Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-24М
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Кашпуровський Д.С.
«____» _____ 2025 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Буравченко К.О.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Кашпуровський Д.С. Дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого моніторингу та контролю стану ІТ.

Метою розробки є дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

Об'єктом дослідження є процес мережевого моніторингу та контролю стану ІТ.

Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, мережа, моніторинг, контроль стану, ІТ

ABSTRACT

Kashpurovskyi D.S. Research and software implementation of the network monitoring and control system for IT status. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed, which is intended for the network monitoring and control system for IT status.

The purpose of the development is the research and software implementation of the network monitoring and control system for IT status.

The object of the research is the process of network monitoring and control of IT status.

The subject of the research is the methods of network monitoring and control of IT status.

The research methods are based on the methods of computer network theory, methods of mathematical statistics, and methods of software development.

The result of the work is the software implementation of the network monitoring and control system for IT status.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A user-friendly interface has been developed. Instructions for working with software tools are provided.

The program can be used on PCs with Windows 10/11.

The program is developed in the Python environment.

Keywords: computer engineering, network, monitoring, status control, IT

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

DMA – (Direct memory Access) – прямий доступ до пам‘яті;

ISA – 16 бітна шина персонального комп’ютера;

PC – (Personal Computer) – персональний комп’ютер;

PCI – 32 бітна шина персонального комп’ютера;

Socket – порт взаємодії з мережею;

ВІС – велика інтегральна схема;

ЕОМ – електронна обчислювальна машина;

ЗП – зовнішній пристрій;

ЗЗП – зовнішній запам‘ятовуючий пристрій;

ІС – інформаційна система;

ІТ – інформаційні технології;

КПДП – контролер прямого доступу до пам‘яті;

КС – комп’ютерна система;

МП – мікропроцесор;

НГМД – накопичувач на гнучких магнітних дисках;

НМД – накопичувач на магнітних дисках;

ОЗП – оперативний запам‘ятовуючий пристрій;

ОС – операційна система;

ПДП – прямий доступ до пам‘яті;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СЦМК – сервіс централізованого моніторингу та контролю.

ВСТУП

Актуальність теми. Інструменти моніторингу мережі – це програмні рішення для контролю, аналізу та управління продуктивністю та станом мережі. Ці інструменти постійно контролюють різні мережеві компоненти, такі як маршрутизатори, комутатори, сервери та програми, щоб забезпечити їх правильне функціонування.

Відстежуючи такі показники, як трафік, затримка та час безвідмовної роботи, вони допомагають IT-командам виявляти та вирішувати проблеми, перш ніж вони переростуть у серйозні проблеми. Основною метою інструментів моніторингу мережі є підтримка доступності, надійності та безпеки мережі. Вони забезпечують видимість мережевої активності, дозволяючи організаціям виявляти неефективність, збої або загрози безпеці.

Крім того, ці інструменти підтримують планування потужностей, оптимізацію продуктивності та дотримання угод про рівень обслуговування (SLA). Сучасні інструменти моніторингу мережі часто інтегрують такі функції, як аналітика в режимі реального часу, аналітика на основі штучного інтелекту та підтримка хмарної інфраструктури.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевого моніторингу та контролю стану IT.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевого моніторингу та контролю стану IT.

– Дослідження системи мережевого моніторингу та контролю стану IT.

– Програмна реалізація системи мережевого моніторингу та контролю стану IT.

Об'єктом дослідження є процес мережевого моніторингу та контролю стану IT.

Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого моніторингу та контролю стану ІТ.

– Розроблено вітчизняний продукт мережевого моніторингу та контролю стану ІТ, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевого моніторингу та контролю стану ІТ.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVII Науково-технічній конференції здобувачів вищої освіти LV науково-технічної конференції «Наука в ЦНТУ: основні досягнення та перспективи розвитку» (2025 р.), основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №15.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Рішення для моніторингу мережі повинно включати такі можливості.

Моніторинг продуктивності в режимі реального часу

Моніторинг продуктивності в режимі реального часу включає відстеження та аналіз даних під час їх проходження мережею, що забезпечує миттєвий зворотний зв'язок щодо трафіку, підключення та завантаження сервера. Такий швидкий доступ до показників продуктивності дозволяє IT-командам оперативно виявляти та вирішувати проблеми.

Завдяки моніторингу в режимі реального часу організації можуть підтримувати оптимальну продуктивність мережі та зменшувати час простою. Постійно спостерігаючи за мережевою активністю, IT-команди можуть передбачати проблеми, перш ніж вони вплинуть на взаємодію з користувачами.

Моніторинг доступності

Моніторинг доступності зосереджений на забезпеченні працездатності та доступності всіх мережевих компонентів. Він перевіряє час безперебійної роботи та стан серверів, програм і мережевих пристроїв, оперативно попереджаючи IT-персонал про будь-які проблеми з доступністю. Ця функція життєво важлива для забезпечення безперервної доступності послуг, підтримки критично важливих бізнес-процесів та дотримання угод про рівень обслуговування (SLA).

Впроваджуючи моніторинг доступності, організації можуть зменшити ризик непередбачених простоїв. Безперервне відстеження дозволяє швидко вирішувати проблеми, гарантуючи мінімальний вплив збоїв у роботі мережі.

Аналіз трафіку та пропускної здатності

Аналіз трафіку та пропускної здатності надає уявлення про те, як використовуються мережеві ресурси, та виявляє закономірності, які можуть

свідчити про неефективність або загрози. Інструменти моніторингу мережі використовують методи збору даних для аналізу потоку трафіку, використання пропускної здатності та швидкості передачі пакетів. Цей аналіз допомагає зрозуміти навантаження мережі та точки перевантаження, що дозволяє адміністраторам оптимізувати продуктивність.

Ефективний аналіз трафіку та пропускної здатності допомагає збалансувати мережеві ресурси та запобігти перевикористанню, забезпечуючи, щоб критично важливі програми отримували необхідну пропускну здатність. Визначаючи джерела трафіку та розуміючи моделі використання, ІТ-команди можуть приймати обґрунтовані рішення щодо планування потужностей та модернізації мережі.

Моніторинг безпеки

Моніторинг безпеки – це життєво важлива функція, яка зосереджена на виявленні та пом'якшенні потенційних загроз і вразливостей у мережі. Вона включає відстеження підозрілої активності, спроб несанкціонованого доступу та незвичайних потоків даних. Інструменти моніторингу мережі використовують такі методи, як виявлення вторгнень та аналіз поведінки, для підвищення безпеки мережі.

Впровадження моніторингу безпеки гарантує швидке виявлення та усунення загроз. Така проактивна позиція є важливою для захисту конфіденційних даних та забезпечення відповідності нормативним стандартам. Постійний моніторинг безпеки надає аналітичні дані, які допомагають удосконалювати політики безпеки та покращувати загальний стан безпеки організації.

Моніторинг хмарної інфраструктури

Моніторинг хмарної інфраструктури включає спостереження та аналіз продуктивності та стану хмарних сервісів і ресурсів. Ця функція стає дедалі важливішою, оскільки організації переходять до хмарних середовищ. Вона гарантує, що хмарні сервіси відповідають очікуванням щодо продуктивності,

підтримуючи надійність та доступність програм, розміщених у хмарі.

Ефективний моніторинг хмарних ресурсів допомагає оптимізувати використання хмарних ресурсів та керувати витратами. Відстежуючи стан сервісів, затримки та взаємодію з користувачами, IT-команди можуть швидко вирішувати проблеми та підтримувати рівень обслуговування.

Налаштовувані показники та інформаційні панелі

Налаштовувані показники та панелі інструментів дозволяють організаціям адаптувати моніторинг мережі до своїх потреб і цілей. Користувачі можуть вибирати відповідні показники ефективності та створювати панелі інструментів, які відображають критично важливу інформацію в доступному форматі.

Спеціально налаштовані панелі інструментів та показники дозволяють IT-командам швидко отримувати доступ до мережевих даних та інтерпретувати їх, що дозволяє швидше приймати рішення. Налаштовуючи середовище моніторингу, організації можуть узгодити зусилля з моніторингу з бізнес-цілями та операційними пріоритетами.

1.2 Область застосування

Навіть якщо дані збираються в потрібному обсязі, їх необхідно вчасно обробляти й аналізувати. А цього саме й не відбувається. Заковика полягає в тому, що розвиток моніторингу IT – майже завжди непрофільний і додатковий для власника компанії процес, що звичайно ніяк не планується й не розвивається. У результаті система моніторингу встановлюється, але не допрацьовується й зовсім не поліпшується. А це не той інструмент, якому можна залишити без уваги.

В IT-службі, зайнятий одночасно й моніторингом, і усуненням інцидентів і проблем, неминуче спостерігається конфлікт інтересів. Таке положення справ складається, коли за проведення моніторингу, видачу рекомендацій і корекцію ситуації відповідають ті самі фахівці. Наприклад, якщо IT-фахівець повинен

гарантувати доступність CRM протягом 95% часу, то оповіщення про проблему «псує» йому статистику.

У підсумку оповіщення просто не зареєструють у системі, хоча проблему, можливо, усунуть. Або більше банальний, але не менш сумний приклад: фахівцеві всього лише «небажання» розбиратися з виявленим інцидентом, особливо нетривалим і не занадто помітним. Отже, помилки будуть повторюватися й збирати, приводячи до появи слабких місць в інфраструктурі, а на їхнє усунення буде вимагатися усе більше сил і засобів.

Позаштатні ситуації, що виникають у результаті недбалості або впливу людського фактора, теж найчастіше залишаються незареєстрованними. Все це може приховувати системні проблеми – причому не тільки в інфраструктурі, але й у самому процесі IT-підтримки (особливо в тих компаніях, де IT-служба змушена обслуговувати велику кількість філій). Такі проблеми можуть залишатися непоміченими доти, поки моніторинг не стане остаточно марним.

Цю ситуацію можна змінити шляхом впровадження не просто технічної системи, а повноцінного сервісу централізованого моніторингу та контролю (СЦМК).

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого моніторингу та контролю стану IT, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Naumen Network Manager

Інструменти моніторингу, інтегровані в Naumen Service Desk, забезпечують контроль над станом об'єктів інфраструктури мережі, дозволяють відслідковувати доступність, безперервність і якість надання бізнес-послуг у рамках єдиної інформаційного й подійного середовища. Програмна система Naumen Network Manager включає сотні компонентів для контролю й наочного відображення інформації, які створені на основі типових інструментів обробки даних. Їх можна налаштовувати й вносити зміни без коректування програмного коду, використовуючи лише візуальні засоби. Network Manager пропонує широкі можливості для рішення завдань IT і бізнесу.

Гнучкий функціонал обробки даних

Моніторинг IT-інфраструктури в режимі реального часу полегшує персоналу служби підтримки контроль стану компонентів мережі й дозволяє швидко реагувати на поточні події. Запатентована технологія нормалізації інформації дозволяє зводити дані, що надходять за різними протоколами з різнорідних пристроїв, до єдиного формату універсальної таблиці. Для подальшої обробки даних передбачений гнучкий і зручний функціонал: діаграми, датчики, звіти й т.д.

Інтеграція з Service Desk

Система моніторингу займає важливе місце в керуванні IT-інфраструктурою. Інтеграція модулів Network Manager і Service Desk дозволяє забезпечити більше ефективне керування проблемами, конфігураціями й інцидентами, зберігаючи стабільний рівень підтримки користувачів.

Комплексний моніторинг інфраструктури

У сучасних компаніях якість обслуговування користувачів прямо впливає на обсяги продажів, тому пріоритетними стають завдання запобігання й усунення збоїв на тих етапах, коли вони ще не приводять до втрати продуктивності або неприступності послуг.

Рисунок 2.1 – Інтерфейс користувача Naumen Network Manager

Одержання послідовної й точної інформації про поточний стан той або інший бізнес-сервісу часом утруднено різноманіттям наявних у підприємств IT-об'єктів (мультивендорний парк обчислювальної техніки, різні серверні платформи й т.д.). Система Network Manager успішно справляється з такими проблемами, надаючи універсального функціонала для контролю стану мережі, інструменти візуалізації й аналітики, керування віртуальними й фізичними компонентами мережі.

Моніторинг і керування бізнес-послугами

В умовах перегони високих технологій перемога дістається не тому, хто вклав максимум засобів, а тому, хто організував максимально ефективне керування ресурсами. Інтеграція Service Desk і Network Manager надасть у ваше розпорядження комплексну систему керування бізнес-процесами. Рішення дозволяє забезпечити безперервне надання сервісів і відкриває нові можливості для підвищення якості послуг.

«Софт менеджмент»

Для забезпечення прозорості IT-інфраструктури й для відстеження працездатності всіх її компонентів застосовуються інструменти моніторингу. Рішення по моніторингу допомагають IT-фахівцям автоматизувати виконання більшості завдань по керуванню інфраструктурою, збирати інформацію про поточний стан її елементів на різних рівнях, визначати уразливі місця, і, на підставі цих відомостей, попереджати виникнення збоїв і критичних ситуацій.

Технології проактивного моніторингу дозволяють зробити IT-систему більше стабільною й відказостійкою, що позитивно відбивається на швидкості всіх бізнес-процесів.

«Софт менеджмент» пропонує впровадження системи моніторингу й аудита IT-інфраструктури на основі продукту Microsoft System Center Operations Manager (SCOM).

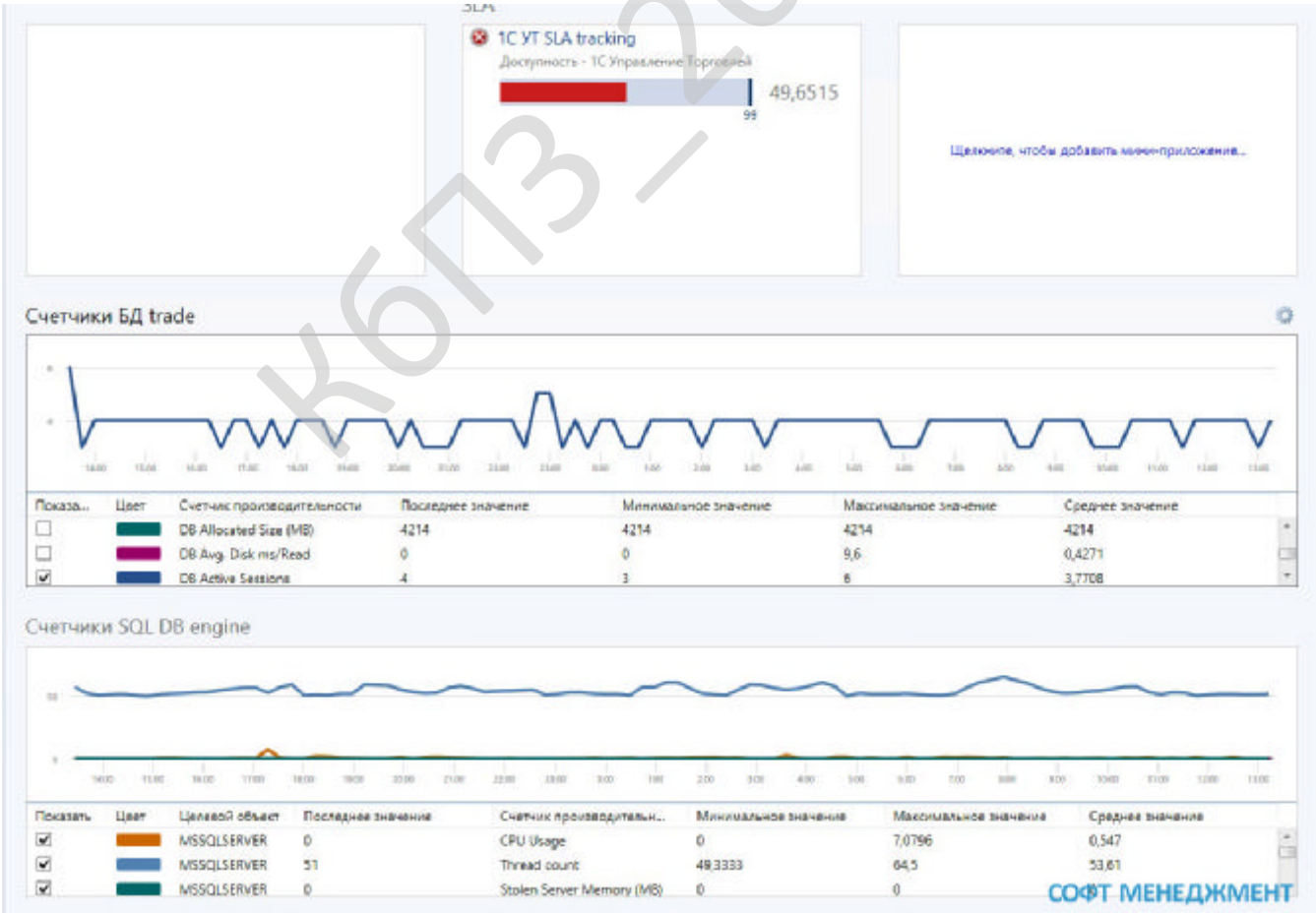

Рисунок 2.2 – Інтерфейс користувача «Софт менеджмент»

Переваги рішення SCOM:

– Консолідація інформації про працездатність, продуктивність і доступність різних компонентів і рівнів IT-інфраструктури, – від гіпервізорів до джерел безперебійного живлення.

– Узагальнене подання всіх відомостей з єдиної консолі керування.

– Підтримка гетерогенних середовищ.

1. Можливість інтеграції System Center Operations Manager із хмарною платформою Microsoft Azure, – контроль стану компонентів хмарної й локальної IT-сфер.

– Інтеграція з іншими рішеннями й службами Microsoft:

– продуктами сімейства System Center для автоматизації «приватної хмари»;

– каталогом Active Directory;

– SQL server;

– Exchange server.

Схема впровадження системи моніторингу IT-інфраструктури виглядає в такий спосіб:

1. Підготовка.

– Аудит IT-інфраструктури, складання технічних характеристик IT-системи замовника.

– Складання списку робіт із проекту.

– Розгортання System Center Operations Manager.

2. Налаштування.

– Збір статистики. Поширення «агентів» SCOM для збору мінімального набору вихідних даних.

– Підключення встаткування до системи SCOM.

– Налаштування граничних значень працездатності для всіх елементів моніторингу.

– Тестування системи.

– Навчання IT-фахівців замовника роботі із системою моніторингу.

3. Підтримка.

Для підтримки системи моніторингу в актуальному стані потрібно періодична доналаштуванна параметрів. Наприклад, при виході відновлення програмного забезпечення або з появою нового обладнання в компанії, потрібно правильним образом застосувати налаштування в системі моніторингу SCOM, перевірити правила збору даних.

«Софт менеджмент» пропонує своїм замовникам компетентну технічну допомогу на всіх етапах впровадження системи моніторингу й аудита IT-інфраструктури:

– розгортання системи на базі Microsoft System Center Operations Manager «під ключ»

– налаштування вже розгорнутого Operations Manager

– підтримка працездатності й супровід уже працюючої системи моніторингу.

Alloy Navigator

Поза залежністю від того, має компанія свій розвитий парк устаткування й програмного забезпечення або надає послуги по обслуговуванню чужий IT-інфраструктури, рано або пізно виникає необхідність у контролі й керуванні. Причому важливо правильно організувати керування не тільки на рівні робочих станцій, але й на рівні всієї мережі й підрозділів. Можна використовувати набір розрізнених інструментів, а можна вести весь облік у єдиному інтерфейсі. Останній підхід дозволяє комплексно оцінювати стан IT-активів, будувати взаємозв'язку, якісно й у строк обслуговувати вступники заявки й системно підходити до керуванню інфраструктурою. Це заощаджує час, сили й нерви.

Основним завданням продукту Alloy Navigator є забезпечення ефективності, прозорості й оперативності керування IT-інфраструктурою; це цілісне функціональне рішення керування активами, запитами користувачів, ліцензуванням і інше.

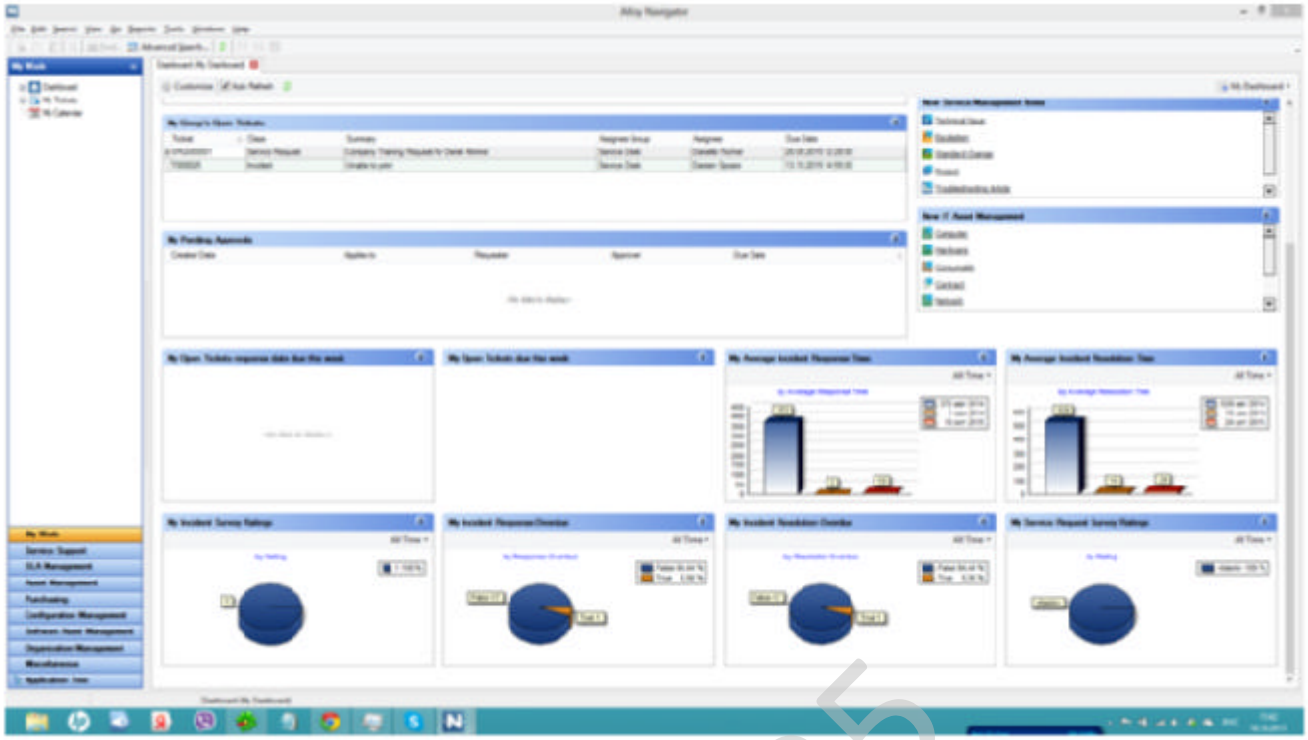

Рисунок 2.3 – Інтерфейс користувача Alloy Navigator

Часто стандартизація й своєрідна «кодифікація» правил у сфері системного адміністрування сприймається в багнети. Однак відмова від рекомендованих практик починає сильно позначатися на стані IT-інфраструктури в період інтенсивного зростання, коли інженери й і адміністратори, а також IT-менеджери починають зазнавати труднощів у зв'язку з тим, що парк устаткування й програмного забезпечення їхньої власної компанії розростається або з'являється трохи замовників з різним типом ведення бізнесу. У таких умовах кожний дріб'язок стає важливим елементом роботи й процесний підхід відмінно допомагає встежити за всім, нічого не випустити з уваги й не забути.

Розробляючи **Alloy Navigator**, споконвічно вирішили випливати рекомендаціям ITIL і створити продукт таким чином, щоб він сам занурював клієнта в налагоджену парадигму підходу ITSM. В Alloy Navigator 7.0 реалізовані основні модулі, які дозволять управляти IT-інфраструктурою компанії відповідно до принципів ITIL, але при цьому забезпечуючі максимальну гнучкість для налаштування продукту під потреби кожного конкретного користувача.

Технічна підтримка (Service Support). У цьому модулі збирається інформація з інцидентів – випадкам переривання або зниження якості IT-послуги. Важливо вчасно створювати інциденти з метою забезпечення мінімального впливу неполадок на бізнес-процес і максимально швидкого відновлення елемента IT-інфраструктури. Кожний запис містить докладну інформацію про виниклу проблему: тип, категорію, опис, пріоритет, строки виправлення, активності по інциденті, опис рішення, зв'язані об'єкти інфраструктури, історію взаємодій.

Користувач може створювати угруповання інцидентів по виконавцях, статусу, строкам усунення, черговості надходження заявки й т.д. Це необхідно для того, щоб установити порядок обробки інцидентів відповідно до їх терміновості й важливістю. Крім того, угруповання по типі інциденту й сервісу, що зачіпається, допомагають ідентифікувати проблеми, які можуть впливати на роботу безлічі користувачів або навіть на весь бізнес у цілому.

Ще одна важлива сутність даного розділу – проблема, причина, що лежить в основі одного або декількох інцидентів. Як правило, проблема встановлюється в ході роботи над усуненням інциденту.

Всі дані організовані у вигляді таблиць із можливістю гнучкої фільтрації по наборі параметрів, а це значить, що можна створювати будь-які угруповання й легко бачити вирішені завдання або тікети, що вимагають негайного рішення. Модуль технічної підтримки може використовуватися як для зовнішніх клієнтів у сервісних службах, так і для обслуговування внутрішніх заявок. Така організація технічної підтримки вкрай корисна у великих компаніях з більшим офісом або розподіленою мережею філій. Механізми Service Support у сполученні з KPI і планувальниками, убудованими в Alloy Navigator, здатні вирішити важливі управлінські завдання:

– спланувати завантаження співробітників технічної служби й інженерів;

– спланувати закупівлі встаткування, програмного забезпечення й видаткових матеріалів;

– визначити відповідальних;

– перерозподілити завдання залежно від складності й важливості між співробітниками відповідно до досвіду й кваліфікацією;

– автоматично розрахувати KPI (ключові показники діяльності), які можуть лягти в основу ухвалення рішення про преміювання або депреміювання співробітників.

Тікет створюється в прив'язці до будь-якого елемента IT-інфраструктури й у повній відповідності з рекомендаціями ITIL може бути створений з будь-якого розділу.

Тікет є однієї з базових сутностей Alloy Navigator і містить у собі всю історію взаємин і дій по запиті. Фактично, тікет забезпечує прописаний в ITSM принцип максимальної уваги до потреби кінцевого клієнта.

Модуль SLA (SLA Management). Угода про рівень надання послуги (Service Level Agreement (SLA)) – термін ITIL, що позначає формальний договір між замовником послуги і її постачальником, що містить опис послуги, права та обов'язки сторін і погоджений рівень якості надання даної послуги. Угода про рівень послуг описує IT-послугу, документує цільові показники рівня послуги, указує зони відповідальності сторін – постачальника IT-послуг і замовника. Одна угода про рівень послуг може поширюватися на безліч IT-послуг або безліч замовників. Простіше говорячи, угода визначає, хто, кому, коли і якої якості робить послуги. SLA регулює не тільки зовнішні й аутсорсерські, але й внутріфірмові відносини між підрозділами. В Alloy Navigator визначаються годинник доступності підтримки сервісу, рівень якості, час дії SLA, тип, категорія й статус. У цьому модулі фактично можна задавати правила реагування технічної служби на запити.

Модуль керування IT-активами компанії (Asset Management) містить у собі список матеріальних (устаткування) і нематеріальних (софт) активів з урахуванням дати їхнього введення в експлуатацію й вартості. Також у цьому модулі є список контрактів (договорів) по обслуговуванню, сервісу й гарантії.

Усередині картки контракту створюються зв'язки з конкретним устаткуванням/ПЗ, історією тікетів і подій за даним контрактом. У розділі бібліотеки (Library) створюються картки підлягаючому обліку встаткування й програмного забезпечення (активу), у яких відображається дата запуску, історія переміщень (наприклад, один монітор може належати за своє життя декільком співробітникам), тип, опис, зв'язані об'єкти інфраструктури. У цій же картці можна зарезервувати встаткування прямо в інтерфейсі календаря (наприклад, проектор на час презентації або ноутбук на час відрядження); всі резерви відображаються в окремому розділі.

У модулі активів також ураховуються локації (кімнати, зали, кабінети) і видаткові матеріали. Цей модуль значно спрощує систему керування IT-активами:

– завжди відомо, за ким і на який строк закріплене або зарезервоване встаткування;

– точно відомі строки впровадження й терміни служби встаткування, вартість устаткування;

– у кілька кліків можна звернутися до документації й гарантійних угод.

У розділі закупівель (purchasing) відображаються рахунки, список вендорів і постачальників, продуктовий каталог із вказівкою точного найменування, моделі й виробника встаткування.

Software Asset Management – розділ, створений для реалізації затребуваної концепції SAM, керування ліцензіями програмного забезпечення. Якщо ви маєте справу із програмним забезпеченням, то вам відомо, що ліцензії ПЗ мають кілька особливостей:

– Ліцензії бувають зайвими й реально не використовуються в діяльності компанії, у той час як їх обновляють і купують нові версії. Якщо компанія досить більша, системний адміністратор не встигає відслідковувати зміни в профілях користувачів і дороге ПЗ «повисає» до моменту обліку, тобто приблизно на рік. Таке положення справ приводить до додаткових нераціональних витрат.

– Іноді проблему оптимізації кількості ліцензій можна вирішити за допомогою покупки не іменних, конкурентних ліцензій (не на користувача, а на підключення). Але для цього необхідно знать, у який час і який образ співробітники використовують ПЗ.

– Морально застарілі ліцензії необхідно вчасно обновляти по запиті користувачів.

Модуль SAM вирішує ці проблеми. В основі модуля лежить каталог програмного забезпечення й три пов'язаних з ним роздягнула. Software Licences містить враховані ліцензії програмного забезпечення з урахуванням кількості установок, відповідності вимогам і відновлень.

У картці ліцензії враховуються загальні параметри, прописуються ключі й ідентифікатори, утримуються відомостях про апгрейдах і зв'язаний тікетах.

Tracked Software і Discovered Installations ураховують установлене програмне забезпечення, зберігають параметри його установки й відслідковують фактичне використання існуючих ліцензій.

Модуль Configuration Management (керування конфігураціями) містить трохи зв'язаних між собою розділів, які дають подання як про окремі елементи інфраструктури, так і про цілі вузли:

– Computers містить перелік робочих станцій із вказівкою операційної системи, категорії, власника, ім'я комп'ютера, дати аудита й інших параметрів. У цьому розділі зручно створювати самі різні угруповання на підставі технічних характеристик ПК: обсягу пам'яті, CPU і інше. Така можливість досягається за рахунки безлічі параметрів картки комп'ютера, по яких можна робити фільтрацію. Крім конфігурації, у кожній картці можна бачити все програмне забезпечення, установлене на комп'ютері, вартість устаткування, зв'язані тікети. Для роботи з кожною робочою станцією можна застосувати зовнішні інструменти: пропінгувати комп'ютер, скористатися Telnet і Remote Desktop.

– Hardware містить у собі залізо, що відповідає робочій станції або групі робочих станцій (наприклад, мережний принтер), а також портативне

встаткування (проектори, мобільні телефони та інше). У картках утримується інформація про встановлені програми, асоційованих об'єктах і тікетах. Прямо з картки можна здійснювати списання встаткування, указавши підставу.

– Networks включає опис мереж з пулом IP-Номерів, вказівкою власника, статусу активності, організації-холдера або локації.

– Documents містить будь-які регламентуючі документи й процедури, необхідні для керування конфігураціями.

– Configurations включає створені конфігурації баз даних, інтранету, підключень до Інтернету й інше.

– All Cls агрегує у собі інформацію з попередніх розділів для повного подання конфігурацій усередині IT-інфраструктури.

Модуль Organisation Management складається з декількох розділів, що включають організації (можна вносити підрозділу), локації (можна вносити міста, можна кімнати й поверхи), людей і робітники групи. У картку персони заносяться контакти, відомості про займану посаду, активність, зв'язані об'єкти інфраструктури, тікети, робочий календар, якщо мова йде про співробітника.

Таке рішення дозволяє не тільки вкрай прозоро контролювати IT-інфраструктуру у зв'язуванні з конкретним співробітником зовнішньої компанії або власної компанії, але й мати простий і швидкий доступ до відомостей про кожну персону. Це особливо важливо у випадку, якщо потрібно оперативно зв'язатися з відповідальною особою із зовнішньої організації. Цей модуль є важливою сполучною ланкою й завершує логікові програми як повністю відповідної ITIL.

Крім основних модулів, Alloy Navigator включає ще кілька важливих елементів, які не тільки необхідні логіці програми, але й вирішують самостійні завдання.

Звіти + KPI. В інтерфейсі системи можна сформувати звіти з будь-якою вкладеністю даних, створити свої кастомні подання й згенерувати звітність по показниках KPI за обраний період. Система ключових показників діяльності

KPI – найважливіший елемент методології ITIL, що, крім усього іншого, дозволяє проконтролювати результат роботи як усього підрозділу, так і кожного співробітника окремо. Подібний моніторинг показників дуже важливий саме для сервісних служб і технічної підтримки, тому що дозволяє оцінити рівень задоволеності зовнішнього/внутрішнього клієнта.

База знань організована досить стандартно для тих, хто звик до облікових програм: це своєрідний набір карток питань, що створюється за допомогою простого убудованого текстового редактора. У картці питання можна залишати коментарі, прикріплювати файли, зберігати посилання. Деякі компанії прийшли до внутрикорпоративних довідника в wiki-розмітці, однак рішення, убудоване в Alloy Navigator, відповідає загальній логіці програми й легко доступно для потреб операторів. До речі, додаткова цінність інтегрованої бази знань – швидка адаптація нових співробітників, які під час навчання можуть звертатися до накопичених статей. Доступ до бази даних може бути наданий зовнішнім користувачам – у такому випадку вони зможуть самостійно вирішувати найпоширеніші проблеми.

Робочий стіл програми може бути настроєний за бажанням співробітника. У ньому відображаються тікети по статусах, нова інформація про уведене встаткування, а також дашборди, що відображають гістограми, необхідні користувачеві для оперативної оцінки ситуації в його сфері впливу. Розділи модулів відкриваються в окремих вкладках, між якими можна перемикатися. Картки в кожному модулі відкриваються в окремих вікнах. Всі угруповання лівого сайдбара кастомізуємі й можуть бути створені так, як це максимально зручно користувачеві.

Основна програма не локалізована, всі розділи англомовні, усередині карток підтримується внесення даних російською мовою. Всі англомовні терміни зрозумілі користувачам, що володіє мінімальним технічним словником. Користувачам (клієнтам) доступний русифікований веб-портал самообслуговування, які скорочує число звернень до служби технічної підтримки

за рахунок можливості доступу до бази знань і можливості самостійного створення заявок (тікетів). Крім цього, існують мобільні версії для зручного й безперервного доступу до системи.

У продукті Alloy Navigator всі об'єкти взаємозалежні, до них можна звертатися з різних розділів і карток. Така архітектура вирішує кілька ключових завдань керування IT-інфраструктурою:

– Забезпечує комплексний, системний підхід до керування й контролю.

– Дозволяє оперативно одержати доступ до карток всіх об'єктів, пов'язаних з інцидентом або тікетом: персонам, устаткуванню, програмному забезпеченню, локації й т.д.

– Дозволяє поєднувати тікети в проекти і якщо буде потреба управляти всіма процесами по проектах.

– Відіграє важливу роль у ході інвентаризації, коли необхідно зібрати й проаналізувати інформацію в стислий термін.

На відміну від конкурентів, Alloy Navigator являє собою комплексне програмне забезпечення, що включає максимальний набір модулів для успішного керування IT-інфраструктурою. При розробці ми уникли спроб створити новомодний інтерфейс на шкоду функціональності продукту, і в нас вийшла структуроване рішення з високою швидкістю роботи й зручним розташуванням елементів. Ми взяли до уваги принципи ITIL і організували Alloy Navigator таким чином, щоб користувачам для ефективної роботи не довелося вивчати всю методологію. Нашою метою було надати ефективний інструмент керування й контролю інфраструктури. Користувач може настроїти поводження системи «під себе», у такий спосіб сполучаючи базові ідеї ITIL і вимоги реального життя. Досить установити **Alloy Navigator** і почати працювати. Порядок в IT-інфраструктурі й значній економії на зайвих активах не змусять себе чекати.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – це об’єктно-орієнтована мова програмування високого рівня загального призначення з відкритим кодом. Це визначення може бути важким для новачків, тому розглянемо кожну характеристику окремо, щоб зрозуміти, що вона означає:

– Відкритий вихідний код: це безкоштовно та доступно для подальших покращень, таких як додавання корисних функцій або виправлення помилок.

– Об’єктно-орієнтована: заснована не на функціях, але в об’єктах з певними атрибутами й методами.

– Високий рівень: зручний для людини, а не для комп’ютера.

– Загальне призначення: можна використовувати для створення будь-яких програм.

Ця мова використовується в будь-якому програмному забезпеченні, про яке ви тільки можете подумати. Ви можете використовувати його для створення веб-сайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу та багато іншого. Також застосовується в науці про дані, аналізі даних, машинному навчанні, інженерії даних, веб-розробці, розробці програмного забезпечення та інших галузях.

Переваги та недоліки Python

Переваги:

– Її легко читати, вчити та писати. Це мова програмування високого рівня з англійським синтаксисом. Це полегшує читання та розуміння коду. Її дійсно легко зрозуміти і вивчити, тому багато людей рекомендують Python новачкам. Вам потрібно менше рядків коду для виконання того ж завдання в порівнянні з іншими основними мовами, такими як C/C++ та Java.

– Підвищує продуктивність. Це дуже продуктивна мова. Завдяки її простоті розробники можуть зосередитися на розв’язанні проблеми. Їм не

потрібно витрачати багато часу на розуміння синтаксису або поведінку мови програмування. Ви пишете менше коду та виконуєте більше завдань.

– Інтерпретована мова. Python мова, що інтерпретується, а це означає, що вона безпосередньо виконує код по рядку. Якщо сталася помилка, вона зупиняє подальше виконання та повідомляє про її виникнення. Вона показує лише одну помилку, навіть якщо у програмі їх кілька. Це спрощує налагодження.

– Динамічно типізована. Python не визначає тип змінної, доки ми не запустимо код. Вона автоматично надає тип даних, коли відбувається процес виконання. Фахівець може не турбуватися про оголошення змінних та типи даних.

– Безкоштовна та з відкритим вихідним кодом. Ця мова постачається під схваленою OSI ліцензією з відкритим вихідним кодом. Це робить його безкоштовним для використання та розповсюдження. Ви можете завантажити вихідний код, змінити його та навіть розповсюджувати свою версію. Це корисно для організацій, які хочуть використати свою версію для розробки.

– Підтримка великих бібліотек. Стандартна бібліотека Python є величезною, ви можете знайти майже всі функції, необхідні для вашого завдання. Таким чином ви не залежите від зовнішніх бібліотек.

– Портативність .У багатьох мовах, таких як C/C++, потрібно змінити свій код, щоб запустити програму на різних платформах. З Python все інакше. Ви тільки пишете один раз і запускаєте її будь-де.

Недоліки:

– Низька швидкість. Вище ми обговорювали, що це інтерпретована мова з динамічною типізацією. Порядкове виконання коду часто призводить до повільного виконання. Динамічна природа Python також є причиною її низької швидкості, оскільки їй доводиться виконувати додаткову роботу при виконанні коду. Тому вона не підходить для цілей, де швидкість важливий аспект проєкту.

– Неефективна для пам’яті. Ця мова програмування використовує великий обсяг пам’яті, це може бути недоліком при створенні програм, коли віддають перевагу оптимізації пам’яті.

– Слабка у мобільних обчисленнях. Python зазвичай використовується у серверному програмуванні. Ми не бачимо – її на стороні клієнта або в мобільних програмах з таких причин: вона не заощаджує пам’ять і має повільну обчислювальну потужність у порівнянні з іншими мовами.

– Доступ до бази даних. Програмувати на цій мові легко, але коли ми взаємодіємо з базою даних, її не вистачає. Рівень доступу до бази даних у Python примітивний та недостатньо розвинений у порівнянні з іншими популярними технологіями.

– Помилки виконання. Це мова з динамічною типізацією, тому тип даних змінної може змінюватись у будь-який час. Змінна, що містить ціле число, у майбутньому може містити рядок, що може призвести до помилок виконання.

Застосування Python:

– Для аналізу даних. Дані стали цінним активом у будь-якій сучасній галузі, і більшість компаній зацікавлені у збиранні, обробці та аналізі релевантних даних, щоб витягти з них цінну інформацію для бізнесу. І тут Python виходить за межі будь-якої конкуренції. Python особливо цінна тим, що крім великої стандартної бібліотеки надає величезний набір додаткових модулів, розроблених спеціально для аналітичних цілей. Найвідоміші бібліотеки Python для аналізу даних – це pandas і NumPy . Ці інструменти дозволяють робити з вашими даними майже все, наприклад, очищати і аналізувати їх, вивчати статистику або візуалізувати приховані тенденції у ваших даних.

– Для візуалізації даних. Візуалізація даних – це окрема частина аналізу даних, яка допомагає нам подавати інформацію, необроблену чи очищену, у більш змістовній формі. Тут Python знову входить у гру, пропонуючи широкий спектр інструментів візуалізації даних. Найпопулярніші з них – matplotlib і

заснований на ній seaborn. Використовуючи їх, ми можемо створювати буквально всі види візуалізації: від найпростіших до складніших.

– Для машинного навчання. Машинне навчання (ML) є основою більшості завдань науки даних. Він є областю штучного інтелекту, пов'язаною з використанням алгоритмів, що дозволяють машинам вивчати закономірності та тенденції на основі історичних даних, щоб робити прогнози на основі невідомих даних. – Використовуючи методи ML, ми можемо створювати моделі, які можуть точно передбачити швидкість відтоку клієнтів компанії, оцінити ризик виникнення у людини певного захворювання, визначити оптимальне розташування автомобілів таксі й т.д. За допомогою Python ми можемо побудувати модель ML, використовуючи лише три рядки коду.

– Для розробки програмного забезпечення. Крім свого багатостороннього застосування в галузях науки про дані, Python використовується на кожному етапі розробки програмного забезпечення, включаючи контроль складання, автоматичну безперервну компіляцію, прототипування, відстеження помилок, тестування та обслуговування програмного забезпечення. За допомогою цієї мови можемо створювати аудіо- або відеопрограми на основі методів штучного інтелекту, машинного навчання, API (інтерфейсів прикладного програмування), GUI (графічних інтерфейсів) або будь-якого іншого типу програмного забезпечення.

– Для веброзробки. У той час як для створення візуальної частини вебсайту ми переважно будемо використовувати такі мови, як HTML, CSS та JavaScript, для його невидимої частини ми часто вибираємо Python. Серед масштабних вебсайтів та програм, створених за допомогою цієї мови, варто згадати Google, Facebook, Instagram, YouTube, Dropbox та Reddit.

– Для автоматизації задач/скриптингу. Це відмінний інструмент для написання програм для автоматизації різних завдань, що повторюються. Цей процес називається скриптингом. Зокрема, можна робити скрипти для роботи з файлами та папками. Наприклад, можна створювати, перейменовувати,

перетворювати, розділяти, об’єднувати або видаляти файли, перевіряти їх на наявність помилок. Ви також можете використовувати автоматизацію Python для пошуку та завантаження інформації з Інтернету, заповнення та надсилання онлайн-форм та надсилання регулярних повідомлень або електронних листів.

Яким фахівцям потрібно володіти Python:

– Фахівець з даних.

– Аналітик даних.

– Інженер даних.

– Інженер з машинного навчання.

– Журналіст даних.

– Архітектор даних.

– Повний стек веб-розробника.

– Backend-розробник.

– DevOps-інженер.

– Інженер-програміст.

Можемо зробити висновок, що Python ще довго буде популярною мовою, хоч і має низку недоліків. Цю мову використовують для створення вебсайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу, аналізу даних, машинного навчання, інженерії даних та для багатьох інших областей. Це перспективна і затребувана навичка, яка необхідна у всіх галузях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевого моніторингу та контролю стану ІТ.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Сформулюємо поради, які допоможуть вам вибрати, розгорнути та максимізувати цінність інструментів моніторингу мережі:

1. Пріоритет гібридної та багатохмарної сумісності: оскільки гібридні та багатохмарні середовища стають нормою, обирайте інструменти моніторингу, які пропонують безперешкодну інтеграцію з постачальниками публічних хмарних послуг (наприклад, AWS, Azure, Google Cloud) та інфраструктурою приватних хмар. Це забезпечує видимість на різних мережевих рівнях.

2. Впроваджуйте поетапний підхід до розгортання: уникайте розгортання інструментів моніторингу по всій мережі одночасно. Натомість розгортайте рішення поетапно, починаючи з критичної інфраструктури, щоб мінімізувати перебої та точно налаштувати конфігурації під час масштабування.

3. Інтеграція з платформами SIEM та SOAR: підключіть інструменти моніторингу до рішень SIEM або SOAR для централізації аналізу даних, покращення виявлення загроз та забезпечення автоматизованих робочих процесів реагування на інциденти. Така інтеграція допомагає створити єдину екосистему безпеки.

4. Використовуйте виявлення аномалій на основі штучного інтелекту: використовуйте інструменти, що включають штучний інтелект та машинне навчання, для виявлення незначних відхилень від нормальної поведінки мережі. Такий підхід зменшує залежність від статичних порогів та покращує виявлення загроз нульового дня або повільних атак.

5. Встановлення базового профілю продуктивності: Проведення комплексного базового дослідження показників продуктивності мережі (наприклад, затримки, пропускної здатності та пропускної здатності) під час

нормальної роботи. Це допоможе швидко виявити аномалії та оцінити майбутні покращення продуктивності.

Як вибрати правильний інструмент для моніторингу мережі

Ось деякі основні фактори, які слід враховувати під час оцінки рішень для моніторингу мережі.

Міркування щодо масштабованості

Зі зростанням організацій їхні мережі стають складнішими, що вимагає інструментів, здатних обробляти збільшений обсяг даних та складність мережі. Масштабоване рішення для моніторингу може враховувати додаткові пристрої, користувачів та робочі навантаження без шкоди для продуктивності чи точності.

Вибір інструменту з опціями масштабованості дозволяє організаціям адаптуватися до змінних вимог мережі. Інструменти, що пропонують механізми горизонтального та вертикального масштабування, забезпечують безперебійний моніторинг під час зростання мережі.

Можливості інтеграції

Сучасні IT-середовища часто включають різноманітні технології та системи. Інструмент, який добре інтегрується з іншими програмами та платформами, може забезпечити комплексне уявлення про стан та продуктивність мережі. Така інтеграція дозволяє автоматизувати робочі процеси та обмін даними.

Обираючи інструменти моніторингу з потужними функціями інтеграції, організації можуть спростити IT-операції та зменшити ручну роботу. Інтегровані системи забезпечують централізований моніторинг та управління, пропонуючи єдину платформу для всіх мережевих дій.

Інтерфейс користувача та зручність використання

Інтерфейс користувача (UI) інструменту моніторингу мережі суттєво впливає на його зручність використання та ефективність. Добре розроблений інтерфейс дозволяє IT-фахівцям легко орієнтуватися в інструменті, налаштовувати конфігурації та інтерпретувати дані. Простота використання гарантує, що команди можуть швидко реагувати на проблеми та приймати

обґрунтовані рішення на основі чіткої візуалізації продуктивності мережі.

Вибір інструменту з інтуїтивно зрозумілим інтерфейсом скорочує криву навчання та підвищує продуктивність. Зручні функції, такі як панелі інструментів з функцією перетягування елементів та автоматизована звітність, покращують впровадження та ефективність використання користувачами.

Моделі вартості та ліцензування

Організаціям необхідно враховувати початкові витрати, поточні платежі та потенційні приховані платежі. Моделі ліцензування різняться, включаючи варіанти на основі підписки, безстрокові або freemium, кожна з яких має свої власні витрати та переваги залежно від бюджету та потреб організації.

Оцінка загальної вартості володіння допомагає організаціям збалансувати бюджетні обмеження з вимогами до функціональності. Розуміння умов ліцензування та майбутніх витрат на масштабованість гарантує, що інвестиції задовольнять як поточні потреби, так і майбутнє зростання.

Інструменти моніторингу мережі є важливими для підтримки продуктивності, надійності та безпеки сучасних мереж. Вибираючи рішення, яке відповідає конкретним потребам організації, враховуючи такі фактори, як масштабованість, інтеграція, зручність використання та вартість, IT-команди можуть забезпечити оптимальну роботу мережі та проактивно вирішувати проблеми. Інвестування в правильний інструмент моніторингу не лише покращує стан мережі, але й підтримує безперервність бізнесу та операційну ефективність.

3.2 Розробка структурної схеми

Моніторинг мережі включає спостереження та аналіз продуктивності та стану мережі за допомогою різних пристроїв та програмних інструментів. Цей процес спрямований на забезпечення безперебійної роботи мережевої інфраструктури шляхом відстеження потоків даних, станів пристроїв та потенційних несправностей, які можуть порушити роботу сервісу.

Мережеві адміністратори часто використовують ці дані для керування пропускною здатністю, виявлення аномалій та забезпечення проактивного обслуговування, зменшуючи час простою та пом'якшуючи ризики, пов'язані з проблемами мережі.

Інструменти моніторингу мережі збирають дані за допомогою таких протоколів, як SNMP (простий протокол керування мережею) та ICMP (протокол керування інтернет-повідомленнями), що дозволяє адміністраторам оцінювати стан мережі в режимі реального часу. Ці інструменти часто надають графічні інтерфейси, які відображають такі показники, як втрата пакетів, затримка та час безвідмовної роботи, що спрощує розуміння стану мережі.

Важливість моніторингу мережі

Існує кілька причин, чому організації повинні впроваджувати стратегії моніторингу мережі.

Раннє виявлення проблем з мережею

Раннє виявлення мережевих проблем передбачає постійне сканування мережевої активності для виявлення порушень. Ці порушення можуть включати незвичайні обсяги трафіку, неочікувані простої або несправності обладнання. Мережеві адміністратори можуть швидко втрутитися, виявивши ці проблеми на ранній стадії та усунувши першопричину, перш ніж вони порушать роботу мереж. Це заощаджує час і ресурси, необхідні для тривалого усунення несправностей.

Раннє виявлення може запобігти порушенням безпеки, виявляючи потенційні загрози в міру їх виникнення. Наприклад, раптові сплески передачі даних можуть свідчити про спроби несанкціонованого доступу або витоку даних. Завдяки сповіщенням та звітам у режимі реального часу системи моніторингу мережі можуть повідомляти адміністраторів про ці аномалії, що дозволяє швидко реагувати та негайно зменшувати ризики безпеки.

Забезпечення продуктивності та доступності мережі

Відстежуючи ключові показники продуктивності, такі як використання пропускної здатності та затримка, мережеві адміністратори можуть забезпечити ефективне використання ресурсів та уникнути потенційних вузьких місць. Постійний моніторинг надає уявлення про стан мережі, що дозволяє своєчасно оновлювати або перерозподіляти ресурси для підтримки зв'язку в організації.

Крім того, моніторинг мережі підтримує високу доступність, оперативно сповіщаючи команди про збої або погіршення стану мережевих компонентів. Ці сповіщення дозволяють швидко діяти, мінімізуючи час простою та підтримуючи доступність послуг.

Моніторинг відповідності та безпеки

Відповідність вимогам та безпека є важливими питаннями, на які звертають увагу системи моніторингу мережі. Ці системи відстежують журнали доступу, дії користувачів та передачу даних, забезпечуючи відповідність використання мережі нормативним стандартам та політикам організації. Моніторинг може допомогти виявити прогалини у відповідності, що дозволяє компаніям оперативно вживати коригувальних заходів, щоб уникнути штрафів.

Моніторинг безпеки зосереджений на виявленні та реагуванні на потенційні загрози, такі як несанкціонований доступ та проникнення шкідливого програмного забезпечення. Моніторинг мережі в режимі реального часу виявляє відхилення від встановлених норм безпеки, запускаючи сповіщення для негайного реагування. Це посилює захист організації від кіберзагроз, захищаючи конфіденційні дані.

Ключові компоненти систем мережевого моніторингу

Методи збору даних

Збір даних включає збір інформації про мережевий трафік, стан пристроїв та показники продуктивності. Традиційні методи включають SNMP, який збирає та впорядковує дані про мережеві пристрої, та ICMP-зонди, які вимірюють час підключення та відгуку. Ці інструменти працюють разом, щоб створити

детальний огляд мережі, допомагаючи адміністраторам приймати обґрунтовані рішення щодо оптимізації продуктивності або усунення несправностей.

Методи збору даних також використовують технології на основі потоків, такі як NetFlow та sFlow, які пропонують детальну видимість моделей мережевого трафіку та використання пропускної здатності. Ці методи надають безцінну інформацію про продуктивність програм та поведінку користувачів, допомагаючи виявляти вузькі місця або несанкціоноване використання даних.

Топологія та відображення мережі

Топологія мережі та картографування є критично важливими компонентами мережевого моніторингу, що забезпечують візуальне уявлення про те, як пристрої та з'єднання організовані в мережі. Таке графічне зображення дозволяє мережевим адміністраторам краще зрозуміти, як трафік передається між пристроями, виявляти потенційні точки збою та оцінювати вплив перебоїв у роботі мережі.

Точне картографування топології допомагає ефективно виявляти несправності та оптимізувати мережеві шляхи. Інструменти картографування мережі автоматично виявляють та документують зміни в мережевому середовищі, підтримуючи актуальність топологічних представлень. У міру розвитку мереж з появою нових пристроїв та технологій динамічне картографування підтримує інтеграцію та прозорість.

Механізми оповіщення та звітності

Механізми сповіщень та звітності є незамінними для моніторингу мережі, надаючи сповіщення про аномалії або збої в режимі реального часу. Сповіщення налаштовуються на спрацьовування за певних порогових значень, таких як збільшення затримки або відключення пристроїв. Коли ці умови виконуються, сповіщення надсилаються адміністраторам мережі, що спонукає до негайного розслідування та вирішення проблеми.

Функції звітності доповнюють системи сповіщень, надаючи інформацію про довгострокові тенденції та показники ефективності. Регулярно генеровані

звіти допомагають виявити закономірності, які можуть свідчити про основні проблеми або можливості для оптимізації. Вони також підтримують дотримання вимог, документуючи мережеву активність та демонструючи дотримання нормативних стандартів.

Сформулюємо поради, які допоможуть вам оптимізувати стратегії моніторингу мережі для підвищення продуктивності та безпеки:

1. Використовуйте штучний інтелект та машинне навчання для прогнозної аналітики: використовуйте інструменти моніторингу на базі штучного інтелекту для аналізу історичних даних та прогнозування потенційних збоїв або вузьких місць. Такий підхід допомагає вирішувати проблеми до того, як вони вплинуть на продуктивність мережі.

2. Сегментація мереж для покращення видимості: розділіть мережу на логічні сегменти (наприклад, за відділами чи програмами), щоб зосередити зусилля моніторингу та швидше виявляти проблеми. Сегментація також підвищує безпеку, обмежуючи обсяг потенційних загроз.

3. Використовуйте моніторинг на основі потоку разом із традиційними метриками: інтегруйте такі інструменти, як NetFlow або sFlow, для аналізу потоків трафіку для глибшого розуміння використання пропускної здатності, продуктивності програм та аномальної поведінки. Це доповнює моніторинг на основі SNMP для отримання більш повного уявлення.

4. Впроваджуйте порогові значення для сповіщень на основі часу: встановлюйте динамічні порогові значення для показників продуктивності на основі тенденцій часу доби. Наприклад, налаштуйте вищі порогові значення пропускної здатності в години пікової зайнятості, щоб зменшити кількість хибних спрацьовувань та зосередитися на справді аномальній активності.

5. Поєднання локальних та хмарних інструментів моніторингу: використовуйте гібридні рішення для отримання видимості в традиційних та хмарних інфраструктурах. Інструменти, що інтегруються в різних середовищах, є важливими для моніторингу гібридних або багатохмарних мереж.

Метрики та протоколи моніторингу мережі

Загальні показники, що відстежуються

Ефективний моніторинг мережі залежить від відстеження показників, які показують стан, продуктивність та надійність мережі. Зазвичай моніторингові показники включають:

1. Використання пропускної здатності: Цей показник показує, яка частина доступної пропускної здатності мережі використовується в певний момент часу. Високий рівень використання може свідчити про перевантаження мережі, що вимагає перерозподілу ресурсів або оновлення.

2. Затримка: Затримка вимірює час, необхідний для передачі даних від джерела до місця призначення і назад. Висока затримка впливає на програми реального часу, такі як VoIP та відеоконференції, що вимагає своєчасного втручання для покращення взаємодії з користувачем.

3. Втрата пакетів: Втрата пакетів – це відсоток пакетів даних, які не досягають місця призначення. Навіть невелика кількість втрачених пакетів може порушити роботу програм, чутливих до доставки даних, таких як потокове передавання або онлайн-ігри.

4. Час безперебійної роботи та простої: Моніторинг часу безперебійної роботи пристроїв та послуг дає уявлення про надійність мережевих компонентів. Часті або тривалі простої можуть сигналізувати про несправне обладнання, неправильні конфігурації програмного забезпечення або ширші проблеми з інфраструктурою.

5. Коефіцієнт помилок: Цей показник відстежує кількість помилок у переданих даних, таких як колізії, втрачені пакети або повторні передачі. Високий коефіцієнт помилок часто вказує на такі проблеми, як збій обладнання або погане кабельне з’єднання.

6. Пропускна здатність: Пропускна здатність вимірює фактичну швидкість передачі даних по мережі. Розбіжності між пропускною здатністю та

використанням пропускної здатності можуть сигналізувати про проблеми з продуктивністю, такі як вузькі місця або перешкоди.

7. Джиттер: Джиттер стосується варіації часу доставки пакетів. Цей показник особливо важливий для програм реального часу, оскільки надмірний джиттер може призвести до погіршення якості голосового та відеозв'язку.

8. Використання процесора та пам'яті на пристроях: моніторинг використання ресурсів на мережевих пристроях, таких як маршрутизатори, комутатори та сервери, допомагає запобігти зниженню продуктивності через перевантажене обладнання.

9. Стан з’єднання: Регулярна перевірка стану з’єднань між пристроями забезпечує працездатність усіх компонентів. Швидке виявлення несправних з’єднань мінімізує перебої в обслуговуванні.

SNMP (Простий протокол керування мережею)

SNMP – це критично важливий протокол для моніторингу мережі, який дозволяє збирати та керувати мережевими даними на різних пристроях. Він працює шляхом запиту інформації до пристроїв, такої як показники продуктивності та сповіщення, що забезпечує централізоване управління мережею. Завдяки широкому розповсюдженню та сумісності з багатьма пристроями, SNMP допомагає в зусиллях з моніторингу.

Архітектура SNMP, що складається з агентів, менеджерів та баз управлінської інформації (MIB), формує структурований підхід до пошуку та управління даними. Агенти SNMP працюють на мережевих пристроях, звітуючи перед менеджерами SNMP, які обробляють та аналізують дані. MIB визначають структуру даних, забезпечуючи стандарти щодо того, яка інформація доступна та як до неї здійснюється доступ.

NetFlow та sFlow

NetFlow та sFlow – це технології, що використовуються для забезпечення видимості мережі та аналізу трафіку шляхом захоплення потоків пакетів. NetFlow, розроблений Cisco, збирає дані IP-трафіку та надає інформацію про

джерело, пункт призначення, обсяг та шляхи, що проходять мережею. Така видимість дозволяє проводити поглиблений аналіз трафіку, виявляти тенденції, моделі використання та аномалії.

sFlow – це технологія вибірки пакетів, яка забезпечує статистичне представлення даних, що проходять мережею. Вона ефективна для моніторингу високошвидкісних мереж, де захоплення всіх пакетів може бути неможливим. sFlow пропонує аналітику трафіку як другого, так і третього рівня, що робить її універсальною для моніторингу мережі.

ICMP (Протокол керування інтернет-повідомленнями)

ICMP допомагає в діагностиці та моніторингу мережі, надаючи зворотний зв'язок про проблеми, пов'язані з підключенням. Він в основному використовується для звітування про помилки, що дозволяє обмінюватися повідомленнями між пристроями, щоб вказати на проблеми з підключенням до мережі, такі як недоступні пункти призначення. Утиліти, такі як «ping» та «traceroute», покладаються на ICMP для перевірки доступності хоста та трасування мережевих шляхів.

Незважаючи на свою корисність, ICMP також може становити ризики для безпеки, якщо його використовувати для атак типу «відмова в обслуговуванні» або мережевої розвідки. Тому, хоча ICMP є невід'ємною частиною моніторингу продуктивності, його використання в мережах має бути ретельно керованим та захищеним.

Типи мереж та пристроїв, що контролюються

Маршрутизатори, комутатори та концентратори

Маршрутизатори, комутатори та концентратори – це основні мережеві пристрої, що забезпечують передачу даних. Маршрутизатори керують трафіком між різними мережами, що необхідно для підключення локальних мереж до Інтернету. Моніторинг маршрутизаторів забезпечує усунення потенційних вузьких місць та оптимізацію шляхів маршрутизації для ефективного потоку

трафіку. Це включає відстеження таких показників, як пропускна здатність, затримка та коефіцієнт помилок, для підтримки зв'язку та продуктивності.

Комутатори забезпечують зв'язок у мережі, спрямовуючи дані на певні пристрої, забезпечуючи ефективний розподіл даних. Моніторинг комутаторів допомагає визначити стан портів, використання пропускної здатності та рівень колізій, щоб запобігти зниженню продуктивності. Концентратори, хоча й простіші за функціями, діють як основні з'єднувачі в мережах. Їх моніторинг є важливим для виявлення потенційних несправностей, що впливають на сегменти мережі.

Брандмауери та пристрої безпеки

Пристрої мережевої безпеки, включаючи брандмауери, утворюють критично важливий захист від кіберзагроз та несанкціонованого доступу. Моніторинг цих пристроїв гарантує їх ефективне функціонування у забезпеченні дотримання політик та блокуванні шкідливого трафіку. Ключові показники, такі як спроби атак, порушення доступу та моделі трафіку, ретельно перевіряються для швидкого виявлення інцидентів безпеки та реагування на них.

Крім того, рішення для моніторингу забезпечують дотримання вимог, реєструючи спроби доступу та зміни конфігурації на пристроях безпеки. Такий рівень видимості допомагає проводити судово-медичний аналіз після порушення безпеки, швидко виявляючи скомпрометовані системи або порушення політик.

Сервери та віртуальні машини

Моніторинг серверів і віртуальних машин допомагає підтримувати безперервність та продуктивність обслуговування. На серверах розміщено програми та дані, життєво важливі для бізнес-функцій, що вимагає ретельного моніторингу використання процесора, споживання пам'яті та обсягу дискового вводу/виводу. Ці показники виявляють потенційне перевикористання або збої обладнання, що допомагає своєчасно вживати заходів з технічного обслуговування, щоб запобігти незапланованим простоям.

Віртуальні машини потребують особливого моніторингу через свою масштабованість та тимчасовість. Такі показники, як розподіл ресурсів, завантаження віртуального процесора та використання мережі, стають критично важливими для оптимізації віртуального середовища. Забезпечуючи ефективний моніторинг віртуальних активів, організації можуть динамічно адаптувати ресурси відповідно до потреб.

Хмарна інфраструктура та послуги

Завдяки своїй розподіленій та масштабованій інфраструктурі, хмарні сервіси потребують рішень для моніторингу, які забезпечують видимість розподілу ресурсів, доступності та продуктивності в кількох регіонах. Ключові показники, такі як час відгуку, час безвідмовної роботи сервісу та журнали доступу, є вирішальними для забезпечення надійної роботи та безпеки хмарного середовища.

Моніторинг хмарних сервісів також дозволяє проактивно керувати ресурсами, забезпечуючи масштабування віртуальних екземплярів під час пікових навантажень без погіршення продуктивності. Крім того, моніторинг підтримує управління витратами, виявляючи недостатньо використані ресурси або непотрібні витрати.

Дротові та бездротові мережі

Дротові мережі вимагають моніторингу таких компонентів, як комутатори Ethernet та кабелі, зосереджуючись на цілісності з'єднання та пропускній здатності для запобігання перебоям. Бездротові мережі пов'язані з унікальними проблемами, такими як перешкоди сигналу, перевантаження каналів та оцінка зони покриття. Моніторинг цих аспектів має вирішальне значення для підтримки продуктивності бездротового зв'язку.

Моніторинг бездротової мережі збирає дані про пристрої користувачів і точки доступу, допомагаючи виявляти проблеми з підключенням або спроби несанкціонованого доступу. Аналізуючи силу сигналу та швидкість передачі

даних, адміністратори можуть оптимізувати конфігурації бездротової мережі для покращення покриття та зручності використання.

Проблеми моніторингу мережі

Організації повинні знати про фактори, що ускладнюють моніторинг мережі.

Моніторинг у гібридних та багатохмарних середовищах

Гібридні та мультихмарні середовища вносять багаторівневу складність у моніторинг мережі, вимагаючи рішень, що відповідають різноманітним проблемам інфраструктури та інтеграції. Ці середовища охоплюють приватні та публічні хмарні екземпляри, а також локальні системи, що вимагає інструментів, здатних забезпечувати узгоджені дані про продуктивність усіх компонентів.

Динамічна природа хмарних середовищ означає, що рішення для моніторингу повинні адаптуватися до швидкого масштабування та змін, не порушуючи видимість. Це вимагає гнучких архітектур та функцій автоматизованого виявлення, щоб йти в ногу з розвитком інфраструктури.

Обробка великих обсягів даних

Величезний обсяг даних, що генеруються в сучасних мережах, може бути приголомшливим, що створює значні труднощі для систем моніторингу, які відповідають за обробку та аналіз цієї інформації. Ефективне управління та фільтрація величезних потоків даних є важливими для отримання корисної інформації без перевантаження системних ресурсів.

Забезпечення цілісності та точності даних має вирішальне значення для надійних результатів моніторингу. Неточні або неповні дані перешкоджають прийняттю рішень, що призводить до неправильних діагнозів або пропущених сповіщень.

Забезпечення безпеки мережі та відповідності вимогам

Ефективний моніторинг вимагає стратегій впровадження, які забезпечують дотримання політик безпеки та захищають дані під час передачі та зберігання. Розширене шифрування та засоби контролю доступу необхідні для

захисту процесів моніторингу та забезпечення дотримання таких норм, як GDPR та HIPAA.

Також важливо мати записи, які підтверджують дотримання стандартів безпеки та нормативних вимог, що підтримують процеси аудиту.

Практики для ефективного моніторингу мережі

Ось деякі способи, за допомогою яких організації можуть забезпечити ефективний моніторинг своїх мереж.

1. Визначте чіткі цілі моніторингу

Цілі можуть бути зосереджені на підтримці безперебійної роботи, своєчасному виявленні аномалій або оптимізації використання ресурсів. Встановлюючи точні цілі, організації можуть адаптувати свої стратегії моніторингу для отримання змістовної аналітики та підтримки прийняття стратегічних рішень.

Така чіткість також забезпечує ефективний розподіл ресурсів і допомагає встановити реалістичні показники та контрольні показники ефективності. Завдяки чітко визначеним цілям моніторингу команди можуть визначити пріоритети ключових видів діяльності та розробити цільові плани дій.

2. Регулярно оновлюйте мережеву документацію

Постійне оновлення мережевої документації гарантує точне відображення всіх змін в інфраструктурі, що сприяє ефективному моніторингу та втручанню. Документація повинна детально описувати топологію, конфігурації пристроїв та залежності, надаючи довідник адміністраторам, які керують мережею. Регулярні оновлення дозволяють точно відстежувати активи, зміни конфігурації та зростання мережі з часом.

Вичерпна документація допомагає у вирішенні проблем, швидко виявляючи уражені ділянки під час інцидентів. Вона також підтримує зусилля з дотримання вимог, підтверджуючи дотримання політик і процедур безпеки.

3. Впроваджуйте проактивне оповіщення та реагування на інциденти

Проактивне оповіщення та реагування на інциденти дозволяють швидко діяти, коли виникають проблеми з продуктивністю або загрози безпеці. Налаштування порогів оповіщень на основі тенденцій історичних даних дозволяє адміністраторам виявляти аномалії до того, як вони переростуть у серйозні проблеми. Ці оповіщення підтримують гнучке реагування на інциденти, надаючи практичну інформацію, яка спрямовує цілеспрямовані зусилля з усунення наслідків.

Протоколи реагування на інциденти доповнюють проактивне оповіщення, детально описуючи кроки для діагностики, ескалації та вирішення. Ці протоколи гарантують оперативне вирішення проблем, мінімізуючи час простою та вплив на операції.

4. Виконуйте планові оцінки та аудити мережі

Регулярні оцінки та аудити мережі надають уявлення про продуктивність мережі та стан безпеки. Ці оцінки визначають області для покращення, виявляючи вразливості або неефективність, які можуть перешкоджати роботі. Аудити систематично перевіряють конфігурації мережі, політики та процедури, забезпечуючи відповідність передовим практикам та нормативним вимогам.

Регулярні оцінювання також допомагають вимірювати успішність стратегій моніторингу, що дозволяє постійно вдосконалювати інструменти та процеси.

5. Навчіть персонал інструментам та процедурам моніторингу

Навчання персоналу використанню інструментів та процедур моніторингу мережі має вирішальне значення для максимального використання можливостей систем моніторингу. Добре навчені команди можуть точно інтерпретувати дані, розпізнавати аномалії та вживати обґрунтованих заходів для оперативного вирішення проблем. Регулярне навчання гарантує, що персонал завжди в курсі нових функцій та методологій моніторингу.

Навчання також заохочує спільну роботу між IT-командами, сприяючи спільному розумінню цілей та практик моніторингу. Це покращує комунікацію та координацію під час реагування на інциденти, сприяючи більш ефективним та результативним процесам вирішення проблем.

На рисунку 3.1 зображена структурна схема системи.

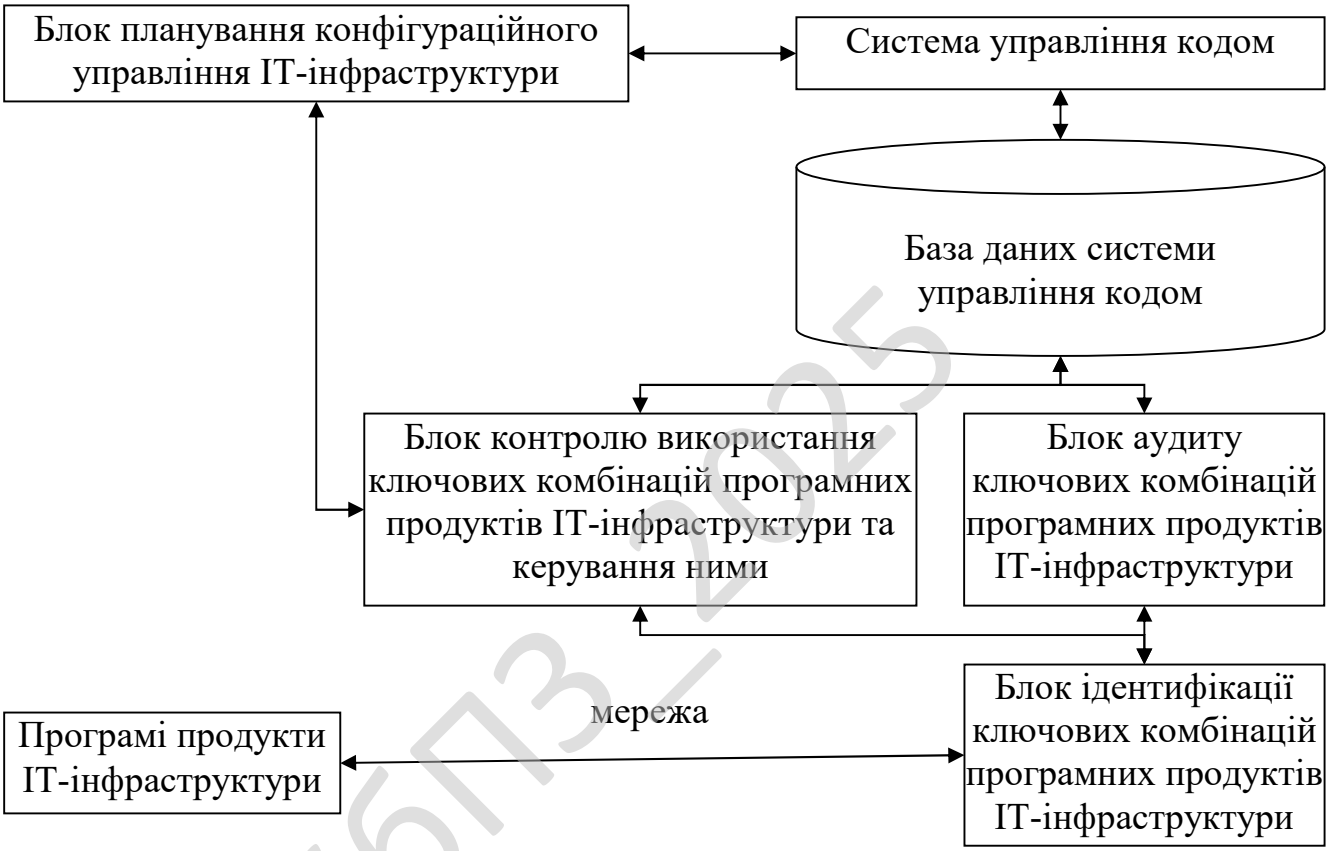

Рисунок 3.1 – Структурна схема системи

Зі структурної схеми видно, що система керування кодом підтримує програмні бібліотеки контролюючи доступ до елементів бібліотек, координує дії безлічі користувачів і допомагає в проведенні робочих процедур. Інші інструменти підтримують процес складання й випуску програмного забезпечення й документації на основі програмних елементів, що втримуються в бібліотеках. Інструменти для керування запитами на зміни програмного забезпечення використовуються для контрольованих системою конфігураційного керування

програмних елементів. Інші інструменти можуть забезпечувати керування базою даних і необхідними менеджменту звітними засобами, а також діяльністю по розробці й забезпеченню якості.

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Нижче розглянемо її більш докладно.

Функціональні можливості сервісу моніторингу й контролю стану IT

За допомогою сервісу моніторингу й контролю стану IT користувачі можуть забезпечити постійну доступність і високу продуктивність використовуваних додатків. Система «знає» про розповсюджені застосунки, сервіси, технології, протоколах і забезпечує інтелектуальний моніторинг важливих для вашого бізнесу комп'ютерних систем.

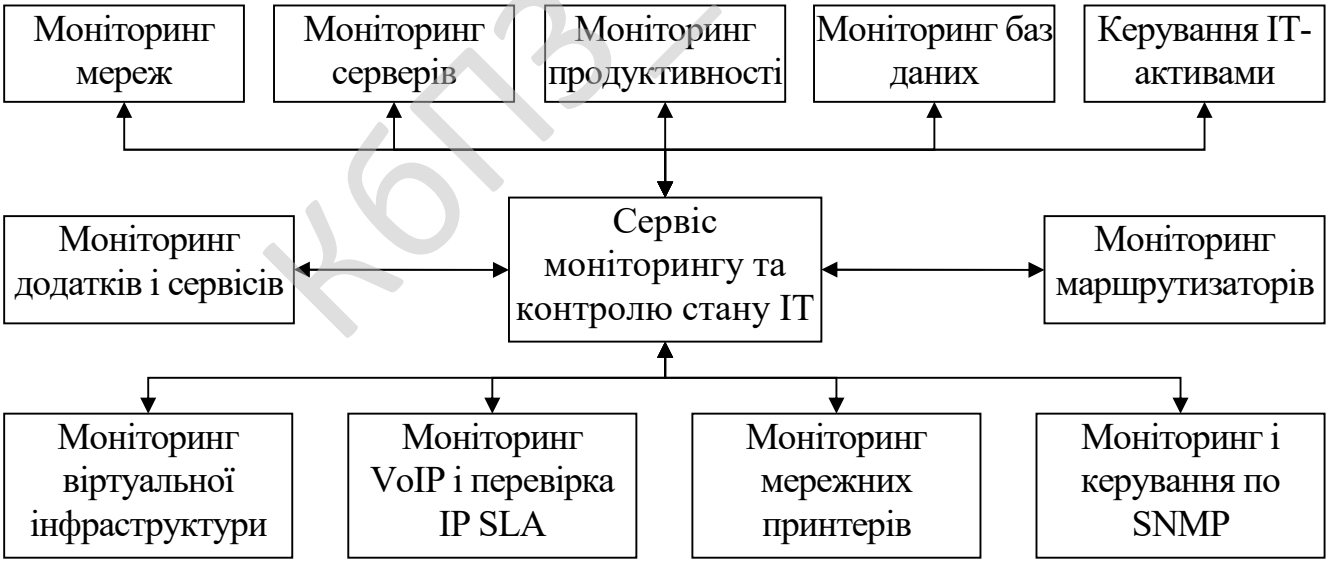

Рисунок 3.2 – Функціональна схема системи

Моніторинг мереж

Сервіс моніторингу й контролю стану IT виконує комплексне сканування мережі, опитуючи всі сервери, робочі станції, комутатори, маршрутизатори, принтери й т.д. На кожному мережному пристрої виявляються запущені мережні сервіси й застосунки, у тому числі нестандартні, працюючі на певних користувачем портах.

Моніторинг серверів

Сервіс моніторингу й контролю стану IT надає комплексне рішення для моніторингу ваших серверів незалежно від їхньої платформи й апаратної бази.

Моніторинг додатків і сервісів

За допомогою сервісу моніторингу й контролю стану IT ви зможете забезпечити постійну доступність і високу продуктивність використовуваних додатків. Система «знає» про розповсюджені застосунки, сервіси, технології, протоколах і забезпечує інтелектуальний моніторинг важливих для вашого бізнесу комп'ютерних систем.

Моніторинг маршрутизаторів

Використовуються передові технології, що забезпечують підтримку як широко розповсюджених мережних пристроїв від Cisco, 3Com, Alcatel, Nortel, Juniper і інших виробників, так і спеціалізованих рішень із використанням нестандартних MIB-описів.

Моніторинг продуктивності

Система збирає дані, необхідні для виявлення причин і запобігання збоїв, допомагаючи спланувати подальший розвиток інформаційної інфраструктури вашого бізнесу.

Моніторинг віртуальної інфраструктури

Використання сервісу моніторингу й контролю стану IT для моніторингу серверів VMware дозволить спростити й автоматизувати завдання контролю, оптимізації й планування вашої віртуальної інфраструктури.

Моніторинг VoIP і перевірка IP SLA

Підтримка технології Cisco IP Service Level Agreement, що контролює рівень якості обслуговування (QoS) в VoIP мережі. Вимір коефіцієнтів втрат пакетів,

затримок, перекручування звуку (jitter), часу проходження сигналу, а також обчислення усередненої оцінки якості (Mean Opinion Score).

Моніторинг мережних принтерів

Сервіс моніторингу й контролю стану IT дозволяє надати повну й детальну інформації про всі аспекти роботи друкувальних пристроїв у вашій мережі в найбільш зручній для аналізу формі.

Моніторинг баз даних

Сервіс моніторингу й контролю стану IT допомагає адміністраторам баз даних діагностувати й усувати збої в роботі баз даних, а також виявляти й виправляти проблеми із продуктивністю

Моніторинг і керування по SNMP

Сервіс моніторингу й контролю стану IT надає широкі можливості для моніторингу й керування SNMP-пристроями.

Керування IT-активами

Сервіс моніторингу й контролю стану IT спрощує завдання інвентаризації й супроводу об'єктів IT-інфраструктури, таких як маршрутизатори, сервери, робочі станції, принтери й інше встаткування.

Розглянемо перераховані вище функції більш докладно.

Моніторинг мереж

Сервіс моніторингу й контролю стану IT виконує комплексне сканування мережі, опитуючи всі сервери, робочі станції, комутатори, маршрутизатори, принтери й т.д. На кожному мережному пристрої виявляються запущені мережні сервіси й застосунки, у тому числі нестандартні, працюючі на певних користувачем портах.

Система не вимагає установки на пристроях додаткового апаратного й програмного забезпечення. Необхідні для автентифікації й авторизації реквізити доступу задаються в центральному репозиторії.

Масштабованість

Система підтримує роботу з мережами будь-якого масштабу – від невеликих офісних, до територіально-розподілених мереж великих підприємств, дата-центрів, міжнародних корпорацій і телекомунікаційних операторів.

При використанні в малих і середніх мережах система дозволяє контролювати продуктивність і доступність найбільш критичних мережних сервісів, здійснює моніторинг і аналіз трафіку й пропускної здатності мереж, спрощує планування подальшого розвитку.

При роботі з багаторівневими, територіально-розподіленими мережними структурами система здійснює контроль за віртуальною інфраструктурою, роботою бездротових пристроїв, VoIP-мережами, моніторинг віддалених інформаційних центрів і т.д.

Інструменти роботи із тривогами

Система моніторингу й керування мережею дозволяє при необхідності ініціювати тривогу як подією, так і станом мережних сервісів, при цьому кількість умов спрацьовування тривоги може бути необмеженим. Одержання тривожних оповіщень можна настроїти будь-яким зручним способом – від спливаючих вікон і звукових сигналів, до відправлення SMS і повідомлень на email. Обробка тривоги може бути виконана як з очікуванням коригувальних дій (у випадку їхньої відсутності може бути проведена ескалація), так і автоматично в інтерактивному або неінтерактивному режимі.

Обробка подій

Центр моніторингу мережі автоматично перетворить у події й зберігає в Журналі подій оповіщення, одержувані від мережних сервісів (повідомлення Syslog, пастки SNMP, системні події Windows і т.д.). Після перегляду в журналі подія можна підтвердити, призначити для нього тривогу та ін. Передбачено зручну фільтрацію й сортування подій у реальному часі й по історії.

Виняткова гнучкість

Система керування мережею сервісу моніторингу й контролю стану IT являє собою гнучку платформу, налаштовується легко під саму складну й багаторівневу інфраструктуру. Для кожного параметра, що відслідковується, можна окремо задати оптимальну конфігурацію, у тому числі інтервали опитування, налаштування зберігання історії змін, кешування й т.д.

Особливості моніторингу й аналізу мереж:

– Для проведення моніторингу не потрібна установка спеціальних агентів на мережні пристрої.

– При додаванні нового мережного пристрою інтервали опитування й параметри моніторингу для нього вибираються автоматично.

– Реалізовано тонке налаштування параметрів опитування й аналізу статистиків, кешуванні зібраних даних, які можуть використовуватися іншими компонентами системи.

– Для найбільш точного візуального відображення різних аспектів роботи додатків і пристроїв можна використовувати різні типи діаграм, у тому числі й динамічно обновлювані.

– Пристрою різних типів можна довільно поєднувати в групи й надалі виконувати з ними групові операції.

– Клієнтська частина програмного продукту дозволяє обробляти інформацію відразу від декількох віддалених серверів, забезпечуючи централізований моніторинг великих територіально-розподілених мереж з одного головного офісу.

Моніторинг серверів

Сервіс моніторингу й контролю стану IT надає комплексне рішення для моніторингу ваших серверів незалежно від їхньої платформи й апаратної бази. Моніторинг здійснюється з використанням SNMP, WMI, Telnet/SSH і інших стандартних технологій. Підтримуються наступні операційні системи:

– Windows;

– Linux/Unix;

– Mac OS;

– Solaris;

– AIX;

– HP-UX.

Моніторинг фізичної й віртуальної інфраструктури

Система не робить розходжень між фізичними й віртуальними серверами. Для гостьових операційних систем, що працюють під керуванням VMware ESX/ESXi, надається той же набір метрик, що й для їх «реальних» аналогів.

Оскільки серверні рішення VMware засновані на Linux, робота з ними здійснюється так само, як з «звичайними» серверами, і з тим же набором показників продуктивності. Разом з тим, моніторинг і керування віртуальною інфраструктурою на рівні віртуальних машин включає ряд спеціалізованих завдань.

Виявлення серверів

Процедура виявлення дозволяє знайти всі сервери у вашій мережі й визначити їхній тип. Мережні застосунки й сервіси можуть бути виявлені за допомогою сканування портів, що дозволяє знаходити сервери, що не відповідають на запити SNMP і ping.

Моніторинг стану й продуктивності серверів

За допомогою тривог, діаграм, звітів, засобів для аналізу поточного й історичних даних сервісу моніторингу й контролю стану IT забезпечує моніторинг усіх найбільш важливих показників стану сервера:

– Доступність.

– Завантаження процесора.

– Використання дискового простору.

– Мережний трафік і використання пропускної здатності.

– Запущені процеси й сервіси.

– Температура процесора/жорсткого диска/материнської плати.

– Швидкість і стан вентилятора.

– Будь-які інші метрики, доступні по SNMP.

Для найбільш важливих і критичних подій таких, як: Невдала авторизація, Вхід у систему суперкористувача, Критична подія в ядрі й т.д. у поставку включені передвстановлені тривоги.

На кожну тривогу можна призначити коригувальну дію, приміром, виконання скрипту або посилку команди Wake-on-LAN.

Інтегрований планувальник дозволяє призначити періодичне виконання завдань, наприклад, щоденне, щотижневе або щомісячне відправлення звітів на поштову адресу адміністратора або керівництва компанії.

Безагентний моніторинг

Сервіс моніторингу й контролю стану IT використовує безагентний моніторинг мережі, а значить вам не знадобиться встановлювати додаткове програмне або апаратне забезпечення на самі об'єкти моніторингу.

Моніторинг додатків і сервісів

Відомі застосунки й сервіси відслідковуються за допомогою спеціалізованих «розумних» засобів, що забезпечують моніторинг працездатності додатка, а не тільки його доступності.

Більшість спеціалізованих засобів моніторингу додатків і сервісів працюють подібним образом:

– З'єднання з додатком/сервісом по підтримуваному їм протоколу.
– Виконання процедури автентифікації/авторизації.
– Одержання стану й ключових метрик.
– Посилка заданого користувачем запиту.
– Збереження отриманої відповіді в ядрі системи для подальшого аналізу.

Повідомлення, отримані від різних додатків за допомогою журналу подій Windows або Syslog, зберігаються в базі даних. При одержанні цих повідомлень можуть спрацьовувати відповідні тривоги, приміром, Помилка роботи поштової системи, Вхід на FTP-сервер і т.п.

Моніторинг TCP/UDP портів

Працездатність невідомих додатків і сервісів, що підтримують TCP або UDP, може відслідковуватися в такий спосіб:

– Для перевірки доступності TCP додатка з ним установлюється з'єднання.

– Застосунки посилають задані користувачем дані.

– Отримана відповідь передається в ядро для зберігання й подальшого аналізу.

– Збирається статистика за часом відгуку від додатка.

Моніторинг баз даних

Сервіс моніторингу й контролю стану ІТ здійснює моніторинг баз даних за допомогою JDBC/ODBC. Підтримуються практично всі сучасні промислові бази даних, включаючи:

– Oracle;

– Microsoft SQL Server;

– MySQL;

– PostreSQL;

– Firebird.

Система підтримує виконання довільних динамічно створених SQL-запитів, включаючи insert/update/delete. Отримані результати конвертуються у формат сервісу моніторингу й контролю стану ІТ для подальшого аналізу.

Моніторинг локальної файлової системи

Моніторинг файлової системи містить у собі періодичне виконання наступних операцій:

– Перевірка існування файлів і папок.

– Перевірка розміру файлу, часу модифікації і його контрольної суми.

– Перевірка кількості файлів у папці і їхньому загальному розмірі.

– Одержання вмісту файлу для аналізу й редагування.

– Перевірка вмісту папки.

Користувач може створити тривоги, що відслідковують одержання несподіваних результатів при моніторингу файлової системи.

Моніторинг додатків і сервісів

За допомогою сервісу моніторингу й контролю стану IT ви зможете забезпечити постійну доступність і високу продуктивність використовуваних додатків. Система «знає» про розповсюджені застосунки, сервіси, технології, протоколах і забезпечує інтелектуальний моніторинг важливих для вашого бізнесу комп'ютерних систем.

Крім моніторингу мережних додатків, за допомогою SNMP забезпечується збір інформації про процеси, що працюють на віддалених машинах. Таким чином, можна, наприклад, використовувати тривоги, діаграми, звіти для спостереження за:

– кількістю екземплярів процесу;

– навантаженням на процесор, створюваної окремим потоком виконання;

– використовуваним певним процесом обсягом пам'яті.

Сервіс моніторингу й контролю стану IT дозволяє настроїти моніторинг IT-сервісів відразу для декількох комп'ютерів, забезпечуючи можливість експортувати/імпортувати ці налаштування.

Панель статусу сервісів

Панель статусу сервісів дає можливість максимально простим способом побачити загальний стан вашої IT-інфраструктури. Панель являє собою матрицю, де за допомогою колірного кодування відбивається стан всіх сервісів на всіх мережних пристроях, що відслідковуються. Ця панель може використовуватися як вхідна крапка для пошуку джерел різноманітних проблем.

Оповіщення про збої в роботі додатків

Сервіс моніторингу й контролю стану IT містить у собі готові тривоги для типових проблем таких, як Занадто велика кількість запитів до веб-сервера Apache або Недостача місця на FTP-сервері.

Виявлення додатків і сервісів

У результаті мережного виявлення система знаходить як відомі їй, так і непізнані («узагальнені») сервіси, останні – шляхом сканування TCP/ UDP-портів. Моніторинг для знайдених активних сервісів активується за замовчуванням при

створенні облікового запису пристрою. При цьому для кожного активованого сервісу автоматично вибираються оптимальні налаштування моніторингу.

Збір повідомлень і повідомлень про помилки

Система віддалено збирає повідомлення додатків і повідомлення про помилки, використовуючи для цього Syslog і журнал подій Windows. Отримані повідомлення зберігаються в центральній базі даних на сервері, забезпечуючи можливість проведення довгострокового аудита.

Отримані повідомлення можуть транслюватися далі за допомогою повідомлень Syslog або пасток SNMP. На будь-яке повідомлення можна призначити тривогу, що може відправляти повідомлення про цю подію по електронній пошті й SMS адміністраторові або виконувати автоматичні дії (перезавантаження сервера, віддалена виконання скрипту й т.д.).

Моніторинг веб-серверів і сайтів

Навіть невеликі на перший погляд проблеми на веб-сайті можуть дуже швидко розростатися й приводити до істотних збоїв у роботі, які у свою чергу можуть позначитися навіть на ефективності всього бізнесу в цілому. Щоб це запобігти, необхідно забезпечити цілодобове спостереження за роботою вашого веб-сайту, що й забезпечує сервісу моніторингу й контролю стану IT .

Моніторинг веб-серверів, у тому числі Apache і IIS, містить у собі:

– Перевірку доступності сервера.

– Виконання процедури авторизації, якщо потрібно.

– Звертання по заданих адресах через HTTP, одержання й аналіз відповіді.

– Передачу вмісту веб-сторінок у ядро системи для більше детального аналізу (приміром, пошуку ключових слів).

– Вимір часу відгуку.

Крім того, система забезпечує спостереження за станом сервера за допомогою відповідних тривог (таких, як «Надлишковий трафік») і діаграм (приміром, «Кількість активних процесів Apache»).

Моніторинг поштових серверів

У сучасних умовах бізнес дуже сильно залежить від роботи корпоративного поштового сервера. сервісу моніторингу й контролю стану IT дозволяє запобігати серйозним збоям у роботі поштової системи за рахунок:

– Перевірки доступності вхідних повідомлень за допомогою моніторингу папок POP3/IMAP.

– Контролю працездатності сервера вихідних повідомлень через SMTP-авторизацію.

– Наскрізної перевірки поштової системи шляхом посилки й прийому тестових поштових повідомлень.

Інші сервіси

Поставка сервісу моніторингу й контролю стану IT містить у собі цілий ряд блоків «інтелектуального» спостереження за різними сервісами:

– FTP-серверами: віддалена перевірка файлів і папок.

– SSH-серверами: авторизація, віддалене виконання скриптів, контроль вихідних даних.

– DNS-серверами: перевірка наявності правильної інформації в DNS-зоні.

– DHCP-серверами: перевірка працездатності шляхом лізингу IP-адрес.

– LDAP-серверами: авторизація, виконання пошукових запитів і аналіз отриманих результатів.

– Radius-серверами: виконання процедури автентифікації.

Моніторинг баз даних

Сервіс моніторингу й контролю стану IT виконує моніторинг баз даних за допомогою JDBC/ODBC. Підтримуються такі сучасні бази даних, як Oracle, Microsoft SQL Server, MySQL, PostreSQL, Firebird і ін.

Система перевіряє доступність сервера, виконує задані користувачем запити й оцінює відповідність отриманих результатів заданим критеріям (кількості полів і записів, значенням у певних полях і т.п.).

Узагальнені моніторинг TCP/ UDP-портів

Контроль працездатності інших мережних додатків і сервісів (працюючих як по TCP, так і по UDP) виконується в такий спосіб:

– Для працюючі по TCP сервісу встановлюється з'єднання й перевіряється його доступність.

– На заданий порт посилають специфіковані користувачем вхідні дані.

– Приймається відповідь і передається в ядро для наступного аналізу.

– Виміряється й зберігається час відгуку.

Моніторинг маршрутизаторів

Використовуються передові технології, що забезпечують підтримку як широко розповсюджених мережних пристроїв від Cisco, 3Com, Alcatel, Nortel, Juniper і інших виробників, так і спеціалізованих рішень із використанням нестандартних MIB-описів.

Моніторинг трафіку й пропускної здатності

Система в реальному часі збирає інформацію про трафік й використання пропускної здатності з окремих портів мережного встаткування. Ці дані зберігаються в базі даних для подальшого використання при побудові графіків і звітів.

Сервіс моніторингу й контролю стану IT оптимізований для швидкого доступу до даних, одержуваним від тисяч мережних інтерфейсів протягом тривалого часів, забезпечуючи побудову усереднених діаграм по трафіку/пропускної здатності в масштабі годин, днів, тижнів, місяців або років.

На відміну від аналогів, архітектура сервісу моніторингу й контролю стану IT забезпечує можливість створення діаграм, що налаштовуються повністю користувачем, і звітів. Приміром, можна об'єднати в рамках однієї діаграми інформацію про трафік, отриманим з різних портів і навіть пристроїв, додати ковзний середній або лінійний тренди, щоб спланувати розвиток мережі.

Побудова звітів про роботу мережі за розкладом

Задавши відповідний розклад, користувач може автоматизувати регулярну побудову й пересилання по електронній пошті звітів про трафік й використання

пропускної здатності. Звіти можуть відсилатися у форматах PDF, HTML, RFT, Excel і ін.

Оповіщення про високе завантаження мережі

У систему включений набір тривог, що спрацьовують у випадку перевищення заданого порога використання пропускної здатності мережі. Оповіщення про тривогу можуть бути доставлені через електронну пошту, SMS і іншими методами.

Докладний аналіз мережного трафіку

Сервіс моніторингу й контролю стану IT підтримує збір і обробку даних про мережний трафік з використанням NetFlow, sFlow і IPFIX.

Моніторинг статусу мережних інтерфейсів

Всі керовані комутатори й маршрутизатори надають інформацію про стан своїх портів/інтерфейсів у реальному часі по протоколі SNMP. сервісу моніторингу й контролю стану IT збирає ці дані, надаючи їхньому користувачеві у вигляді звітів про мережу в цілому або по окремих пристроях.

Коли один з мережних інтерфейсів з якої-небудь причини відключається, спрацьовує одна з наступних тривог:

– Відключення (в основному відбувається при мережних збоях).

– Адміністративне відключення (як результат дій користувача).

Метрики продуктивності

За замовчуванням збирається вся інформація про стан і продуктивність, включаючи доступність, час відгуку, завантаження процесора, використання пам'яті, швидкість вентилятора й т.д. Для аналізу цих даних можуть бути використані різні інструменти:

– Тривоги (Відключення інтерфейсу, Зміна конфігурації маршрутизатора, Втрата зв'язку із сусідом по EGP і т.д.).

– Звіти (наприклад, Перших 10 інтерфейсів по трафіку, Використання пам'яті більше 90%).

– Діаграми (Розподіл мережних інтерфейсів по типах, Перші 10 за часом відгуку й ін.).

Крім того, сервісу моніторингу й контролю стану IT надає унікальну функціональність по створенню й налаштуванню тривог, запитів, звітів і діаграм за довільними показниками продуктивності (приміром, сила сигналу WiMAX).

Виявлення маршрутизаторів і відображення їх на карті

Процедура мережного виявлення забезпечує пошук всіх маршрутизаторів і комутаторів у скануємої мережі, додавання їх у систему й налаштування параметрів моніторингу для всіх мережних інтерфейсів/портів.

Виявлені маршрутизатори можуть бути додані на динамічну карту мережі. При цьому для кожного пристрою на карті будуть відображатися найбільш важливі метрики, що характеризують його поточний стан.

Інформація, що налаштовується, по IT-активах

Сервіс моніторингу й контролю стану IT надає гнучке рішення по супроводу IT-активів. З кожним маршрутизатором, комутатором або іншим об'єктом мережної інфраструктури може бути асоційована не тільки визначена супровідна інформація (серійний номер, модель, місце розташування й т.п.), але й будь-які інші користувальницькі дані в довільному форматі.

Підтримка встаткування Cisco

Мережні пристрої Cisco надають більше точну й детальну інформацію про свою роботу (включаючи завантаження процесора, швидкість обертання вентиляторів і т.п.) через SNMP. Ця інформація доступна й використовується убудованими засобами обробки даних (тривогами, звітами, діаграмами та ін.).

Наприклад, у поставку входять наступні « Cisco-орієнтовані» тривоги:

– Попередження про роботу вентилятора в пристрої Cisco.

– Вимикання пристрою Cisco.

– Попередження про температуру в пристрої Cisco.

– Попередження про навантаження в пристрої Cisco.

– Попередження про резервне живлення в пристрої Cisco.

Моніторинг продуктивності

Система збирає дані, необхідні для виявлення причин і запобігання збоїв, допомагаючи спланувати подальший розвиток інформаційної інфраструктури вашого бізнесу.

Моніторинг продуктивності здійснюється по наступних ключових показниках:

– фактична пропускна здатність комутаторів і маршрутизаторів;

– завантаженість пам'яті й процесорів мережних пристроїв;

– періоди безперервної роботи серверів;

– час відгуку сервісів і додатків;

– якість мережних з'єднань (втрати, затримки пакетів і т.д.);

– використання існуючого простору для зберігання даних на серверах, дискових масивах і інших накопичувачах;

– метрики, задані користувачами (наприклад, рівень Wi-Fi сигналу).

Всі отримані показники продуктивності зберігаються й доступні для подальшого аналізу. Для кожного з показників передбачені відповідні аналітичні інструменти: діаграми, тривоги, звіти.

Моніторинг використання процесорів

Сервіс моніторингу й контролю стану IT проводить моніторинг продуктивності процесорів у серверів, керованих комутаторів, маршрутизаторів і іншого встаткування мережі, що по протоколі SNMP надає дані про завантаження процесора. Інформацію про фактичне використання ресурсів можна одержати окремо по кожному процесорі, а при необхідності й по кожному процесорному ядру.

У системі передбачена можливість спрацьовування тривоги у випадку, якщо на одному з мережних пристроїв завантаження процесора перевищило граничне значення в заданий користувачем період часу. При цьому налаштування процедур оповіщення, тривог і ініціації коригувальних дій можна конфігурувати для кожного пристрою окремо або задавати відразу для групи. Можливий моніторинг завантаження процесора для запущених на віддалених пристроях окремих процесів.

Контроль дискового простору й завантаження оперативної пам'яті

Система здійснює моніторинг дискового простору віддалених серверів і інших мережних пристроїв по протоколі SNMP. Мітки й дані по вільному/використаному простору надходять по всіх файлових системах, дискам і розділам; ці дані можуть бути представлені в наочній графічній формі. При цьому самі графіки можна налаштовувати під конкретні завдання. Також їсти можливість доповнити дані по аналізі дискового простору трендами лінійної регресії, що дозволить спрогнозувати момент, коли на носії закінчиться вільне місце.

Використання пам'яті відслідковується й для процесів, запущених на віддалених серверах і робочих станціях.

Контроль використання пропускної здатності

У системі передбачена можливість оповіщення адміністратора у випадках, коли на якому-небудь із портів комутатора/маршрутизатора обсяг трафіку наближається до пропускної здатності або межі, заданому адміністратором. Скориставшись спеціальними сервісами аналізу (наприклад, NetFlow), можна виявити джерела підвищеного мережного навантаження (вузли, застосунки й т.д.).

Моніторинг часу відгуку

Продуктивність мережного додатка може знижуватися через цілий ряд причин: недоліку пам'яті, повільного мережного з'єднання, підвищеної завантаження процесора, внутрішніх проблем програми й т.д. Досить точно відбиває загальний стан додатка такий параметр, як час відгуку – інтервал часу між відправленням спеціально згенерованого запиту й моментом одержання відповіді на нього.

Наприклад, для різних додатків часом відгуку є період:

– виконання SQL-запиту;

– завантаження веб-сторінки;

– завантаження файлу з віддаленого FTP-сервера;

– виконання скрипту на віддаленому пристрої.

При цьому система здійснює моніторинг часу відгуку контрольованих вузлів за допомогою ICMP-запитів echo (ping) і аналізує відсоток загублених пакетів. Такий

підхід прискорює й спрощує виявлення проблем, пов'язаних із продуктивністю мережі.

Користувальницькі показники продуктивності

Система здатна аналізувати будь-які метрики продуктивності, інформація для розрахунку яких доступна по протоколах SNMP, CLI, WMI, BACnet, Modbus, OPC і т.д.

Показники, які можна включити в моніторинг продуктивності:

– рівень сигналу бездротової мережі (SNMP);

– кількість потоків виконання на сервері додатка (JMX);

– розмір файлу підкачування Windows (WMI).

Панель «Рейтинг продуктивності: Топ 10»

Для спрощення роботи мережного адміністратора в системі існує спеціальна панель «Рейтинг продуктивності: Топ 10». Можливості цієї панелі допомагають звільнити адміністратора від рутинних операцій перевірки різних додатків і ресурсів, відстеження даних по завантажених і проблемних компонентах.

Оповіщення про зниження продуктивності

Підсистема тривог сервісу моніторингу й контролю стану IT дозволяє оперативно виявляти падіння продуктивності в різних ситуаціях, у тому числі самих складних.

Наприклад, активація тривоги виконується:

– Якщо протягом заданого інтервалу часу виникли відразу кілька подій типу «перевантаження» (активується тривога DDOS-атака).

– Якщо за певний часовий проміжок (приміром, більше 5 хвилин) завантаження процесора перевищує 80%. Така тривога може бути автоматично деактивирована, якщо використання процесора падає нижче 30% і зберігається на такому рівні не менш години.

– Якщо продуктивність частини серверів (більше заданого значення) у кластері не відповідає встановленим для них критеріям, або сервери недоступні.

Крім призначення тривоги для кожної події можна задати автоматичні коригувальні дії або зажадати підтвердження від оператора. Наприклад, система здатна самостійно провести перезапуск проблемного сервісу або сервера в цілому.

Моніторинг віртуальної інфраструктури

Використання сервісу моніторингу й контролю стану IT для моніторингу серверів VMware дозволить спростити й автоматизувати завдання контролю, оптимізації й планування вашої віртуальної інфраструктури.

Сервіс моніторингу й контролю стану IT підтримує моніторинг доступності й продуктивності на рівні:

– ESX-серверів;

– віртуальних машин;

– гостьових операційних систем.

Для моніторингу ESX-серверів, по суті що є Linux-машинами, а також гостьових операційних систем можуть використовуватися стандартні засоби з інструментарію AggreGate. Для моніторингу віртуальних машин, їхнього стану, використовуваних ресурсів розроблені спеціальні тривоги, графіки, звіти й віджети.

Моніторинг стану віртуальних машин

Сервіс моніторингу й контролю стану IT виявляє ESX-сервера у вашій мережі, одержує список і характеристики існуючих віртуальних машин, визначає оптимальні параметри для їхнього моніторингу. Для кожної віртуальної машини автоматично створюється набір тривог, що попереджають адміністратора про пов'язаних з нею подіях, таких, як зупинка або запуск.

Загальну інформацію про віртуальні машини можна одержати за допомогою віджета «Інформація про VMware» і звіт «Зведення по VMware». Сюди включаються:

– ідентифікатор віртуальної машини;

– поточний статус віртуальної машини;

– гостьова операційна система;

– стан операційної системи.

Моніторинг продуктивності віртуальних машин

Сервіс моніторингу й контролю стану IT дозволяє відслідковувати використання ресурсів віртуальними машинами як в абсолютних одиницях, так і у відсотках від їхнього доступного обсягу. Залежно від типу ресурсу обоє або один із цих способів використовується для моніторингу:

– навантаження на процесор;

– використання пам'яті;

– читання й записи на диск;

– вхідного/вихідного мережного трафіку.

Моніторинг VoIP і перевірка IP SLA

Підтримка технології Cisco IP Service Level Agreement, що контролює рівень якості обслуговування (QoS) в VoIP мережі. Вимір коефіцієнтів втрат пакетів, затримок, перекручування звуку (jitter), часу проходження сигналу, а також обчислення усередненої оцінки якості (Mean Opinion Score).

Моніторинг мережних принтерів

Сервіс моніторингу й контролю стану IT дозволяє надати повну й детальну інформації про всі аспекти роботи друкувальних пристроїв у вашій мережі в найбільш зручній для аналізу формі. Як часто вам доводиться зіштовхуватися із ситуацією, коли проблема із принтером стопорить всю роботу? Тонер завжди закінчується раптово й дуже недоречно; важливий документ звичайно виявляється десь наприкінці нескінченної черги, що утворилася через непомічений «зажовування» папери... Список можна продовжувати дуже довго. Але більшість таких проблем нескладно запобігти за допомогою централізованого моніторингу друкуючих пристроїв, сервісу моніторингу й контролю стану IT дозволяє зробити це, відслідковуючи статус принтерів у реальному часі й надаючи оповіщення, що налаштовуються, про проблеми.

Централізований моніторинг конфігурації й стану принтерів

Сучасні принтери можуть багато чого повідомити про себе за допомогою SNMP. сервісу моніторингу й контролю стану IT відслідковує всю отриману в такий

спосіб інформацію, консолідуючи її з даними з інших джерел. Це дозволяє надати повну й детальну інформації про всі аспекти роботи друкувальних пристроїв у вашій мережі в найбільш зручній для аналізу формі.

Приміром, поточний статус принтера описується трьома показниками:

– статус принтера як мережного пристрою;

– поточний статус друку;

– виявлені на принтері помилки.

Але в більшості випадків набагато зручніше замінити їхньою однією характеристикою, що представляє готовність принтера до роботи. Такий узагальнений стан принтера може приймати значення «Готовий до роботи», «Іде друк», «Очікування», «Розігрів»,«Зам'яття паперу», «Відкрита кришка» і т.д. сервісу моніторингу й контролю стану ІТ дозволяє користувачеві задати, яким образом показники статусу принтера відображаються в його узагальнений стан. Це забезпечує можливість гнучкого налаштування моніторингу для різних типів друкувальних пристроїв.

Оповіщення про проблеми друку

Сервіс моніторингу й контролю стану ІТ включає набір тривог для оповіщення адміністратора про важливі події друку, таких як:

– Недолік ресурсів: спрацьовує, коли відсутня папір, залишається мало тонера й т.п.

– Відкрито кришку: попереджає про те, що кришка принтера відкрита занадто довго.

– Критична подія: сповіщає адміністратора про те, що друк зупинена й не може бути продовжена.

Моніторинг баз даних

Сервіс моніторингу й контролю стану ІТ допомагає адміністраторам баз даних діагностувати й усувати збої в роботі баз даних, а також виявляти й виправляти проблеми із продуктивністю. Система використовує драйвер JDBC/ODBC, що забезпечує підключення до всіх популярних типів баз даних, включаючи Oracle, MySQL, Microsoft SQL Server, Firebird, Sybase, IBM DB2 і ін.

Аналіз результатів SQL-запитів

Моніторинг здійснюється посилкою заданих користувачем SQL-запитів. Отримані результати конвертуються у формат сервісу моніторингу й контролю стану IT і зберігаються в його власній базі для подальшого аналізу. Запити можуть створюватися динамічно за допомогою мови виражень сервісу моніторингу й контролю стану IT.

Обробка інформації, отриманих від зовнішньої бази даних, може включати, наприклад:

– відображення оброблених результатів SQL-запитів на інструментальних панелях;

– активацію користувальницької тривоги, якщо отримані дані відповідають заданим умовам;

– періодичне відправлення по електронній пошті готових до друку звітів, побудованих за результатами виконання SQL-запитів і таке інше.

Запити можуть виконуватися в декількох режимах:

– періодично за заданим розкладом;

– по події або тривозі;

– по запиті («вручну»).

Підтримується також виконання динамічно створених запитів на додавання/відновлення/видалення даних, що дозволяє, наприклад, обновляти таблиці в зовнішній базі даних при настанні події в системі моніторингу.

Моніторинг продуктивності баз даних

Досвідчені адміністратори планують розвиток інфраструктури баз даних заздалегідь, з огляду на й прогнозуючи ріст вимог до її продуктивності. сервісу моніторингу й контролю стану IT полегшує рішення цього завдання, дозволяючи одержувати й аналізувати статистику виконання тестових запитів. Крім того, можна відслідковувати продуктивність баз даних у реальному часі, наприклад, призначивши тривогу на перевищення порога часу виконання певного запиту. Одержавши оповіщення про це поштою або SMS, адміністратор може негайно приступитися до з'ясування причин виниклої проблеми.

Моніторинг і керування по SNMP

Сервіс моніторингу й контролю стану IT надає широкі можливості для моніторингу й керування SNMP-пристроями.

Можливості програмного продукту:

– Підтримка SNMP v1, v2c і v3.

– Розвинені засоби роботи з базою керуючої інформації (MIB): автоматична компіляція MIB-файлів, єдине сховище, більше 200 MIB-файлів включено в базову поставку.

– Групове додавання MIB-файлів при приміщенні в директорію на сервері.

– Групове виконання конфігураційних команд (SNMP set).

– Виявлення SNMP-пристроїв і автоматичне додавання інформації про їх на карту мережі.

– Сканування SNMP-пристроїв (за допомогою операції walk).

– Налаштування періодичності опитування SNMP-змінних і їх кешування.

– Прості й зручні інструменти для роботи з SNMP-Таблицями.

– Гнучке налаштування SNMP-оповіщень.

– Налаштування SNMP-оповіщень у відповідь на подію автоматично або в ручному режимі.

– Підтримка всіх типів даних SNMP.

Сканування SNMP-пристроїв (виконання SNMP walk)

Як програма для SNMP моніторингу сервісу моніторингу й контролю стану IT полегшує контроль і керування гетерогенними мережами, що поєднують пристрою різних виробників. Система виконує пошук SNMP-пристроїв, на стороні сервера кешує отримані дані й в автоматичному режимі зіставляє їх з інформацією з MIB-файлів.

Такий підхід забезпечує ряд переваг:

– Робота з даними й метаданними пристроїв виконується гранично швидко й зручно, крім необхідності постійного обміну інформацією із пристроєм.

– Для SNMP-змінних і їхніх полів використовуються інтуїтивно зрозумілі описи й імена.

– Роботу з SNMP-пристроями можна настроїти на періодичне опитування тільки потрібних змінних для економії ресурсів.

Моніторинг і керування по SNMP передбачає три режими роботи із пристроями:

– Збір тільки важливих значень. У цьому випадку опитуються тільки ті змінні, дані яких використовуються при моніторингу. Такий підхід дозволяє заощадити обчислювальні й мережні ресурси. Список важливих змінних задається в системі глобально.

– Збір всіх значень із MIB-директорії. Система збирає значення всіх змінних, для яких існують MIB-опису. Режим забезпечує збір повної інформації про роботу пристрою. Проаналізувавши ці дані, ви зможете вирішити, які аспекти мають потребу в моніторингу.

– Збір всіх значень, доступних при скануванні. Система збирає всі доступні SNMP-змінні, незалежно від того, є їхній чи опису ні. Нерозпізнані величини представляються в табличній формі й просто не мають зрозумілих описів і імен. Такий підхід дозволяє одержати всі дані, надавані пристроєм, а потім підібрати для невизначених значень MIB-и з метаінформацією.

Обробка SNMP-даних

У системі сервісу моніторингу й контролю стану IT реалізована можливість зберігання в єдиній базі всієї інформації з історії SNMP-змінних (як табличних, так і скалярних). Для роботи з даними SNMP користувачеві надається розширений набір інструментів, у тому числі датчики й тривоги, діаграми, візуальні редактори, звіти.

Обробка оповіщень від SNMP-пристроїв

Система одержує SNMP-оповіщення у вигляді інформаційних повідомлень (informs) і пасток (traps). Оповіщення конвертуються в стандартні події сервісу моніторингу й контролю стану IT і зберігаються в єдиній базі даних. Надалі до таких оповіщень можна застосовувати всі типові операції: фільтрацію, пошук, підтвердження, сортування, а також призначати тривоги.

Здійснюючи SNMP моніторинг, сервісу моніторингу й контролю стану IT може самостійно генерувати інформаційні повідомлення й SNMP-пастки, виконуючи їхнє розсилання у відповідь на тривоги, по запиті користувача або розкладу.

Керування IT-активами

Сервіс моніторингу й контролю стану IT спрощує завдання інвентаризації й супроводу об'єктів IT-інфраструктури, таких як маршрутизатори, сервери, робочі станції, принтери й інше встаткування.

Облік робочих станцій

Автоматизований збір інформації про конфігурації робочих станцій:

– моделі системних блоків;

– інформація про процесори;

– обсяги ОЗП, ПЗП (з показниками поточного рівня завантаження);

– установлені ОС;

– зв'язок зі Співробітником;

– установлене програмне забезпечення;

– інше.

Облік принтерів і видаткових матеріалів

Автоматизований збір інформації про конфігурації принтерів:

– Автоматизований збір інформації про принтери.

– Автоматизоване одержання інформації про необхідність заміни видаткових матеріалів, на підставі яких виробляється формування запитів на роботи із заміни видаткових матеріалів з автоматичним призначенням відповідального за роботи.

– Нагромадження статистики для обліку заміни видаткових матеріалів (картриджі).

– Звіти для планування закупівлі видаткових матеріалів на наступні періоди.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма процесів розробленої системи зображена на рисунку 3.3. При детальному її розгляді можна побачити як саме проходе взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування).

Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

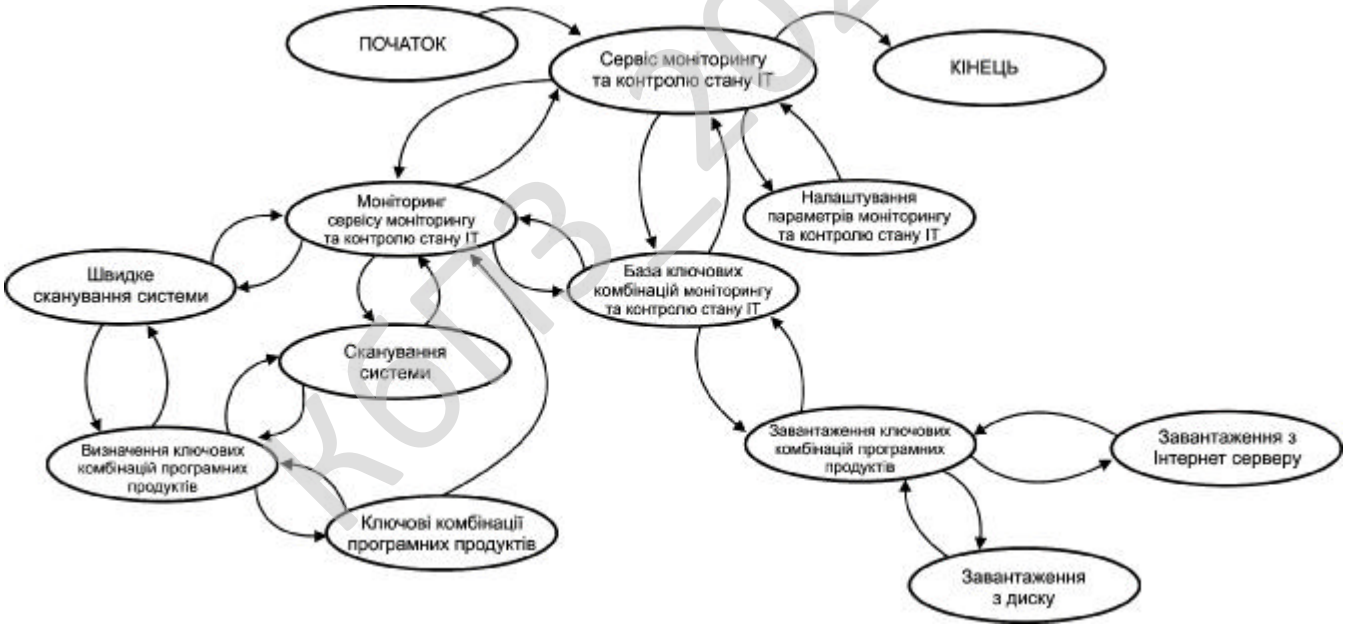

Рисунок 3.3 – Діаграма взаємодії процесів

Діаграми потоків даних містять чотири типи елементів:

– Процеси які являють собою трансформацію даних в рамках описуваної системи.

– Сховища даних (репозиторії).

– Зовнішні по відношенню до системи сутності.

– Потоки даних між елементами трьох попередніх типів.

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Під час роботи над магістерською дипломною роботою було створено блок-схеми. Блок-схеми є першоджерелами стратегії розвитку ПЗ. Тому від точності і детальної блок-схеми залежить результат всієї програми.

При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об’єктно-орієнтована що вимагає оптимізації програми високого рівня, також те, що при розробці програми слід надати особливу увагу модулю сервісу моніторингу та контролю стану ІТ.

На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми.

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підпрограми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ.

При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

Redmine – вільне серверне ПЗ для управління проектами та відстежування помилок. До системи входить календар-планувальник та діаграми Ганта для візуального представлення ходу робіт за проектом та строків виконання.

Redmine написано на мові Ruby і є ПЗ розробленим з використанням відомого веб-фреймворку Ruby on Rails, що означає легкість в розгортанні системи та її адаптації під конкретні вимоги.

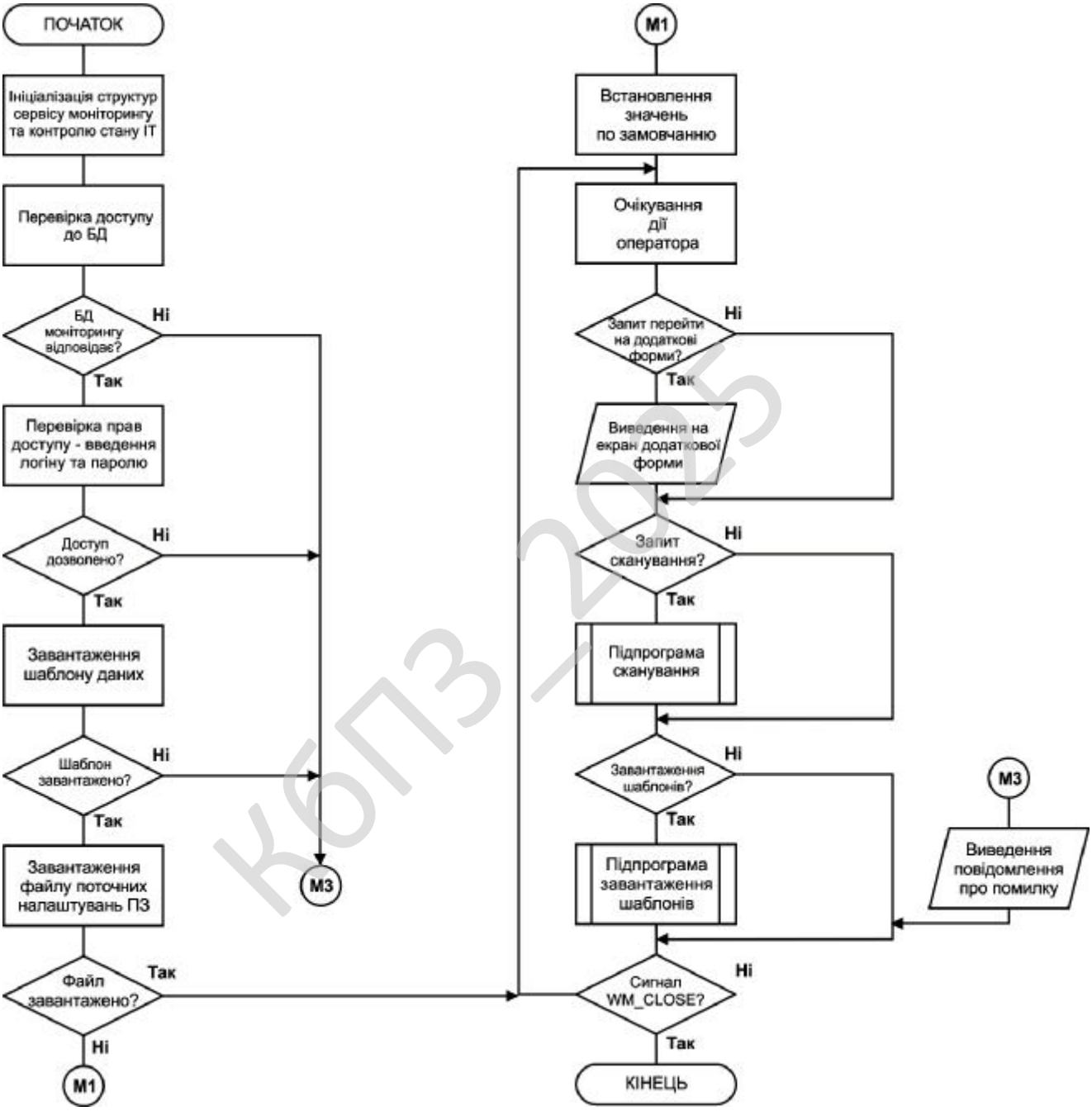

Рисунок 4.1 – Блок-схема основної програми

Для кожного проекту можна вести свої вікі та форуми. Функціональні можливості:

– Ведення декількох проектів.

– Гнучка система доступу з використанням ролей.

– Система відстеження помилок.

– Діаграми Ганта та календар.

– Ведення новин проекту, документів та управління файлами.

– Сповіщення про зміни за допомогою RSS-потоків та електронної пошти.

– Власна Wiki для кожного проекту.

– Форуми для кожного проекту.

– Облік часових витрат.

– Налаштування власних (custom) полів для задач, затрат часу, проектів та користувачів.

– Легка інтеграція із системами керування версіями (SVN, CVS, Git, Mercurial, Bazaar и Darcs).

– Створення записів про помилки на основі отриманих листів

– Підтримка LDAP автентифікації.

– Можливість самореєстрації нових користувачів.

– Багатомовний інтерфейс (у тому числі українська мова).

– Підтримка СКБД: MySQL, PostgreSQL, SQLite.

Діаграма Ганта (*Gantt chart*, також стрічкова діаграма, графік Ганта) – це популярний тип діаграм, який використовується для ілюстрації плану, графіка робіт за будь-яким проектом. Є одним з методів планування та управління проектами. Діаграма Ганта являє собою відрізки (графічні плашки), розміщені на горизонтальній шкалі часу. Кожен відрізок відповідає окремому завданню або підзадачі. Завдання і підзадачі, складові плану, розміщуються по вертикалі. Початок, кінець і довжина відрізка на шкалі часу відповідають початку, кінцю і тривалості завдання. На деяких діаграмах Ганта також показується залежність між завданнями.

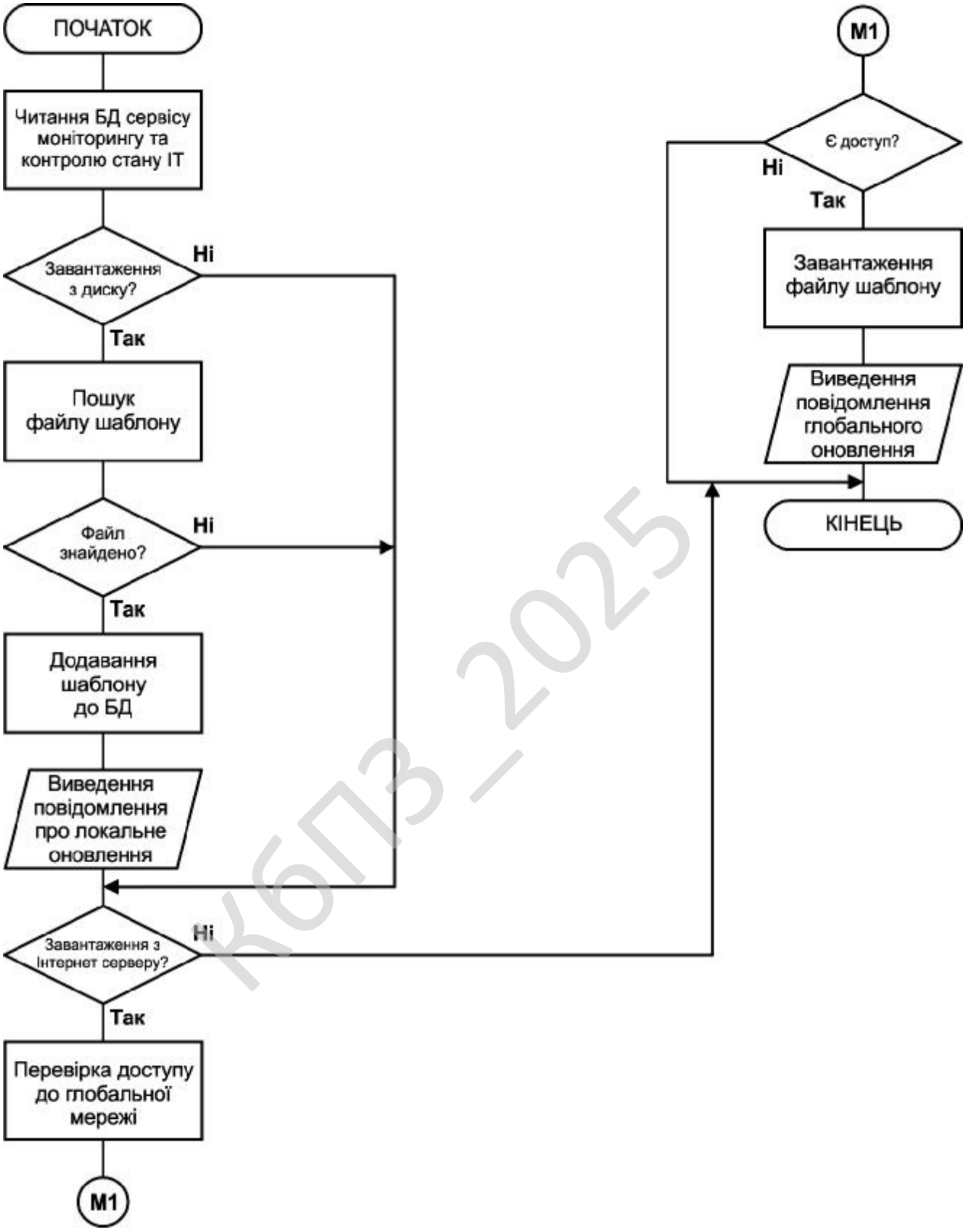

Рисунок 4.2 – Блок-схема роботи підпрограми

Діаграма може використовуватися для представлення поточного стану виконання робіт: частина прямокутника, що відповідає завданню, заштриховується, відзначаючи відсоток виконання завдання; показується вертикальна лінія, що відповідає моменту «сьогодні».

Часто діаграма Ганта використовується спільно з таблицею зі списком робіт, рядки якої відповідають окремо взятій задачі, зображеній на діаграмі, а стовпці містять додаткову інформацію про задачу.

Система відстеження помилок Багтрекер – прикладна програма для допомоги розробникам програмного забезпечення (програмістам, тестувальникам тощо) враховувати і контролювати помилки, знайдені у програмах, питання щодо функціональності, рішення та оновлення, побажання користувачів, а також стежити за процесом їх виконання.

Кожному, хто розробляв програмні продукти, добре знайоме співвідношення «20/80» – останні 20 % роботи тривають 80 % часу.

Як це не парадоксально, але нічого дивного в цій пропорції немає, адже саме на завершальній стадії починається тестування проекту, коли виявляються помилки, і що більший проект, то більше буде знайдено помилок.

Водночас досить часто виявляється, що більшість цих помилок були відомі та могли бути виправлені з меншими витратами на попередніх стадіях роботи, але не були вчасно описані, а потім загубилися серед інших важливих завдань.

Отже, система відстеження помилок у найпростішому варіанті – це процес, що включає в себе виявлення помилки, її опис, виправлення і перевірку цього виправлення, тобто процес «стеження» за багом протягом всього як його життєвого циклу, так і життєвого циклу розробки в цілому.

Сукупність інформації про дефект. Головний компонент такої системи – база даних, що містить відомості про виявлені дефекти. Ці відомості можуть включати в себе:

– номер (ідентифікатор) дефекту;

– хто повідомив про дефект;

– дата і час виявлення дефекту;

– версія продукту, в якій виявлено дефект;

– серйозність (критичність) дефекту та пріоритет рішення;

– опис кроків для відтворення дефекту (неправильної поведінки програми);

– відповідальний за усунення дефекту;

– обговорення можливих рішень та їх наслідків;

– поточний стан виправлення дефекту;

– версії продукту, в якій дефект виправлений.

Крім того, розвинені системи надають можливість прикріплювати файли, які допомагають описати проблему, наприклад, дамп пам'яті або скріншот.

Використання. Основна перевага систем відстеження помилок полягає в забезпеченні чітких централізованих оглядів, запитів на розробку (включаючи помилки і виправлення) та їх стан. У корпоративному середовищі, системи відстеження помилок можуть бути використані для генерації звітів по продуктивності програмістів виправлення помилок. Однак, це може іноді приводити до неточних результатів, тому що різні помилки можуть мати різні ступені пріоритету та серйозності, що пов'язано з складністю їх фіксації.

Життєвий цикл дефекту. Як правило, система відстеження помилок використовує той чи інший варіант «життєвого циклу» помилки, стадія якого визначається поточним станом помилки.

Типовий життєвий цикл дефекту:

1. Новий – дефект зареєстрований тестувальником;

2. Призначений – призначений відповідальний за виправлення дефекту;

3. Дозволений – дефект переходить назад у сферу відповідальності тестувальника. Як правило, супроводжується резолюцією, наприклад:

– Виправлено (виправлення включені у версію таку-то);

– Дубль (повторює дефект, що вже знаходиться в роботі);

– Не виправлено (працює відповідно до специфікації, має занадто низький пріоритет, виправлення відкладено до наступної версії тощо);

– «В мене все працює» (запит додаткової інформації про умови, в яких дефект проявляється).

4. Далі тестувальник проводить перевірку виправлення, залежно від чого дефект або знову переходить у стан «Призначений» (якщо він описаний як виправлений, але не виправлений), або у стан «Закрито».

5. Відкрито повторно – дефект знайдено знову в іншій версії.

Система може надавати адміністраторові можливість налаштування користувачі, які можуть переглядати і редагувати помилки залежно від їх стану, переводити їх в інший стан або видаляти.

У корпоративному середовищі, система відстеження помилок може використовуватися для отримання звітів, що показують продуктивність програмістів при виправленні помилок. Однак, часто такий підхід не дає достатньо точних результатів через те, що різні помилки мають різну ступінь серйозності та складності. При цьому серйозність проблеми прямо не стосується складності її усунення.

Розглянемо обраний метод розробки динамічних систем (Dynamic Systems Development Method, DSDM) – це головним чином методика розробки програмного забезпечення, що базується на концепції швидкої розробки додатків (Rapid Application Development, RAD).

У 2007 році **DSDM** став основним підходом до управління проектом і розробки додатків. DSDM – це ітеративний і інкрементний підхід, який надає особливого значення тривалого участі в процесі користувача/споживача.

Мета методу – здати готовий проект вчасно і вкластися в бюджет, але в той же час регулюючи зміни вимог до проекту під час його розробки. DSDM входить в сімейство гнучкої методології розробки програмного забезпечення, а також розробок, що не входять у сферу інформаційних технологій.

Остання версія DSDM називається DSDM Atern. Назва Atern – це скорочення від Arctic Tern (пер. Полярна крачка). Полярна крачка – птиця, яка може подорожувати на великі відстані. Вона символізує безліч аспектів методу,

наприклад визначення пріоритету або кооперування, які є природним способом ведення робочого процесу.

Попередня версія DSDM (випущена в травні 2003 року), яка все ще діє і широко використовується, – це DSDM 4.2, є дещо розширеною версією DSDM 4. Розширена версія містить настанови щодо того, як використовувати DSDM спільно з Екстремальним програмуванням (Extreme Programming).

Як розширення концепції швидкої розробки додатків, DSDM фокусується на проектах інформаційних систем, що характеризуються стислими термінами і бюджетами. У DSDM присутні вказівки на типові помилки проектів інформаційних систем, таких як перевищення бюджету, запізнення з термінами здачі (виконання), недостатнє залучення користувачів і топ-менеджерів в роботу над проектом. DSDM складається з:

– трьох стадій: передпроектна стадія життєвого циклу проекту і постпроектна стадія;

– стадія життя проекту складається з 5 етапів: дослідження реалізованості, дослідження економічної доцільності, створення функціональної моделі, проектування і розробка, етап реалізації.

При деяких умовах існує можливість включення в DSDM частин інших методик, таких як Rational Unified Process (RUP), Екстремальне програмування, PRINCE2. Інший гнучкий метод, схожий на DSDM по процесу і концепції – Scrum.

Метод DSDM був розроблений у Великобританії в 1990-х Консорціумом DSDM. Консорціум DSDM – це асоціація розробників та експертів в області програмного забезпечення, створена з метою «спільної розробки і просування незалежного фреймворку RAD» комбінуванням кращого практичного досвіду учасників асоціації. Консорціум DSDM – це некомерційна організація незалежних розробників, які володіють та управляють фреймворком DSDM. Перша версія фреймворку була завершена в січні 1995 року і опублікована в лютому 1995 року. У липні 2006 року була представлена відкрита версія DSDM 4.2, яка стала

доступна приватним особам для перегляду і використання. Тим не менш, всі, хто поширює DSDM, повинні бути членами цього некомерційного консорціуму.

На початку 1990-х в індустрії інформаційних технологій став поширюватись новий термін – швидка розробка додатків (Rapid Application Development, RAD). Інтерфейси прикладних програм еволюціонували від старих зелених екранів до графічних інтерфейсів користувача, які використовуються і зараз. На ринок почали виходити нові інструменти для створення додатків, наприклад PowerBuilder. Вони дозволили розробникам простіше ділитися планованими розробками з покупцями – з'явилося прототипування і почалося руйнування класичних, послідовних (каскадних) методів розробки.

Тим не менш, новий рух RAD було дуже неструктурованим: не існувало узгодженого опису цього методу і у багатьох організацій були створені власні опису і підходи до нього. Безліч великих корпорацій були зацікавлені в перспективах, що надаються методом, але вони також були стурбовані тим, щоб не знизився рівень якості їх продукції в кінцевому результаті.

Консорціум DSDM був утворений в 1994 році, коли група людей зустрілася на заході, організованому Butler Group в Лондоні. Всі, хто прийшов на цей захід, працювали у великих організаціях, таких як British Airways, American Express, Oracle and Logica (такі компанії як Data Sciences і Allied Domecq з тих пір були поглинені іншими організаціями).

На цьому зібранні було вирішено, що Дженніфер Степлтон, тоді представляла компанію Logica, розробить архітектуру комлексного, орієнтованого на користувача методу з хорошим контролем якості для ітеративної і інкрементній розробки. Підсумкова архітектура була спроектована так, щоб бути повністю сумісна зі стандартом ISO 9000 і PRINCE2. Коли архітектура була готова (через місяць після зборів), Консорціум сформував групи для її поширення у всіх областях розробки програмного забезпечення, які включали в себе: методи та засоби управління проектом, контроль якості та тестування, методи і засоби розробки. Контрольна група, очолювана творцем архітектури і складається з глав

цих груп, повинна була забезпечити розуміння методу так, як він спочатку замислювався.

Незважаючи на те, що багато членів Консорціуму були прямими конкурентами, вони вільно ділилися тим, як вони вирішують проблеми, що виникають. Практика показала, що найкращий результат може бути досягнутий тільки працюючи як одне ціле. Консорціум збільшився за перший рік від декількох організацій до шістдесяти; опис методу ставало все більш і більш повним. Версія 1 була сформована в грудні 1994 року і опублікована в лютому 1995 року. Результатом став універсальний метод, що охоплює людей, процеси та інструменти. Він сформувався на основі досвіду організацій, різних за родом своєї діяльності і розмірами.

Метод DSDM – принципи. Існує 9 принципів, що складаються з 4 основних та 5 початкових точок.

1. Залучення користувача – це основа ведення ефективного проекту, де розробники ділять з користувачами робочий простір і тому прийняті рішення будуть більш точними.

2. Команда повинна бути уповноважена приймати важливі для проекту рішення без узгодження з начальством.

3. Часта поставка версій результату, з урахуванням такого правила, що «поставити щось хороше раніше – це завжди краще, ніж поставити все ідеально зроблена в кінці». Аналіз поставок версій з попередньої ітерації враховується на наступній.

4. Головний критерій – як можна більш швидка поставка програмного забезпечення, яке відповідає поточним потребам ринку. Але в той же час постачання продукту, який задовольняє потребам ринку, не менш важлива, ніж вирішення критичних проблем у функціоналі продукту.

5. Розробка – ітеративна та інкрементна. Вона ґрунтується на зворотного зв'язку з користувачем, щоб досягти оптимальної з економічної точки зору рішення.

6. Будь-які зміни під час розробки – оборотні.

7. Вимоги встановлюються на високому рівні перш, ніж почнеться проект.

8. Тестування інтегровано в життєвий цикл розробки.

9. Взаємодія і співпраця між усіма учасниками необхідно для його ефективності.

Передумови для використання DSDM.

Щоб успішно використовувати DSDM, необхідно щоб був виконаний ряд передумов. По-перше, необхідно організувати взаємодію між проектною командою, майбутніми користувачами і вищим керівництвом. По-друге, повинна бути можливість поділу проекту на менші частини, що дозволить використовувати ітеративний підхід.

Два приклади проектів, для яких DSDM не дуже підходить:

1. Проекти, критичні безпеки розширене тестування та затвердження в таких проектах конфліктують з метою методу DSDM укластися в терміни і бюджет.

2. Проекти, чия мета зробити компоненти багаторазового використання – вимоги в таких проектах занадто високі і не вкладаються в принцип 80 %/20%.

Життєвий цикл проекту. Фреймворк DSDM складається з трьох послідовних стадій, які називаються передпроектна стадія, стадія життєвого циклу проекту і постпроектна стадія. Стадія життєвого циклу проекту – сама продумана і детально розроблена з усіх інших. Вона складається з п'яти етапів, які формують ітеративний, інкрементний підхід до розробки інформаційних систем.

Ці три фази і відповідні етапи будуть більш детально описані в наступних розділах. Для кожної стадії або етапи будуть розглянуті найважливіші функції і будуть представлені результати.

Стадія 1 – Передпроектна.

На цій стадії визначаються ймовірні проекти, відбувається виділення коштів та визначення проектної команди. Рішення задач на цій стадії допоможе уникнути проблем на більш пізніх стадіях проекту.

Стадія 2 – Життєвий цикл проекту.

На рисунку зображена дана стадія. На ньому показано 5 етапів, які потрібно пройти проекту, щоб стати інформаційною системою. Перші два етапи, дослідження реалізованості та дослідження економічної доцільності, йдуть послідовно і доповнюють один одного. Після завершення цих етапів, відбувається ітеративна та інкрементна розробка системи в етапах: створення функціональної моделі, проектування і розробка, етап реалізації. Ітеративна та інкрементна природа DSDM буде описана далі.

Стадія 3 – Постпроектная.

На цій стадії забезпечується ефективна робота системи. Це досягається за рахунок підтримки проекту, його покращення та виправлення помилок згідно з принципами DSDM. Підтримка проекту здійснюється продовженням розробки, заснованої на ітеративної і інкрементній природі DSDM. Замість того, щоб закінчити проект за один цикл, зазвичай повертаються до попередніх стадій або етапів, щоб поліпшити продукт.

Нижче на діаграмі представлений весь життєвий цикл проекту. Ця діаграма описує ітеративну розробку DSDM. Опис кожного етапу буде представлено нижче.

Чотири етапи стадії життєвого циклу проекту.

Дослідження:

1. Дослідження реалізованості. На даному етапі визначається – потрапляє проект під рамки DSDM. Розглядаючи тип проекту, організаційні і кадрові питання, виноситься рішення – використовувати метод DSDM чи ні. Таким чином буде отримано звіт про застосовність, допустимий прототип і приблизний глобальний план проекту, який включає в себе план розробки і протокол можливих ризиків.

2. Дослідження економічної доцільності. На даному етапі аналізуються основні економічні і технологічні характеристики. Відбувається нараду експертів, на якій обговорюються найбільш важливі сторони системи і приймається рішення

про пріоритети у розробці. На цьому етапі розробляються список основних вимог, опис сфери комерційної діяльності, опис архітектури системи і приблизний план створення прототипів.

Створення функціональної моделі:

1. Визначення функціонального прототипу. Визначення функціоналу, який буде закладено в прототипі на даному етапі. На цьому підетапі розробляється функціональна модель згідно до результатів, отриманих на стадії дослідження економічної доцільності.

2. Узгодження планів. Відбувається узгодження як і в які терміни має бути розроблена функціональність прототипу.

3. Створення функціонального прототипу. Розробка функціонального прототипу, згідно з планами та функціональної моделі.

4. Аналіз функціонального прототипу. Перевірка справності розробленого прототипу. Це може бути досягнуто тестуванням прототипу кінцевим користувачем і/або переглядом документації. Результат – документ, що містить огляд функціонального прототипу.

Проектування і розробка:

1. Визначення конструктивного прототипу. Визначення функціональних і нефункціональних вимог системи. На основі цих вимог повинна бути створена стратегія реалізації. Якщо існує запис про тестування з попередньої ітерації, тоді він теж буде використаний для створення стратегії реалізації.

2. Узгодження планів. Відбувається узгодження як і в які терміни повинні бути реалізовані поставлені вимоги.

3. Створення конструктивного прототипу. Створення системи (конструктивного прототипу), яку можна віддати користувачам для тестування.

4. Аналіз конструктивного прототипу. Перевірити справність спроектованої системи. На цьому підетапі застосовується тестування та перегляд результатів. Створення користувальницької документації та протоколу випробування.

Реалізація:

1. Затвердження системи користувачем. Кінцеві користувачі стверджують протестовану систему для подальшої реалізації і створення довідника користувача.

2. Навчання користувачів. Навчання майбутнього користувача роботі з системою. Результат підетапу – контингент підготовлених користувачів.

3. Реалізація. Реалізація протестованої системи серед користувачів.

4. Аналіз ринку системи. Аналіз впливу випущеної системи на ринок. Головне питання – чи досягнута мета, поставлена при проектуванні системи. Грунтуючись на цьому проект переходить на наступну стадію (постпроектную) або повертається на попередню для доопрацювання. Аналіз буде представлений в документі аналізу проекту.

Чотири етапи життєвого циклу проекту.

Етап 1А: Дослідження реалізованості.

Протягом цього етапу, перевіряється реалізація проекту в рамках DSDM. Передумови для використання DSDM перевіряються відповіддю на питання: «чи Може даний проект задовольнити необхідним економічним вимогам?», «Проект підходить для використання методу DSDM?» і «Які ризики в цьому проекті найважливіші?». Найбільш важливий метод на цьому етапі – використання робочих груп.

Підсумок даного етапу – звіт про застосовність і допустимий прототип, в яких розглянута реалізація проекту, а також приблизний глобальний план проекту та протокол можливих ризиків, що описує найбільш важливі ризики проекту.

Етап 1Б: Дослідження економічної доцільності.

Дослідження економічної доцільності розширює і доповнює етап дослідження реалізованості. Після того, як проект був визнаний реалізованим у рамках DSDM, на цій стадії перевіряються бізнес-процеси, відбувається залучення груп користувачів і аналіз їх вимог і побажань. І знову ж самим затребуваним методом на даному етапі є використання робочих груп. В рамках

робочих груп учасники проекту збираються, щоб обговорити плановану систему. Інформація отримана після даних заходів збирається у список вимог. Важлива властивість цього списку – розподіл пріоритетів серед вимог. Ці вимоги розподілені згідно з методом MoSCoW. На основі отриманої черговості створюється план розробки, який буде орієнтиром для всього проекту.

Для створення цього плану застосовується дуже важлива для проекту методика – тайм-боксинг. Ця методика є обов'язковою для досягнення цілей DSDM – вкладеться у терміни і в бюджет, і при цьому зберегти необхідну якість продукту. Архітектура системи – ще одне підмога в управлінні розробкою інформаційної системи. Підсумком даного етапу є опис сфери комерційної діяльності, в якому міститься контекст проекту всередині компанії, опис архітектури системи, що надає первинну глобальну архітектуру інформаційної системи, що знаходиться в розробці, і план розробки, якому визначені найбільш важливі кроки в процесі розробки. В основі цих двох документів лежить список вимог. Протокол можливих ризиків доповнюється даними, отриманими на цьому етапі.

Етап 2: Створення функціональної моделі.

Вимоги, які були визначені на попередньому етапі, перетворюються на функціональну модель. Вона складається з діючого прототипу і моделей. Прототипування – ключова методика проекту на даному етапі, що дозволяє організувати залучення користувачів до проекту. Розроблений прототип аналізується різними групами користувачів. Щоб досягти необхідної якості, на кожній ітерації застосовується тестування. Найважливіша частина тестування представлена на даному етапі. Створення функціональної моделі можна розділити на наступні підетапи:

– Визначення функціонального прототипу: визначення функціоналу, який буде закладено в прототипі на даному етапі.

– Узгодження планів: відбувається узгодження як і в які терміни повинен бути розроблена функціональність прототипу.

– Створення функціонального прототипу: розробити прототип. Вивчити та доробити прототип на даній ітерації згідно функціонального прототипу, отриманого на попередніх ітераціях.

– Аналіз функціонального прототипу: перевірити справність спроектованої системи. На цьому підетапі застосовується тестування та перегляд результатів.

Підсумком даного етапу є функціональна модель і функціональний прототип, які разом представляють функціональність, отриману на цій ітерації, готову для тестування користувачами. Далі оновлюється список вимог. З нього видаляються вже реалізовані пункти і відбувається повторна зміна черговості решти пунктів. Протокол можливих ризиків також оновлюється, після аналізу функціонального прототипу.

Етап 3: Проектування та розробка.

Головне завдання цієї ітерації – об'єднати функціональні компоненти з попереднього етапу в єдину систему, що задовольняє вимогам користувачів. Тут також розглядаються нефункціональні вимоги. І знову на даному етапі відбувається тестування. Проектування та розробку можна розділити на наступні підетапи:

– Визначення конструктивного прототипу: визначення функціональних та нефункціональних вимог, які повинні бути в системі.

– Узгодження планів: відбувається узгодження як і в які терміни повинні бути реалізовані поставлені вимоги.

– Створення конструктивного прототипу: створення системи, яку можна віддати користувачам для повсякденного використання. Вивчити та доробити прототип на даній ітерації.

– Аналіз конструктивного прототипу: перевірити справність спроектованої системи. На цьому подэтапе застосовується тестування та перегляд результатів. Для створення користувальницької документації використовуються протокол випробування та відгуки користувачів.

Підсумок етапу – створення конструктивного прототипу для тестування користувачами. Протестована система переходить на наступний етап. На даному етапі зовнішній вигляд і функціональність системи загалом готові. Ще один підсумок – створення користувальницької документації.

Етап 4: Реалізація.

На етапі реалізації протестована система разом з користувацької документацією доставляється до майбутнім користувачам і відбувається їх навчання роботи з системою. Система аналізується на відповідність вимогам, поставлених на ранніх етапах проекту. Реалізацію можна розділити на наступні підетапи:

– Затвердження системи користувачем: кінцеві користувачі стверджують протестовану систему для подальшої реалізації і створення керівництва.

– Навчання користувачів: навчання майбутнього користувача роботі з системою. Результат підетапи – контингент підготовлених користувачів.

– Реалізація: реалізація протестованої системи серед користувачів.

– Аналіз ринку системи: аналіз впливу випущеної системи на ринок. Головне питання – чи досягнута мета, поставлена при проектуванні системи. Грунтуючись на цьому проект переходить на наступну стадію (постпроектную) або повертається на попередню для доопрацювання.

Підсумок етапу: закінчена система, придатна для використання кінцевими користувачами, контингент підготовлених користувачів і детальний документ аналізу проекту.

Етап створення функціональної моделі DSDM.

Протокол можливих ризиків – протокол виявлених ризиків. Важливий для подальших стадій, містить проблеми з якими є ймовірність зіткнутися. Повинен постійно оновлюватися.

Список вимог за пріоритетами – список вимог, розподілених по пріоритету. Процес розподілу заснований на методі MoSCoW, який визначає які вимоги повинні бути реалізовані раніше (з економічної точки зору).

Список функціональних вимог – список нефункціональних вимог, з якими доведеться мати справу на наступному етапі.

Функціональне вимога – ця функція використовується для побудови моделі та прототипування згідно пріоритетам.

Функціональна модель – модель, побудована на основі функціональних вимог. Вона буде використана для розробки прототипу на наступному подэтапе. Ця модель буде використана для створення плану прототипування.

Прототипування – процес швидкого виготовлення працюючої моделі (прототипу) для того, щоб перевірити дизайн, проілюструвати закладені ідеї та функції і раніше зібрати відгуки користувачів.

Список інтервалів часу – список інтервалів часу виконання окремих робіт, необхідний, щоб вкластися у графік виконання всього проекту.

План прототипування – план процесу прототипування, який буде виконаний у часові інтервали згідно з графіком.

Графік робіт – набір робіт і часу проведення цих робіт, погоджений сторонами. Використовується в реалізації функціонального прототипу.

Функціональний прототип – прототип, що дозволяє побачити всі функції системи і те, як система буде ці функції виконувати.

План реалізації – підготовка робіт для реалізації функціонального прототипу згідно з графіком робіт та списку вимог.

Покращена функція – функція прототипу, яка була покращена і протестована на даній ітерації до об'єднання з іншими частинами прототипу.

Об'єднана функція – функція прототипу, яка була об'єднана з функціями попередніх ітерацій. Новий об'єднаний функціональний прототип буде протестований на наступному етапі.

Протокол випробування – запис тестування, що складається з сценарію тестування, процедури тестування та результатів тестування.

Документ аналізу функціонального прототипу – складається з коментарів користувачів про поточної версії, необхідних для роботи над наступними

ітераціями. Цей документ використовується для оновлення протоколу можливих ризиків та списку вимог.

Модель розвитку процесу.

Робота за визначенням функціонального прототипу полягає у визначенні функціоналу, який буде присутній в прототипі на даній ітерації. Аналітика та програмування закінчено; прототипи зібрані; і досвід отриманий від них використаний для поліпшення моделей аналізу (а також ґрунтується на оновлених списку вимог і протоколі можливих ризиків).

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм LOKI_91. Механізм алгоритму LOKI_91 подібний DES (рисунок 4.3). Блок даних розщеплюється на ліву й праву половини й проходить 16 раундів, що досить нагадує DES. У кожному раунді права половина спочатку піддається операції XOR із частиною ключа, а потім розширювальній перестановці (таблиця 4.1).

Таблиця 4.1 – Перестановка з розширенням

4	3	2	1	32	31	30	29	28	27	26	25
28	27	26	25	24	23	22	21	20	19	18	17
20	19	18	17	16	15	14	13	12	11	10	9
12	11	10	9	8	7	6	5	4	3	2	1

48-бітовий вихід розділяється на чотири 12-бітових блоки. У кожному блоці виконується така підстановка з використанням S-блоку: береться кожний 12-бітовий вхід, 2 старших і 2 молодших біти використовуються для утворення номера r, а вісім внутрішніх біт утворять номер c. Вихід S-блоку, O, має наступне значення: $O(r,c) = (c + ((r*17) \oplus 0xff) \ \& \ 0xff)^{31} \bmod P_r$.

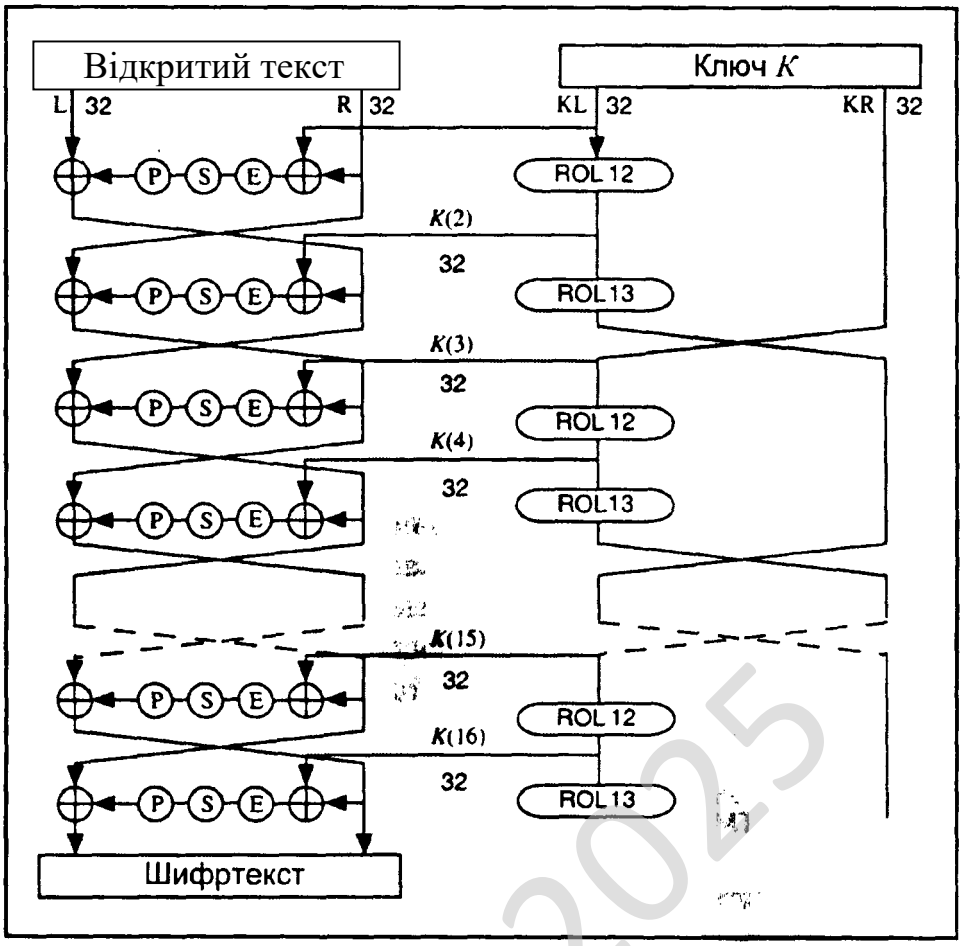

Рисунок 4.3 – Алгоритм LOKI91

Таблиця 4.2 – Значення P_r

r	1	2	3	4	5	6	7	8
P_r	375	379	391	395	397	415	419	425
r	9	10	11	12	13	14	15	16
P_r	433	445	451	463	471	477	487	499

Після цього чотири 8-бітових результати знову поєднуються, утворюючи 32-бітове число, що піддається операції перестановки, описаній в таблиці 3. Нарешті, для одержання нової лівої половини виконується операція XOR правої половини з колишньою лівою половиною, а ліва половина стає новою правою

половиною. Після 16 раундів для одержання остаточного шифртексту знову виконується операція XOR над блоком і ключем.

Таблиця 4.3 – Перестановка за допомогою P-блоку

32	24	16	8	31	23	15	7	30	22	14	6	29	21	13	5
2	20	12	4	27	19	11	3	26	18	10	2	25	17	9	1

Підключи генеруються із ключа досить прямолінійно. 64-бітовий ключ розбивається на ліву й праву половини. На кожному раунді підключем служить ліва половина. Далі вона циклічно зрушується вліво на 12 або 13 біт, потім після кожних двох раундів ліва й права половини міняються місцями. Як і в DES, для зашифрування й розшифрування використовується один й той самий алгоритм із деякими змінами у використанні підключів.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Розглянемо розроблене ПЗ сервісу моніторингу та контролю стану ІТ яке зображено на рисунку 5.1. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

– Навігаційне меню: Файл; Налаштування; Допомога.

– Розділу обрання шляхів сканування.

– Розділу виведення результату роботи системи.

– Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.

– Функціональних кнопок ПЗ.

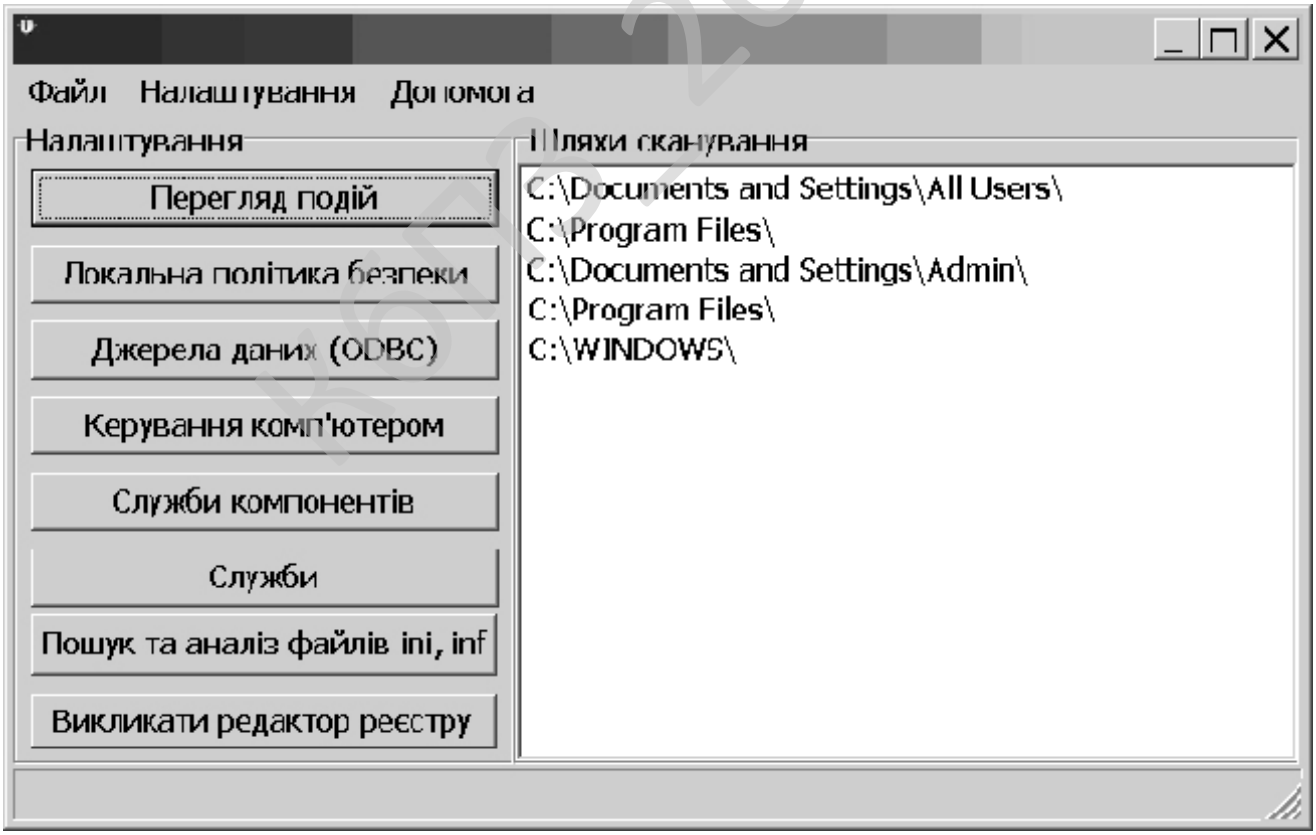

Рисунок 5.1 – Головне вікно ПЗ

Традиційний підхід до моніторингу IT-інфраструктури не відповідає її складності, мінливості й ступеню впливу на роботу всієї організації. Це ставить під погрозу всі рівні підтримки IT-інфраструктури: від планування (помилки при виділенні необхідних ресурсів, неадекватні витрати на окремі сервіси й т.д.) до оперативної діяльності (довге з'ясування причин інцидентів і їхня невірна класифікація, зниження рівня доступності сервісів, усунення наслідків замість визначення причин, відсутність проактивності).

Найчастіше на сформовану невідповідність починають реагувати, коли воно вже приймає вкрай хворобливі форми, але навіть у цьому випадку мало хто намагається вирішити проблему кардинально! Чому? І що можна зробити вже сьогодні, щоб все це залишилося в минулому? Нижче я постараюся відповісти на ці питання. Але спочатку давайте розберемося, які саме застарілі ідеї (стереотипи) не дають реалізувати потенціал технологій моніторингу.

Розроблена програма має дуже простий і інтуїтивно зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий.

Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити.

Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

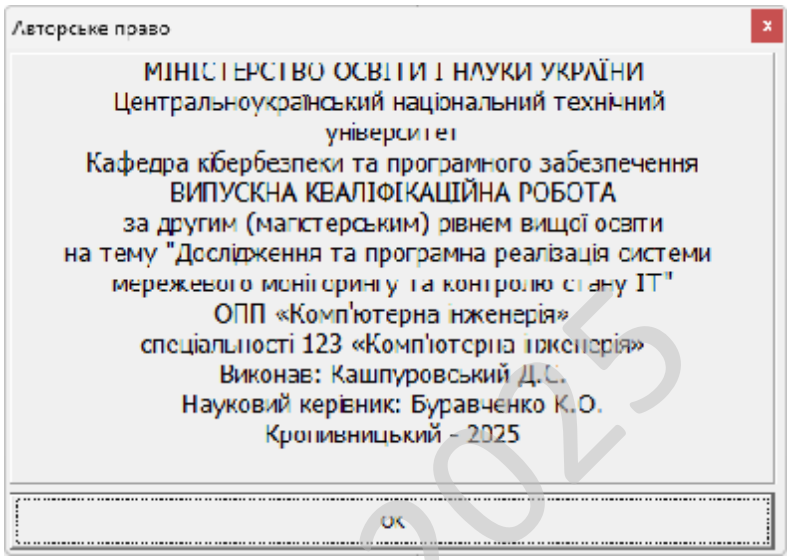

Рисунок 5.2 – Авторське право

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

– Випуск.

– Встановлення та активація.

– Деактивація.

– Адаптація.

– Обновлення.

– Вмонтування.

– Відстежування версій.

– Видалення.

– Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати IT рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене IT рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження.

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в IT рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

– відповідності поставленим вимогам;

– правильна відповідь для усіх можливих вхідних даних;

– виконання функцій за прийнятний час;

– практичність;

– сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування форматом білої скриньки засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

У цьому випадку формуються тестові варіанти, в яких:

– Гарантується перевірка всіх незалежних маршрутів програми.

– Знаходяться гілки True, False для всіх логічних рішень.

– Виконуються всі цикли (у межах їхніх кордонів та діапазонів).

– Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

– Кількість незалежних маршрутів може бути дуже велика.

– Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

– У програмі можуть бути пропущені деякі маршрути.

– Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки" пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

– Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.

– Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

– При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

– Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

Обрано умови розповсюдження – Freeware.

Це власницьке програмне забезпечення, котре можна Безоплатно використовувати протягом необмеженого терміну без обмежень у функціональності, і поширюване без сирцевих кодів.

Автори такого програмного забезпечення, як правило, хочуть «дати щось спільноті», але хочуть також контролювати його подальшу розробку. Іноді, коли програмісти вирішують припинити розробку, вони передають сирцевий код іншим програмістам, або ж спільності як вільне програмне забезпечення.

Дуже часто плутають поняття «безплатне програмне забезпечення» та «вільне програмне забезпечення», хоча вони суттєво відрізняються.

Безплатне програмне забезпечення можна безоплатно встановлювати та використовувати (іноді з певними обмеженнями, як, наприклад, «безплатне для домашнього або некомерційного вжитку»), в той час як вільне програмне забезпечення можна продавати за будь-яку суму, але при тому, у користувача, котрий його отримує, повинні бути права на вивчення, модифікацію та поширення сирцевих кодів одержаної програми.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого моніторингу та контролю стану ІТ.

Метою розробки є дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

Об'єктом дослідження є процес мережевого моніторингу та контролю стану ІТ.

Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого моніторингу та контролю стану ІТ.

– Розроблено вітчизняний продукт мережевого моніторингу та контролю стану ІТ, який має більш широкі можливості, на відміну від існуючих аналогів.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Визначення цільової аудиторії кінцевого готового продукту

Результати дослідження та розробки системи мережевого моніторингу та контролю стану ІТ можуть бути насамперед корисними для підприємств, які мають розгалужену ІТ-інфраструктуру й використовують сервери, мережеве обладнання та корпоративні сервіси для підтримки своєї діяльності. Для таких компаній стабільність і безперебійність роботи інформаційних систем є критично важливими, тому можливість своєчасного виявлення несправностей або перевантажень стає суттєвою конкурентною перевагою. Саме система моніторингу допомагає контролювати роботу мережевих пристроїв у режимі реального часу, виявляючи проблеми ще до того, як вони вплинуть на користувачів.

Особливий інтерес до таких систем можуть проявити ІТ-компанії, які займаються наданням послуг хостингу, розробкою програмного забезпечення або підтримкою клієнтів. Для них швидкість реагування на інциденти та якість технічного обслуговування є показниками репутації, а отже, від роботи системи моніторингу залежить рівень довіри клієнтів і лояльність користувачів. Такі підприємства часто працюють у середовищі, де навіть хвилинна затримка чи зупинка сервера призводить до фінансових збитків, тому автоматизація контролю за станом мережі – це не розкіш, а необхідність.

Крім комерційних компаній, результати дослідження будуть актуальними для державних структур, освітніх установ і організацій, які мають внутрішні мережі та зберігають великі обсяги інформації. У таких установах впровадження системи моніторингу підвищує ефективність роботи ІТ-відділів, зменшує ризик втрати даних і допомагає раціонально використовувати наявні ресурси.

Не менш важливим є значення цієї розробки для навчальних і наукових закладів. Вони можуть використовувати систему як навчальну платформу для підготовки фахівців у сфері інформаційних технологій. Студенти отримають можливість не лише спостерігати за реальною роботою системи моніторингу, а й аналізувати дані, моделювати різні ситуації та вчитися реагувати на інциденти. Таким чином, результати дослідження мають універсальний характер і можуть бути впроваджені як у бізнесі, так і в освіті.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Для оцінки привабливості програмного продукту було проведено експертне опитування серед фахівців у галузі IT-інфраструктури, адміністраторів систем і представників компаній, що мають досвід використання схожих рішень. Експертам було запропоновано оцінити систему за основними критеріями – функціональні можливості, надійність, простота впровадження, масштабованість, вартість експлуатації та потенційна економічна ефективність.

Більшість експертів високо оцінили саме інтелектуальну частину системи – можливість автоматичного сповіщення про інциденти, генерацію аналітичних звітів і прогнозування потенційних відмов обладнання. Особливо було відзначено, що система працює стабільно навіть при великому навантаженні й може адаптуватися до різних типів мережевої інфраструктури, що робить її універсальною.

За результатами оцінки середній рівень привабливості продукту склав 8,7 бала з 10 можливих. Експерти зазначили, що така система може мати великий попит серед середніх і великих підприємств, особливо якщо її вартість залишатиметься конкурентною. Також було підкреслено, що простота інтерфейсу та можливість кастомізації під конкретного користувача є суттєвими перевагами, які підвищують комерційний потенціал рішення.

Таким чином, метод експертних оцінок показав, що система має високу ринкову привабливість, відповідає актуальним потребам бізнесу та може стати успішним продуктом за умови належного маркетингового просування та підтримки користувачів.

7.3 Вибір методу оцінки вартості ПЗ

Для оцінки вартості розробки системи мережевого моніторингу та контролю стану ІТ доцільно використовувати витратний метод. Він передбачає визначення всіх фактичних витрат, які були понесені під час створення програмного продукту, включаючи оплату праці розробників, витрати на апаратне забезпечення, ліцензії, тестування та впровадження. Такий підхід дозволяє точно визначити базову собівартість проєкту, що є особливо важливим для невеликих команд і стартапів.

Однак, у випадку комерційного впровадження, доцільно поєднати цей підхід із дохідним методом. Дохідний метод дає змогу оцінити майбутні вигоди, які підприємство отримає після впровадження системи. Наприклад, скорочення простоїв серверів, підвищення ефективності роботи персоналу та зменшення витрат на ручну діагностику мережі є прямими джерелами економічної вигоди.

Такий комбінований підхід дозволяє не лише визначити початкову вартість розробки, а й обґрунтувати економічну доцільність проєкту. Він допомагає потенційним інвесторам побачити не просто витрати, а реальні фінансові перспективи, які відкриває впровадження системи.

У результаті використання комбінованої моделі оцінки можна отримати повну картину вартості та окупності проєкту, що стане основою для прийняття управлінських рішень щодо його реалізації чи масштабування.

7.4 Розрахунок економічної ефективності від впровадження реалізованого ПЗ як фактору його привабливості

Компанія має розгалужену IT-інфраструктуру, яка включає сервери, мережеве обладнання, робочі станції, системи зберігання даних і корпоративні сервіси. До впровадження системи моніторингу контроль за станом мережі здійснювався вручну: адміністратори виявляли проблеми лише після звернень користувачів або повного виходу сервісів із ладу. Це призводило до простоїв, затримок у роботі та фінансових втрат. Основна мета впровадження системи мережевого моніторингу – забезпечити цілодобове автоматичне відстеження стану обладнання, серверів і додатків, оперативне реагування на інциденти, зниження кількості простоїв і запобігання критичним збоям у роботі IT-інфраструктури. Вхідні дані зафіксовано в таблиці 7.1.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	До впровадження	Після впровадження	Економічний ефект
Кількість простоїв серверів на рік	20 випадків	5 випадків	–15
Середня тривалість простою одного сервера	4 години	1 година	–3 години
Середні втрати підприємства за 1 годину простою	25 000 грн	5 000 грн	–20 000 грн
Витрати на ручну діагностику й усунення збоїв	300 000 грн/рік	150 000 грн/рік	–150 000 грн
Вартість впровадження системи моніторингу	—	—	450 000 грн
Річні витрати на підтримку системи	—	—	100 000 грн

Розрахунок економічного ефекту демонструє наступне: зменшення збитків від простоїв – 1 975 000 грн/рік, економія на технічному обслуговуванні – 150 000 грн/рік, сукупний річний ефект – 2 125 000 грн/рік, чистий ефект – 2 025 000 грн/рік, термін окупності (Payback Period) – 0,22 року (~2,5 місяці), коефіцієнт ефективності (ROI) – 450%.

Додаткові (немонетарні) переваги: підвищення стабільності IT-інфраструктури завдяки ранньому виявленню збоїв, зменшення навантаження на IT-персонал через автоматизацію моніторингу, покращення SLA (Service Level Agreement) і задоволеності користувачів, прогнозування потенційних проблем через аналітику та звітність у реальному часі, зростання репутації підприємства, адже мінімізуються ризики затримок у наданні послуг або збою критичних бізнес-процесів.

Таким чином, моніторинг стає не лише технічним інструментом, а й важливою складовою операційної надійності та конкурентоспроможності підприємства.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Просування системи моніторингу має будуватися на поетапному підході, що включає як технічну демонстрацію, так і інформаційне просування. На першому етапі варто створити пілотний проєкт і запропонувати його впровадження у невеликій кількості підприємств для збору відгуків і реальних кейсів. Це дозволить перевірити ефективність системи в реальних умовах і створити довіру до продукту.

Далі важливо забезпечити інформаційну присутність продукту – через участь у галузевих конференціях, IT-форумах, онлайн-презентаціях і спеціалізованих публікаціях. Саме через публічну експертну комунікацію формується репутація розробника та усвідомлення цінності рішення на ринку.

Наступним етапом є розширення партнерських зв’язків. Доцільно співпрацювати з ІТ-компаніями, які займаються інтеграцією корпоративних систем, адже вони можуть пропонувати продукт своїм клієнтам як частину комплексного рішення. Водночас слід розробити гнучку цінову політику – наприклад, ліцензування за кількістю пристроїв або модель передплати, що зробить продукт доступнішим для малого та середнього бізнесу.

Просування має супроводжуватися технічною підтримкою користувачів, оновленнями та навчанням персоналу. Це створює позитивний досвід використання продукту та сприяє формуванню довгострокових відносин із клієнтами. У підсумку правильна стратегія просування допоможе не лише збільшити продажі, а й побудувати впізнаваний бренд на ринку ІТ-рішень.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Для оптимізації каналів збуту варто поєднати прямі продажі з цифровими платформами розповсюдження програмного забезпечення. Власний сайт компанії може стати не лише вітриною продукту, а й каналом комунікації з клієнтами, де вони зможуть отримати демо-версію, консультацію або підтримку. Це сприятиме зниженню витрат на маркетинг і збільшенню довіри.

Додатково ефективним буде впровадження партнерської програми для системних інтеграторів і реселерів, які вже мають доступ до корпоративних клієнтів. Така модель дозволяє розширити охоплення ринку без суттєвих додаткових інвестицій.

Також можна запропонувати гібридну форму реалізації: ліцензування для великих компаній і модель SaaS (Software as a Service) для малого бізнесу. Це підвищить доступність системи та дозволить гнучко реагувати на потреби різних сегментів ринку.

Ключовим напрямом оптимізації збуту є створення якісного сервісу після продажу – технічна підтримка, регулярні оновлення, аналітичні звіти. Усе це забезпечує стабільність роботи клієнта й стимулює його до подальшої співпраці.

7.7 Визначення ключових факторів успіху конкретного проєкту

Основним фактором успіху є стабільність і надійність системи. Якщо система моніторингу працює без збоїв і забезпечує реальну користь, вона швидко здобуває довіру користувачів. Технологічна якість продукту, його здатність масштабуватися й інтегруватися з іншими IT-рішеннями відіграють ключову роль у його життєздатності.

Другим важливим чинником є професійна команда розробників і технічної підтримки. Клієнти цінують не лише продукт, а й можливість отримати швидку допомогу у випадку проблем або питань. Від рівня компетенції фахівців залежить не лише якість обслуговування, а й довгострокові відносини з партнерами.

Не менш значущим є гнучкість системи – можливість адаптувати її під специфіку кожного клієнта. Різні компанії мають різну інфраструктуру, тому універсальне, але налаштовуване рішення стає перевагою.

І, нарешті, успіх будь-якого IT-проєкту визначається здатністю постійно вдосконалюватися. Регулярні оновлення, впровадження нових технологій і зворотний зв’язок із користувачами формують довіру й підтримують актуальність продукту на ринку. Саме ці чинники разом створюють основу для стабільного розвитку та комерційного успіху системи моніторингу.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Електронно-обчислювальна машина (ЕОМ) відіграє важливу роль у житті сучасної людини. Кожного дня мільйони людей використовують ЕОМ для пошуку необхідної інформації, спілкуванні у соціальних мережах, перегляду новин, роботи тощо. Багато людей користуються ЕОМ у професійних цілях, оскільки завдяки ЕОМ з'явилося багато нових професій. Тому для розробника хмарних сервісів так важливо розробити зручний інтерфейс для зручного сприйняття інформації, та необхідний функціонал, який буде відповідати необхідним вимогам та навантаженням. Все це вимагає багато часу та великого навантаження з боку розробників. Тому так важливо слідкувати за умовами праці, в яких відбувається робочий процес. Оскільки захворювання можуть бути спричинені надмірним фізичним або розумовим навантаженням, через велику нервово-емоційну напругу, або через виробниче середовище. В даному розділі магістерської роботи проведемо аналіз основних чинників при роботі програміста.

Законом України "Про охорону праці" регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98.

8.2 Шкідливі і небезпечні фактори при роботі з комп'ютером

Електронно-обчислювальна машина (ЕОМ) та інше обладнання є джерелами небезпеки ураження електричним струмом. Так як робота програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють люди (у т.ч. програмісти) необхідно створити належний мікроклімат, параметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-98.

На роботу програміста впливають наступні фактори: невідповідний мікроклімат приміщення (температура, вологість), недостатня освітленість робочої зони, підвищений рівень шуму та електромагнітного випромінювання, порушення іонного складу повітря, неправильна ергономічна організація робочого місця, ризики, пов'язані із погіршенням зору, порушенням фізичного стану, стресом тощо.

Шкідливими факторами при роботі з персональним комп'ютером є неіонізуюче випромінювання промислової частоти, збільшене нервово- емоційне навантаження на оператора, збільшення навантаження на органи зору та дрібні стереостатичні рухи кінцівок. Ці фактори можуть викликати у працівника певні розлади здоров'я, зокрема підвищення артеріального тиску, кон'юктивіти, тендовагініти та інші захворювання.

Комп'ютер, як і будь-який електричний прилад, особливо при його неправильному підключенні, може бути джерелом ураження оператора електричним струмом. Саме тому всі працівники, які працюють з персональним комп'ютером, повинні мати першу (або другу) групу допуску з електробезпеки.

Через наявність зазначених факторів працівники, які працюють з персональними комп'ютерами, підлягають попередньому та періодичному медичному огляду згідно з пунктом 6.2.3 додатку 4 до наказу Міністерства охорони здоров'я України «Про затвердження Порядку проведення медичних оглядів працівників певних категорій» від 21 травня 2007 року № 246.

8.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Оптимальна температура в приміщенні для праці має становити 20-24°С, відносна вологість – 40-60 %, атмосферний тиск – 750 мм. рт. ст., запиленість не повинна перевищувати 10 мг/м^3, швидкість руху повітря – 0,1 м/с.

Через те, що обчислювальна техніка є джерелом тепловиділення, організація мікроклімату потребує додаткових зусиль: кондиціонування, провітрювання, використання систем опалення тощо. Об’єм приміщень повинен передбачатися з урахуванням як мінімум 20 м^3 /на особу [4].

Монітори комп’ютерів є джерелом випромінювання, яке може зашкодити здоров’ю людини. Для убезпечення роботи з комп’ютером відстань від монітора повинна становити не менше 50 см, бажано використовувати монітори зі зниженим рівнем, скорочувати час безперервної роботи за комп'ютером (робити п’ятнадцяти хвилинні перерви після кожних півтори години праці). Також в приміщенні необхідно встановлювати іонізатори повітря, використовувати нейтралізатори та зволожувачі.

Комп’ютери та периферійні пристрої є джерелами шуму, висока інтенсивність якого може призвести до проблем з органами слуху та негативно впливати на психологічний стан. Рівень шуму на робочому місці не повинен перевищувати 50 дБА [5]. Для зменшення рівня шуму можна використовувати звукопоглинальні пристрої, а стіни приміщень з комп’ютерами можуть бути покриті звукопоглинальними матеріалами. Поряд із шумом часто виникає вібрація. Для зменшення рівня вібрації в приміщенні на поверхні необхідно встановлювати віброізолятори.

Ергономічні показники робочого місця програміста мають бути наступними: висота робочої поверхні повинна складати 720 мм, розмір поверхні має становити 1600 х 1000 мм; під столом повинен бути простір з розмірами по глибині 650 мм; стіл повинен мати підставку для ніг, розташовану під кутом

15°до поверхні; відстань клавіатури від краю столу має бути не більше 300 мм; відстань між очима й екраном повинна складати 40 – 80 см; стілець повинен мати підйомно-поворотний механізм; висота сидіння має регулюватися в межах 400 – 500 мм, глибина – не менше 380 мм, а ширина – не менше 400 мм, висота опорної поверхні спинки має бути не менше 300 мм, ширина – не менше 380 мм. Кут нахилу спинки стільця до площини сидіння повинен змінюватися в межах 90 – 110° [6].

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року.

В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

У приміщенні знаходяться наступні джерела шуму: принтер Prinics PicKit M1 Smartphone Photo Printer White, електродвигуни вентиляторів ЕОМ.

Робота програміста передбачає постійний візуальній контакт з моніторами комп'ютерів, та, як наслідок, значне навантаження на зір. Традиційно, це зорова робота високої або середньої точності. Для зорової роботи високої точності загальне освітлення (розподіл світла у всьому об'ємі приміщення) має становити 300 лк, комбіноване освітлення (поєднання загального і місцевого освітлення) – 750 лк. Штучне освітлення повинно бути рівномірним та використовуватися в світлий і темний час доби. Джерелами штучного освітлення можуть слугувати люмінесцентні лампи. Правильне освітлення передбачає уникнення відблисків на екранах.

З 2019 року діють Державні будівельні норми України "Природне і штучне освітлення" – ДБН В.2.5-28:2018 [4], у яких прописані вимоги до використання всіх освітлювальних приладів, у т.ч. світлодіодних.

Працю працівника, який постійно працює за комп'ютером, згідно ДБН В.2.5-28:2018 [4], можна віднести до роботи з малою точністю (найменший

розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В). Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [4], Крім того все поле зору повинно бути освітлено достатньо рівномірно – це основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

8.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який

повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов'язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

8.5 Розрахункова частина

Проведемо розрахунок штучного освітлення за методом коефіцієнта використання світлового потоку для приміщення ширина якого складає 6 м, довжина – 7 м, висота – 2,9 м.

У зазначеному приміщенні працює 4 людей.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою [1]:

$$F = E \cdot S \cdot K \cdot Z / n,$$

де:

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; E = 300 Лк;

S – площа освітлюваного приміщення (у нашому випадку S=6 х 7 = 42 м^2);

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення

залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку $K = 1,5$);

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1.1... 1.2, у нашому випадку $Z = 1,1$);

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку від усіх ламп і обчислюється в долях одиниці [8]; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{стін.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{стін} = 50\%$ і $\rho_{стелі} = 50\%$.

Обчислимо індекс приміщення за формулою:

$$i = S/(h\cdot (A+B)),$$

де:

S – площа приміщення, $S = 42$ м2;

h – розрахункова висота підвісу, $h = 2,9$ м (співпадає з висотою стелі, оскільки лампи освітлення закріплюються на стелі);

A – ширина приміщення, $A = 6$ м;

B – довжина приміщення, $B = 7$ м.

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$i=1,4.$$

Знаючи індекс приміщення, за знаходимо $n = 0,29$ (з табличних даних коефіцієнтів використання світлового потоку (n) світильників з відповідним типом лампам) [8]. Підставимо всі значення у формулу, визначимо світловий потік: F=71689 Лм.

Для розрахунку будемо використовувати світлодіодні стельові панелі Delux LED Panel 41 44 Вт, світловий потік яких $F_л = 3600$ Лм.

Число ламп визначається за формулою:

$$N=F/F_л$$

де:

F – світловий потік,

$F_л$ – світловий потік однієї лампи.

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$N= 71689 / 3600 =19,9 \text{ шт.}$$

Приймаємо необхідну кількість світлодіодних світильників 20 шт.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз умов праці, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок штучного освітлення, як одного з ключових факторів впливу на працездатність та здоров'я програміста. Розроблено заходи з умов поліпшення охорони праці.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевого моніторингу та контролю стану ІТ.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого моніторингу та контролю стану ІТ.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого моніторингу та контролю стану ІТ.

– Досліджена система мережевого моніторингу та контролю стану ІТ.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевого моніторингу та контролю стану ІТ.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм LOKI_91.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Проведено маркетингове та економічне обґрунтування ІТ-проєкту, що дозволило визначити ключові фактори успіху даного проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кашпуровський Д.С. Дослідження та програмна реалізація системи мережевого моніторингу та контролю стану ІТ // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

2. Ramon Nastase «Computer Networking: The Beginner's guide for Mastering Computer Networking, the Internet and the OSI Model». 2018. – 186 p.

3. Russ White & Ethan Banks «Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient, Modern Networks». 2017. – 832 p.

4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». *Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка»* (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.

5. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.

6. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

7. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології,* 2024, № 13, с. 28-35.

8. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y.

«Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

9. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

10. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

11. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.

12. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи,* 2023, том 7, № 2, С. 49-56.

13. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.

14. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

15. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації*

та зв'язку, 2022, № 3(69). С. 93-98.

16. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»,* № 2 (307). С. 46-52. 2022.

17. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

18. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.

19. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

20. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

21. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

22. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In:

Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

23. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

24. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.

25. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.

26. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.

27. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

28. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T),* Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

29. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications,*

Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.

30. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.

31. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019*/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

32. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

33. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352.

34. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings* Volume 2353, *CEUR Workshop Proceedings* 2019, Pages 618-629.

35. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

36. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95

37. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О.,

Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки.* №4. С. 103-110. 2020.

38. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.

39. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

40. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у *Кібербезпека та інформаційні технології: монографія.* – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

41. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». *Центральноукраїнський науковий вісник. Технічні науки.* № 2(33). с. 161-172, 2019.

42. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

43. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

44. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С.

Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

45. Дрєєва Г.М., Смірнов О.А., Дрєєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 173-183, 2019.

46. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дрєєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 184-194, 2019.

47. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87.

48. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

49. Смірнов О.А., Котелянець В.В. Стійкі до колізій стохастичні моделі функціонування безпроводових сенсорних мереж. Вісник інженерної академії України, №3, с. 145-152, 2018

50. Смірнов О.А., Смірнов С.А., Дідик А.К., Дрєєв А.М. Алгоритми формування безлічі маршрутів передачі метаданих у антивірусні хмарні системи. Збірник наукових праць "Системи обробки інформації". – Випуск 5 (142). – Х.: ХУПС – 2016. – С. 148-152.

51. Смірнов О.А., Смірнов С.А. Дідик А.К., Дрєєв О.М. Моделі системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних системах. Збірник наукових праць "Системи обробки інформації". – Випуск 3 (140). – Х.: ХУПС – 2016. – С. 36-39.