначається множиною контрольних сум файлів *h(file)* та каталогів *h(Dir)* з використанням хеш-функції як інструменту створення унікальних ідентифікаторів ресурсів системи. Першочерговим контролем здійснюється контроль каталогів учбової системи, що дозволяє зменшити кількість контрольних розрахунків, і безпосередній контроль файлів здійснюється тільки в тому разі, коли виявлені зміни в каталозі.

Друга секція визначає події, пов’язані з доступністю хостів лабораторії (лабораторного обладнання) та сервісів, які з ними пов’язані. Контроль доступності кінцевих вузлів здійснюється універсальними засобами, котрі здатні використовуватись стосовно будь-якого типу обладнання, яке здійснює функції в комп’ютерній мережі. Зокрема, для контролю доступності вузлу використовуються три основні методи:

– *ping* сканування вузлів *Hping* визначає доступність вузлу на рівні стеку TCP/IP та дозволяє робити висновки про роботу операційної системи та мережевих інтерфейсів;

– arpping сканування *Harp* здійснює виявлення мережевих пристроїв на канальному рівні, що дозволяє виявлявляти вузли, які блокують icmp запити на рівні операційної системи;

– сканування кінцевих вузлів *Hscan* дозволяє визначати додаткову інформацію, якщо необхідно обійти певні захисні системи або виявити більше інформації про об’єкт системи учбової лабораторії.

Контроль сервісів визначається множиною характеристик, які надають інформацію про наявність відповідного застосування або сервісу на кінцевому вузлі. Серед основних методів виявлення доступності сервісів є сканування відповідних TCP-портів, які закріплені за сервісом або застосування, а також віддалене з’єднання з відповідним сервісом.

Третя секція визначає контроль подій, які пов’язані із діяльністю студентів, зокрема факти входу або виходу з системи навчання або учбової лабораторії, а також факти несанкціонованого доступу до ресурсів учбової системи:

– параметр <fa1, fa2, …, fai> визначає множину спроб несанкціонованого доступу до ресурсів учбової системи. На даний момент це єдина система оцінки як доступу з ціллю несанкціонованого доступу так і невдалих спроб авторизації, тож, в подальшому, передбачено розмежування даної множини на декілька підмножин для структурованого опису подій, пов’язаних з безпекою даних в системі;

– множина пар <ei, idi> визначає кортеж характеристик доступу (входів, звертання до ресурсів) користувачів системи за рахунок їх унікальних ідентифікаторів та часових міток входів та виходів з системи або вузлу лабораторії;

– на основі часових міток входу та виходу, характристики <ta1, ta2, …, tan> визначає множину значень присутності користувача в системі з позиції значень часу, який був затрачено на виконання певної активності. Даний параметр дозволяє, в подальшому, проводити аналіз використання лабораторних ресурсів та визначення середнього часу, який потрібно виділяти на виконання завдання.

Останній параметр визначає множину сигналів, які формуються при звертанні студентів за консультацією або допомогою. Кожний сигнал визначається часовою міткою його формування та ідентифікатором студента, котрий його ініціював.

3.3 Контроль виконання задач

Для контролю виконання задач та завдань необхідно, щоб були виконані наступні дії:

Етап 1. Викладачу необхідно підготувати лабораторну роботу. Виконання цього етапу залежить від типу дисципліни та здійснюється виключно профільними викладачами та їх асистентами. Основні дії на цьому етапі:

– підготовка та завантаження файлу активності, форматування файлу для доступу до нього з мережі інтернет (html документ);

– планування середи виконання активності. Визначаються вузли, сервіси та інші елементи, які необхідні для виконання активності;

– підготовка віртуального стенду. Формування структури віртуальної середи виконання завдань на основі файлу опису проекту;

– формування структурного опису контролю проекту для завантаження на сервер моніторингу.

На цьому етапі здійснюються організаційни заходи щодо формування представлення проекту.

По перше, план (методичні вказівки) проекту проходять етап форматування у веб документ. Враховуючи, що в більшості випадків, доцільно організувати доступ до методичних ресурсів з використанням мережі інтернет, методичні вказівки формуються в html документ.

Якщо лабораторна система передбачає використання віртуальних ресурсів, які автоматично розгортаються на відповідних лабораторних платформах, на основі плану необхідно сформувати файл опису, на основі якого буде видано ресурси лабораторії та опис елементів, які підлягають моніторингу.

XML опис системи контролю визначає наступні параметри:

– віртуальні лабораторні вузли, які підлягають контролю;

– сервіси, які використовуються для функціонування лабораторного проекту;

– етапи виконання завдання;

– тригери, на основі яких система моніторингу повинна сповіщати про події в системі;

– умови, при яких функціонують відповідні характеристики, які спостерігаються.

Таким чином, здійснюється підготовка даних для веб системи лабораторії, для надання учбових завдань, системи віртуалізації лабораторії для формування об’єктів, необхідних для виконання завдань і системи моніторингу, яка спостерігає за визначеним переліком характеристик функціонування відповідного лабораторного або практичного проекту.

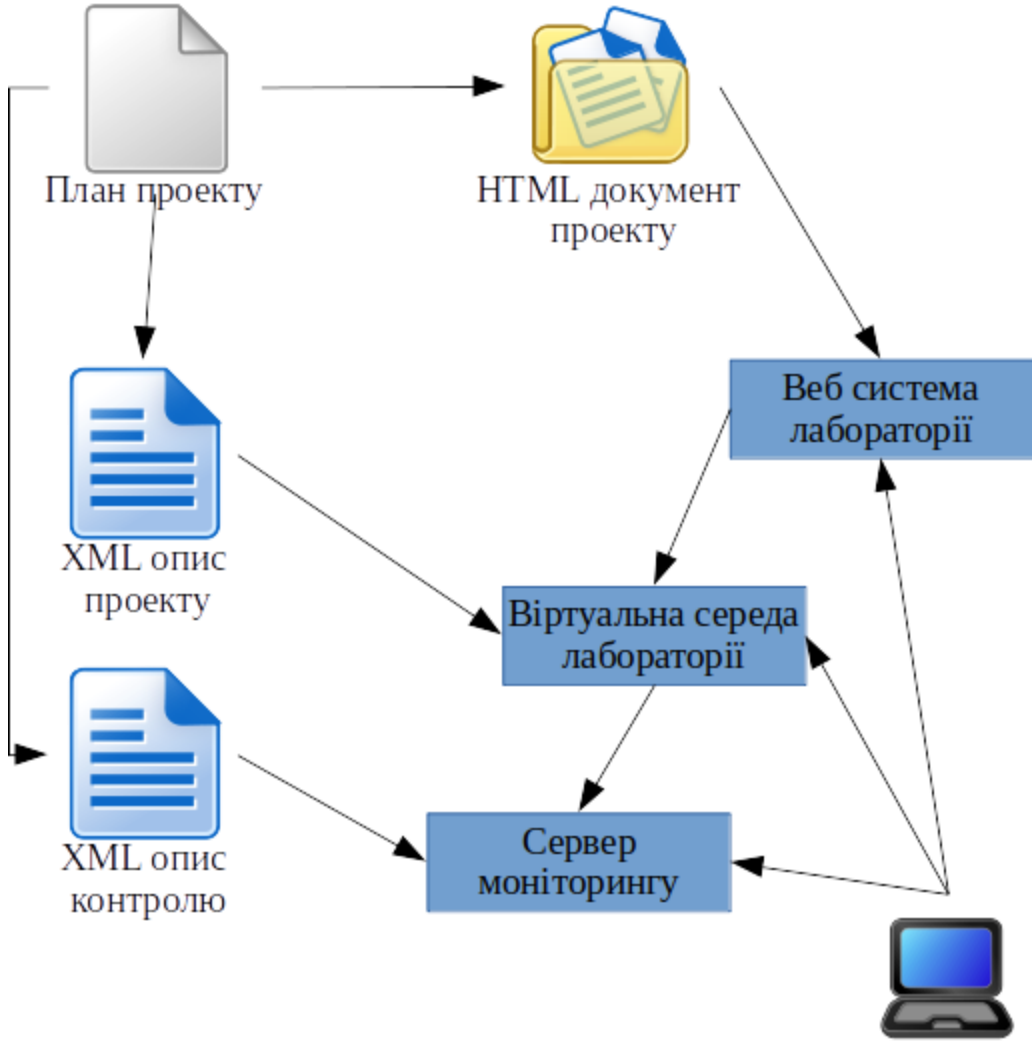

Рисунок 3.4 - Формування проекту та його системи контролю

Етап 2. На другому, і основному, етапі необхідно визначити послідовність виконання відповідної активності студентом. Основними задачами викладача на цьому етапі є:

- розмітка етапів виконання активності;
- визначення еталонних значень виконання кожного етапу;
- формування відповідного файлу конфігурації контролю активності;
- завантаження файлу на сервер моніторингу.

Всі ці кроки описуються наступною інформаційною моделлю

$$act = \{taski, Qi, Mi\}$$

де, taski = <Qsi, ti>

Qi = <qi, Δq>

ti = <tist, tim>

Mi = {m1, m2, …, mk}

Параметр taski визначає задачу, яка виконана студентом за час ti та отримав результат Qsi. При цьому, отриманий результат порівнюється з шаблонним значенням Qi, яке складається з множини оцінок qi та визначених викладачем відхилень від них Δq.

Параметр часу ti визначає визначає час, який затрачено на виконання етапу, за рахунок визначення часу початку виконання завдання tist та часу досягнення маркеру tiM, який виставлено викладачем для оцінення та відображення в системі моделювання.

Mi визначає множину маркерів, які виставив викладач для даного проекту.

3.4 Контроль звітності

В ході виконання активностей необхідно здійснювати контроль звітності про виконання завдань студентами. Мінімальним завданням для контролю звітності є сповіщення про виконання активності або її окремого етапу. Для цього, в попередньому пункті було розроблено моделі формування контролю активностей. Проте, окрім цього, необхідно забезпечити контроль більш широкого спектру діяльності студентів в ході виконання проектів:

- виконання етапу завдання;
- виконання завдання;
- ідентифікація результатів студентів;
- ідентифікація завантажень звітів студентів.

Загальну структуру контролю звітності активностей можна визначити ієрархією, як зображено на рисунку 3.5, яка визначає процес взаємодії елементів активностей із системою зберігання.

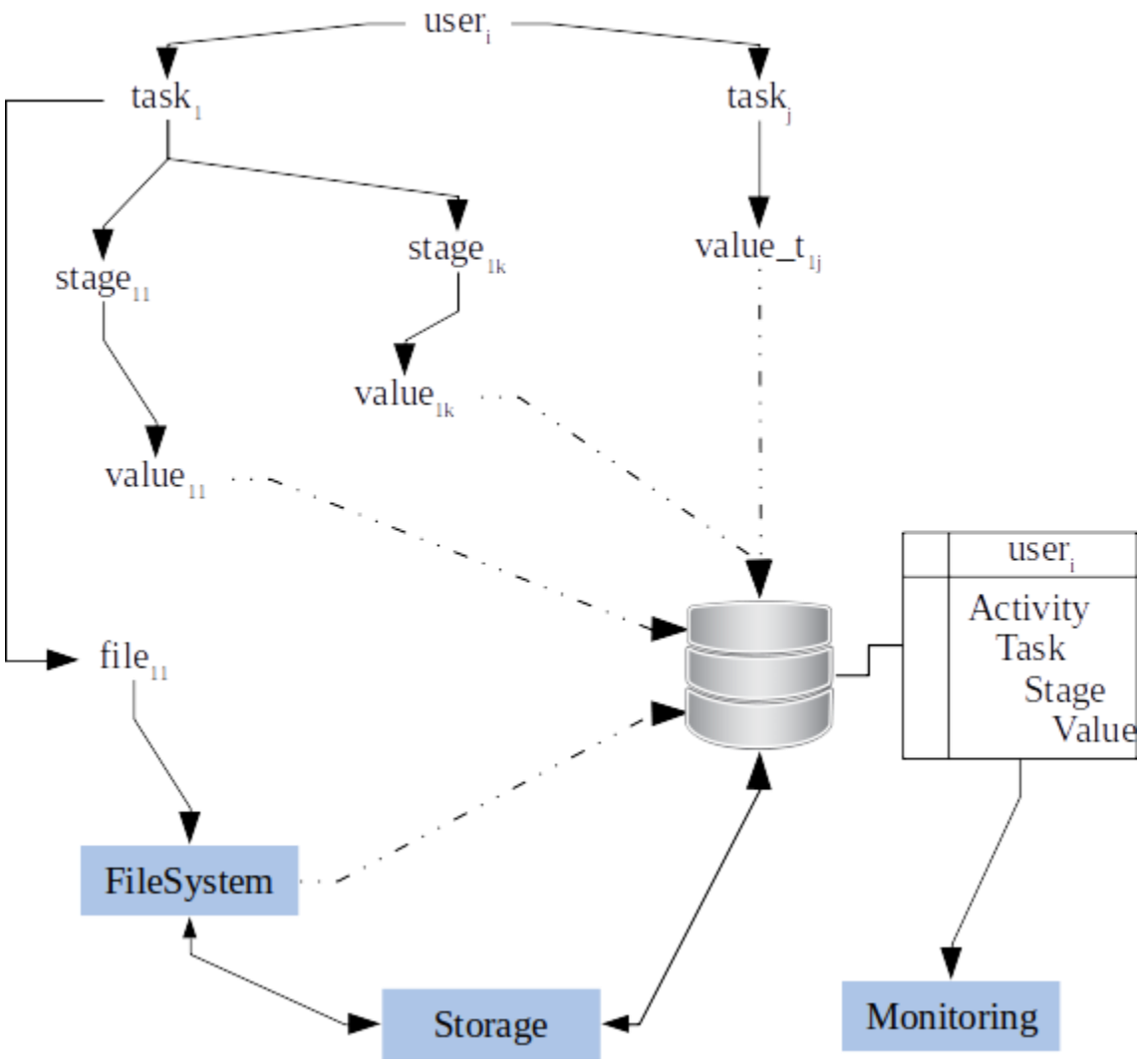

Рисунок 3.5 - Структура контролю звітності

Для кожного студента створюється асоціація із відповідною активністю (лабораторна робота, практичне завдання, розрахункова робота тощо), яка є основною одиницею оцінювання роботи. Робота складається з одного або декількох завдань $task_i$.

Кожне завдання розбивається викладачем на етапи, які підлягають оцінці $value_i$. Оцінка виставляється за кожний виконаний етап $stage_k$, а також за виконане завдання $value\_t_{ij}$.

В якості оцінювального елементу, в системі контролю, допускається завантаження файлів відповідей. Однак, враховуючи, що на момент проведення дослідження не було створено системи аналізу змісту файлів, система контролю та моніторингу фіксує та сповіщає про сам факт завантаження документу та виставляє умовну оцінку, визначену викладачем на етапі розмітки проекту.

Кожна оцінка підлягає фіксації в окремій базі даних для подальшого зберігання та відображеня в веб-панелі системи моніторингу. В тієї ж базі даних фіксуються посилання на усі завантажені студентами файли, що дозволяє отримувати ієрархію оцінок за виконання всіх задач активності та оцінки самої активності.

Файли активностей та база даних оцінок розташовуються в окремій системі зберігання, яка забезпечує надлишковість даних для організації їх цілісності та створювати структуризацію оцінок активностей.

У відповідності до цієї структури, в ході дослідження було розроблено модель, яка описує дані які зберігаються в сховищі та підлягають контролю з боку викладача та інших осіб.

Загальна модель даних контролю визначається наступним чином

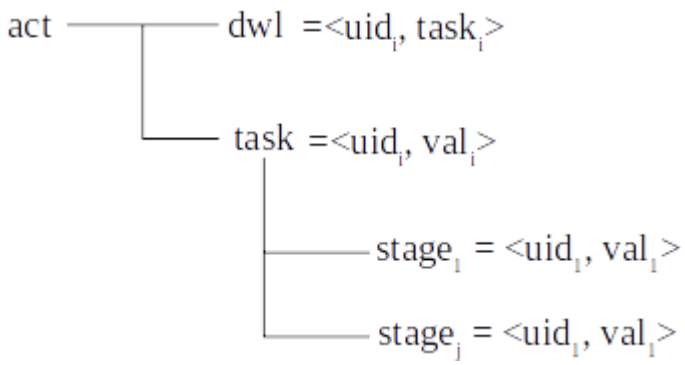

Рисунок 3.6 - Модель даних контролю учбової діяльності

Модель задає структуру відображення звітності про перебіг учбових активностей, яка дозволяє ідентифікувати тип активності, виконавця активності, виконані завдання та оцінки за ці завдання.

3.5 Контроль використання ресурсів

В ході виконання учбових завдань, студенти здійснюють підключення до навчальних порталів, локальних та віддалених лабораторій, сховищ та інших апаратних та програмних ресурсів віддаленої лабораторії. Відповідно, виникає необхідність у здійсненні контролю використання цих ресурсів, що дозволяє оперативно відреагувати на проведення навчального процесу.

Основні ресурси, які підлягають моніторингу:

- кількість процесів на сервері веб-порталу учбового закладу;
- кількість процесів на сервері зберігання;
- використання дискового простору сховища учбової системи;
- завантаження процесору відповідного серверу;
- доступність ресурсів.

Контроль даних ресурсів з боку викладачів та інженерів, необхідний для організації процесу навчання студентів, зокрема:

- створення черг доступу до ресурсів. Даний процес необхідний, коли обчислювальні ресурси серверів лабораторії не можуть забезпечити виконання задач для всіх студентів одночасно;
- контроль ресурсів в ході виконання завдань. Якщо в процесі роботи виявляється, що ресурси лабораторії близькі до вичерпання, необхідні повідомлення, які дозволять викладачу прийняти відповідні міри;
- викладачам та інженерам необхідно в реальному режимі часу бачити доступність ресурсів віддаленої лабораторії для оперативного реагування на інциденти.

Таким чином, моніторинг ресурсів системи, також є частиною системи моніторингу учбової діяльності та повинний відображати роботу інформаційної системи лабораторії наряду з іншими контрольованими параметрами. Також, для адекватної оперативної реакції на події, необхідно,

щоб система моніторингу визначала, які конкретно проекти використовують найбільшу кількість ресурсів, для визначення реакції.

В такому разі, модель контролю використання ресурсів може визначатись наступним чином

$$Res = \{R_{CPU}, R_{MEM}, R_{Proc}, R_{CPU}, R_{Disk}, R_{Mav},\},$$

де, $R_{CPU} = \{<sid_i, cid_{ij}>\}$ - множина процессорів,

$R_{MEM} = \{<sid_i, M_i>\}$ - множина показників ОЗП,

$R_{Proc} = \{<sid_i, P_i>\}$ - множина процесів в системі,

$R_{Disk} = \{<sid, D_{io}, D_t, D_{SMART}>\}$ - множина характеристик дискової підсистеми,

$R_{Mav} = \{<eid_i, M_i, t_k>\}$ - множина маркерів доступності обладнання

Кожний з параметрів визначається, в першу чергу, із сервером, від якого отримано інформацію і який має свій унікальний, в рамках системи, ідентифікатор *sid*. Інші параметри визначаються як композиія з ідентифікатором сервера:

– за ідентифікатором процесору *cid* визначається, множина процесорів серверу та їх навантаження;

– кількість використаної пам’яті M_i визначає використання оперативної пам’яті відповідного серверу системи;

– кількість процесів P_i на відповідному сервері визначає які сервіси та програми запущені на сервері і за якими користувачами ці процеси закріплені;

– множина параметрів $\{<sid, D_{io}, D_t, D_{SMART}>\}$ визначає інтенсивність роботи дискової підсистеми в лабораторії, зокрема характеристики вводу/виводу D_{io}, перевищення температурних режимів D_t, наявність помилок на конкретному диску D_{SMART};

– множина маркерів доступності визначає активність обладнання та його сервісів в учбовій мережі.

Виходячи з цього, побудована структурна модель даних контролю використання ресурсів, яка описує взаємодію параметрів моніторингу та їх відображення. Контроль ресурсів, які використовуються певним проектом зображено на рисунку 3.7.

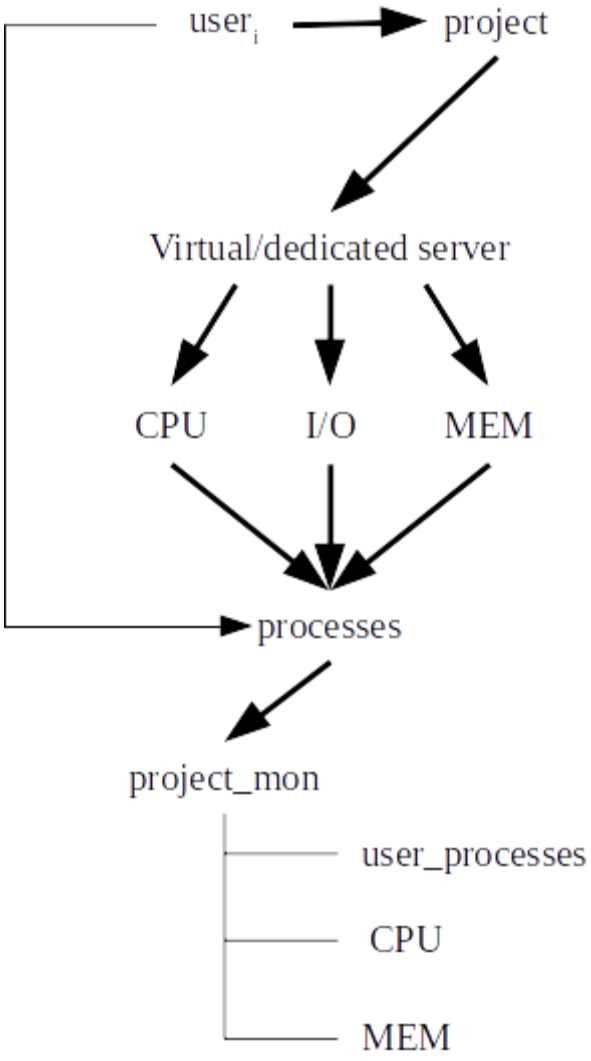

Рисунок 3. 7 - Структурна модель контролю ресурсів

Враховуючи, що будь-яка система визначає процес, користувача, котрий ініціював цей процес, та ресурси, який цей процес затронув, можна побудувати ланцюг залежностей, який визначає наступні параметри:

1. користувач виконує певний проект, і тим самим створюється відповідна зв’язка між ними;

2. проект розгорнутий на певному віртуальному або виділеному серверу, що визначається повним шляхом знаходження файлів проекту;

3. після визначення сервера, можна отримувати його дані про використання ресурсів;

4. визначення інформації про користувача надає можливості отримувати інформацію, які саме процеси на сервері породжені ним;

5. для кожного процесу отримуються значення використання процесору та оперативної пам’яті;

6. інформація про завантаженість системи від процесів, а також кількість процесів від одного користувача визначає вплив проекту на загальне навантаження на сервер від кожного проекту.

Отримана структура дозволяє визначати використання ресурсів від проектів, наряду із загальним навантаженням на мережеве обладнання учбової лабораторії. В свою чергу, викладач, на основі отриманої інформації може приймати рішення про призупинення проекту, зупинення виконання конкретних студентів або виділення додаткових ресурсів для проекту.

3.6 Висновки до розділу

В даному розділі було проведено розробку та аналіз моделей, які визначають основні процеси здійснення контролю учбового процесу для лабораторій з віддаленим та локальним доступом.

Попередній аналіз систем моніторингу комп’ютерних мереж та мережевого обладнання показав, що найбільш адекватним інструментальним засобом для досягнення поставлених цілей дослідження є система моніторингу Zabbix. Система дозволяє контролювати мережеві об’єкти на основі опису цих об’єктів спеціальному форматі XML. Це дозволило створювати структуровані моделі, які вписуються в концепцію структурованого опису в форматах XML та YAML.

Розроблені моделі дозволили описувати структуру самих процесів здійснення контролю учбового процесу та описувати характеристики параметрів, які підлягають моніторингу викладачами та інженерами. Такі моделі легко сприймаються розробниками та адміністраторами та інтерпретуються в структурований опис, програмні засоби та інші системні утиліти.

В результаті використання даних моделей, можливо формувати опис параметрів, які необхідні для моніторингу учбового процесу, виявляти взаємозв’язкі між цими параметрами та завантажувати відповідні конфігураційні моделі в систему моніторингу.

ВИСНОВКИ

В ході виконання дослідження було проведено огляд, аналіз та розробку моделей моніторингу, які використовуються в системах моніторингу з огляду на специфіку організації інформаційних систем в учбовому процесі.

Розроблені моделі дозволяють визначати характеристики об’єктів, які підлягають моніторингу та структуру взаємодії параметрів моніторингу. Це дозволяє оперативно адаптувати систему моніторингу для нових об’єктів, або клонувати описи типових об’єктів, які вводяться в учбову лабораторію.

Серед переваг використання розроблених моделей можна зазначити наступні:

- серед вбудованих засобів контролю учбової діяльності, немає зручних та адекватних інструментів, або є необхідність суттєво втручатись в кодову базу LMS або використовувати додаткові модулі та плагіни;
- використання моделей контролю виконання завдань дозволило зменшити час оцінки робіт викладачем на 26% за рахунок динамічного відображення інформації на панелях моніторингу;
- використання моделей контролю використання ресурсів дозволяє оперативно реагувати на перевантаження лабораторного обладнання та керувати чергами студентів на виконання активностей;
- моделі контролю звітності дозволили скоротити час оцінювання виконання активностей студентів на 23,6%;
- вибрана система моніторингу дозволяє адаптувати моделі об’єктів контролю та впроваджувати нові, за рахунок використання структурованих описів цих об’єктів.

Також, в ході даного дослідження не розглядалося, або не враховувалось певні фактори функціонування систем контролю учбового контенту, зокрема:

- результати дослідження не враховують можливості організації модулів, які інтегруються в сучасні LMS;
- адекватність роботи системи моніторингу суттєво залежить від апаратних ресурсів, які використовуються даною системою, що може призвести до затримок в отриманні інформації, в разі великої кількості користувачів та об’єктів моніторингу;
- підтримка системи моніторингу вимагає певного рівня кваліфікації від викладача або інженера лабораторії.

Серед напрямів подальшого розвитку даного дослідження можна зазначити автоматизацію отримання описів параметрів контролю учбової діяльності, зокрема, створення моделей присутності та виконання завдань. Також необхідним є розробка системи контролю доступу студентів до ресурсів віддаленої лабораторії без втручання викладача або його мінімальним втручанням.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. M. Just. Designing authentication systems with challenge questions. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Use, сторінки 143–155, Sebastopol, CA, 2005. O'Reilly Media, Inc. [Електронне джерело] Режим доступу: ttps://pdfs.semanticscholar.org/fbfb/c601e 582f904decf2f739a4e1d41ee86ec0d.pdf

2. K. D. Mitnick and W. L. Simon. The Art of Deception: Controlling the Human Element of Security. Wiley, 2012. [Електронне джерело]Режим доступу: http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

3. Social Authentication. Alex Rice[Електронне джерело] Режим доступу: blog.facebook.com/blog.php?post=486790652130.

4. J. Podd, J. Bunnell, and R. Henderson. Cost-effective computer security: Cognitive and associative passwords. In OZCHI '96: Proceedings of the 6th Australian Conference on Computer-Human Interaction (OZCHI '96), page 304, Washington, DC, USA, 1996. IEEE Computer Society. [Електронне джерело] Режим доступу: http://ieeexplore.ieee.org /document/560026/?reload=true

5. M. Zviran and W. J. Haga. User authentication by cognitive passwords: an empirical assessment. In JCIT: Proceedings of the Fifth Jerusalem Conference on Information technology, pages 137–144, Los Alamitos, CA, USA, 1990. IEEE Computer Society Press. [Електронне джерело]Режим доступу: https://www.researchgate.net/publication/3505320_User_authentication_by_cognitive_passwords_an_empirical_assessment

6. CREDANT Technologies. Mountains of mobiles left in the back of New York cabs, 16, 2008. [Електронне джерело]Режим доступу: www.credant.com/mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html.

7. T. Bridis. Hacker impersonated Palin, stole e-mail password, Sept. 18, 2008. Associated Press. Режим доступу: http:// www.ycorpblog.com/2008/10/08/ impersonated.zip.

8. S. Schechter, S. Egelman, and R. W. Reeder. It’s not what you know, but who you know: A social approach to last-resort authentication. In CHI ’09: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, 2009. ACM. [Електронне джерело]Режим доступу: http://www.guanotronic.com/serge/ papers/chi09b.pdf