

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
“ ____ ” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи інтелектуального
моніторингу ЦОД з середою передачі даних реалізованою за
стандартом IEEE 802.3bq”

Виконав здобувач вищої освіти
IV курсу, групи КН-22
ОПП «Комп’ютерні науки»
спеціальності 122 «Комп’ютерні науки»
_____ Сурженко В.О.
« ____ » _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Коваленко А.С.
« ____ » _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань . 12 “Інформаційні технології”
Спеціальність 122 “Комп’ютерні науки”
Освітньо-професійна (освітньо-наукова) програма “Комп’ютерні науки”

ЗАТВЕРДЖУЮ

Завідувач кафедри

д.т.н., проф.

Олексій СМІРНОВ

« 15 » січня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Сурженку Володимиру Олександровичу

(прізвище, ім’я, по батькові)

1. Тема роботи *Програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq*

2. Керівник роботи *Коваленко Анна Степанівна, канд. техн. наук, доцент*

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 116-02 від 06.02.2026 року

3. Строк подання студентом роботи до захисту *23.05.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію.

6. Висновки

6. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

Структурна схема системи *1 аркуш*

Функціональна схема системи *1 аркуш*

Діаграма процесів *1 аркуш*

Блок-схема алгоритму роботи додатку *2 аркуша*

7. Дата видачі завдання « 15 » січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.03.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2026 р.	
3.	Розробка моделі компонента	20.03.2026 р.	
4.	Розробка структур даних	25.03.2026 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026 р.	
6.	Програмування алгоритмів	10.04.2026 р.	
7.	Оформлення ПЗ	17.04.2026 р.	
8.	Попередній захист роботи	23.05.2026 р.	

Дата видачі завдання
« 15 » січня 2026 р.

Підпис керівника

Коваленко А.С.
(прізвище та ініціали)

Завдання прийнято до виконання
« 15 » січня 2026 р.

Підпис здобувача

Сурженко В.О.
(прізвище та ініціали)

АНОТАЦІЯ

Сурженко В.О. Програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. 122 Комп'ютерні науки. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Метою розробки є програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Результат роботи – програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

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'ютерні науки, інтелектуальний моніторинг, ЦОД, IEEE 802.3bq.

ABSTRACT

Surzhenko V.O. Software for the intelligent monitoring system of a data center with a data transmission medium implemented according to the IEEE 802.3bq standard. 122 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed, which is intended for the intelligent monitoring system of a data center with a data transmission medium implemented according to the IEEE 802.3bq standard.

The purpose of the development is the software for the intelligent monitoring system of a data center with a data transmission medium implemented according to the IEEE 802.3bq standard.

The result of the work is the software implementation of the intelligent monitoring system of a data center with a data transmission medium implemented according to the IEEE 802.3bq standard.

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 convenient user 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 science, intelligent monitoring, data center, IEEE 802.3bq.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	7
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	7
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	21
2.3 Розгорнута постановка завдання	22
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	24
3.1 Опис функціонування системи	24
3.2 Розробка структурної схеми.....	27
3.3 Розробка функціональної схеми	50
3.4 Розробка діаграми процесів.....	59
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	62
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	62
4.2 Захист розробленого програмного забезпечення.....	82
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	87
6 ОСНОВНІ ВИСНОВКИ.....	93
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	95

					ВКРБ-122.26.0029.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення системи інтелектуального моніторингу ЦОД, середою передачі даних реалізованою за стандартом IEEE 802.3bq	Літ.	Аркуш	Аркушів
Розроб.	Сурженко В.О.					Б	1	101
Перев.	Коваленко А.С.							
Н.контр.	Коваленко А.С.					ЦНТУ КН-22		
Затв.	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

БД	—	база даних
ЛОМ	—	локальна обчислювальна мережа
ASP		Active Server Pages – активні серверні сторінки
DHCP	—	Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла
HTTP	—	HyperText Transfer Protocol – протокол передачі гіпертексту
IMAP	—	Internet Message Access Protocol – протокол доступу до електронної пошти Інтернету
ICMP	—	Internet Control Message Protocol – міжмережний протокол керуючих повідомлень
MMC	—	Microsoft Management Console
POP3	—	Post Office Protocol Version 3 – протокол поштового відділку, версія 3
SQL	—	Structured Query Language – мова структурованих запитів
SMTP	—	Simple Mail Transfer Protocol – простий протокол передачі пошти
SNMP	—	Simple Network Management Protocol – простий протокол керування мережею
Syslog	—	стандарт відправки повідомлень про зміни які відбуваються в мережі
UDP	—	User Datagram Protocol – протокол користувальницьких дейтаграм

ВСТУП

Актуальність теми. Периферійні обчислення розвиваються прискорено, переміщуючи більше ІТ-інфраструктури у віддалені місця. Цей зсув зробив 2026 рік ключовим для переосмислення розгортання центрів обробки даних. Чи є центральний центр обробки даних – або навіть центральна хмара – найкращою стратегією розгортання для дедалі більш розподіленого ІТ-середовища? Чи варто ІТ-директорам та менеджерам центрів обробки даних розширювати свою присутність за допомогою мікроцентрів обробки даних на периферії?

У цьому прагненні до периферії бізнес-варіанти використання численні та різноманітні. Вони включають віддалене виробництво; розподільчі центри та роздрібні магазини, які повинні працювати «самостійно»; безпеку Інтернету речей та портативні пристрої в розподілених об'єктах та кампусах; логістичні операції з автомобілями, вантажівками та залізничними вантажами, які переміщуються та повинні відстежуватися за допомогою датчиків Інтернету речей по всьому ланцюжку поставок; а також телемедицинські конференції та медичні пристрої для домашніх потреб, які контролюють здоров'я пацієнтів. Підприємства мають левову частку цих впроваджень периферії, оскільки саме вони є компаніями, які найімовірніше матимуть розподілені операції.

Ось що не змінюється в русі на межі можливостей: від ІТ-відділу все ще очікується підтримка всього цього.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

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

– Огляд існуючих систем інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

- Дослідження системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.
- Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

КБПЗ-2026

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Доцільність стандартизації швидкості 25 Гбіт/с

До середини 2000-х років кожне нове покоління мережного встаткування Ethernet підтримувало в 10 разів більшу пропускну здатність, ніж попереднє. Ситуація початку мінятися тільки після 2010 року, і це було обумовлено декількома обставинами.

По-перше, в електропровідних лініях, на відміну від волоконно-оптичних систем, подальше екстенсивне збільшення пропускну здатності стало неможливо через фізичне обмеження кількості субканалів, оскільки є всього чотири пари проводів.

По-друге, темпи росту швидкостей передачі істотно сповільнилися, що пов'язане з можливостями електроніки. У таких умовах економічна ефективність телекомунікаційної частини ІТ-інфраструктури може підтримуватися більше частою заміною апаратури.

По-третє, нарощування швидкості в 2,5-4 рази є більше простою з технічної точки зору процедурою в порівнянні зі збільшенням її на порядок.

Стосовно до ЦОД використання більше дешевої 25-гігабітної техніки дозволить, крім іншого, збільшити строк її експлуатації: із часом це встаткування може бути зняте з магістральної частини й переведено на нижні рівні. Не можна скидати з рахунків краща відповідність швидкості 25 Гбіт/с потребам підсистеми масової пам'яті.

Немаловажне значення має помітне зменшення обсягів і тривалості науково-дослідних та дослідно-конструкторських робіт (НДДКР), причому це стосується як активного встаткування, так і кабельної техніки. Для реалізації електронної частини активного встаткування масово задіюються рішення, які вже

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

застосовуються в 25-гігабітній волоконно-оптичній магістральній техніці. На фізичному рівні виробляється нова – проста – ресертифікація на відповідність частотному діапазону техніки Категорії 6_A (Категорія 8.1) і 7_A (Категорія 8.2).

1.2 Область застосування

Областю застосування є ЦОД. ЦОД або Дата центр – усе ще рідкі поняття для українських компаній. І якщо серед ІТ-шників його роль питань не викликає, то починаючи від менеджерів до власників компаній інших областей виникає маса питань. Питання дуже різноманітні – від того, що таке Дата-центр, як улаштований процес його роботи й властиво навіщо він потрібний.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

Delta InfraSuite: Інтелектуальні Рішення для Центрів Обробки Даних

Зростаюча ділова активність і використання високих інформаційних технологій стали настільки зв'язаними явищами, що проектування й будівництво високопродуктивних центрів обробки даних є однією з найбільш важливих завдань сучасних ІТ-менеджерів. Займаючи протягом 40 років лідируюче положення в області силової електроніки, команда фахівців компанії Delta Electronics розробила нове покоління інтелектуальних рішень для центрів обробки даних: InfraSuite, що дозволяє створювати енергоефективні дата-центри з мінімальним впливом на навколишнє середовище.

Рішення InfraSuite для дата-центрів компанії Delta містять у собі систему живлення, стійки й аксесуари, прецизійне охолодження, системи моніторингу й керування. Центр обробки даних повинен володіти відказостійкою системою електропостачання, у зв'язку із чим зростає потреба в збільшенні потужності джерела безперервного живлення (ДБЖ). Модульний ДБЖ NH Plus, що входить у рішення InfraSuite для дата-центрів, при виникненні несправності й відключенні ушкодженого модуля продовжує харчувати навантаження в режимі онлайн.

Кабінет розподілу живлення, що також входить у систему живлення InfraSuite, легко переміщається в процесі змін живильної мережі дата-центру, при цьому він забезпечує всі необхідні функції захисту й контролю електроживлення.

Система моніторингу й керування дозволяє відслідковувати параметри навколишнього середовища, а також має функцію збору, зберігання й відображення інформації про центр обробки даних.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

InfraSuite легко інтегрується з усіма системами центру обробки даних і забезпечує надійний захист його встаткування.

Delta InfraSuite Продукти й Служби

Переваги InfraSuite:

- Модульна конструкція, що забезпечує швидке й легке складання.
- Масштабованість. Дозволяє нарощувати потужність центру обробки даних відповідно до росту потреб.
- Висока ефективність. Застосування компонентів з незначним енергоспоживанням дозволяє створювати ЦОДи з мінімальним впливом на стан навколишнього середовища.
- Легка інтеграція з усіма структурами центру обробки даних.
- Система відстеження параметрів навколишнього середовища, що забезпечує надійну роботу встаткування центру.

Мікро-ЦОД

Delta InfraSuite – це високоінтегроване рішення нового покоління для модульних ЦОД. Рішення містить у собі стійки й всі підсистеми ЦОД, повністю інтегровані між собою: системи живлення, охолодження, розподілу живлення, блискавкозахисту, пожежного захисту (опціонально), проводки, керування повітряними потоками, інтелектуального моніторингу й багато чого іншого. Рішення Delta для модульних ЦОД надає середовище, що забезпечує безпечну роботу встаткування в стійках, і підтримує розвиток і стандартизацію мікро-ЦОД. Delta InfraSuite займає дуже мало місця, що дозволяє швидко виконувати розгортання в умовах обмеженого простору, і існує в 10 варіантах, що вимагають ДБЖ потужністю 20 кВт.

Застосування

Delta InfraSuite можна використовувати в мікро-ЦОД площею до 50 кв.м або з ІТ-навантаженням до 20 кВт. Підходить для застосування в регіональних компаніях і малому бізнесі.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

Переваги

Висока надійність

- Найвищий рівень надійності класу А.
- Відповідає трьом рівням надійності А, В і С національного стандарту GB50174; підтримує конфігурації N, N+1 або 2N відповідно до потреб клієнта. Відповідає вимогам до найвищого рівня надійності класу А.
- Зверхнадійне аварійне охолодження.
- Система охолодження включається при одержанні сигналу про занадто високу температуру. Вона оснащена високонадійною системою забезпечення живлення й не вимагає використання ДБЖ.
- Підвищення надійності завдяки розподіленому керуванню.
- Використовується розподілена система керування кондиціонуванням повітря, ДБЖ, умовами середовища й інтелектуальних стійок (регулює температуру й вологість, висвітлення, блоки розподілу живлення, датчики відкривання дверей і ін.). Нормальне відображення й завантаження інших повідомлень від устаткування зберігається навіть при збої одного з контролерів.

Оптимізація загальної вартості володіння

- Енергозбереження. Коефіцієнт ефективності енергоспоживання нижче 1,4.
- Система гарячих і холодних коридорів ефективно перешкоджає змішуванню холодного й гарячого повітря. У стійках використовується охолодження горизонтальним повітряним потоком, що дозволяє скоротити кількість гарячих ділянок у ЦОД. ДБЖ забезпечує ККД перетворення АС-АС до 94% і вище навіть при навантаженні 50%.
- Найвища ефективність використання простору.
- Внутростійкова система охолодження використовує відцентровий вентилятор, що спрямований у холодний коридор. Горизонтальний повітряний потік зменшує опір і скорочує довжина холодного коридору. Глибина 1200 мм ідеально вписується в планування ЦОД і заощаджує займаний простір.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

Висока адаптуємість

- Швидке розгортання.
- Підходить для ЦОД невеликого й середнього розміру в сферах державного керування, утворення, фінансів, малого й середнього бізнесу. Забезпечує гнучкість, короткі строки будівництва й можливість розширення в будь-який момент часу без великих інвестицій.
- Ступінь готовності до роботи можна регулювати.
- Ступінь готовності системи до роботи можна змінити на будь-якому етапі, включаючи проектування, монтаж або експлуатацію. Системи електроживлення й охолодження не вимагають повторного проектування.

Інтелектуальне керування

- Можливість підключення даних про умови середовища й безпеки в ЦОД.
- Оповіщення про температуру й вологість у ЦОД, виявленні задимлення, доступі в ЦОД, сигнали з IP-камер і інше, можна підключити до стандартної системи керування. Система готова до використання й не вимагає повторної розробки.
- Оповіщення через Whatsapp і мобільний додаток.
- У той час як оповіщення за допомогою SMS вимагає додаткових витрат, використання Whatsapp не тільки дозволяє скоротити витрати, але й більше відповідає сучасним тенденціям. Мобільні додатки дозволяють обслуговуючому персоналу й керівникам одержувати інформацію про функціонування системи в будь-який час і в будь-якому місці.
- Убудована система керування доступом у системну шафу.
- Запобігає здатне привести до відмови системи порушення режиму експлуатації такого встаткування, як ДБЖ або система охолодження, персоналом з недостатньою кваліфікацією. Системи доступу розміщені на передніх і задніх дверцятах системної шафи. Тільки вповноважені співробітники можуть

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

відкривати дверцят, увівши пароль на сенсорному екрані. При збої системи доступу можна відкрити дверцята ключем.

Модульний ЦОД

Модульний ЦОД Delta – гнучке інтелектуальне рішення для малого й середнього бізнесу. Крім інтеграції основних систем, таких як системи живлення, пристрою охолодження, стійки й системи моніторингу, рішення також передбачає холодні й гарячі коридори, які забезпечують передові можливості керування повітряним потоком, що підвищують ефективність охолодження. Будівництво традиційного ЦОД займає від 1,5 до 2 років, у той час як на розгортання модульного ЦОД потрібно всього лише кілька тижнів. Завдяки модульній конструкції модульний ЦОД Delta надає можливість оплати в міру росту (as-you-grow), забезпечує високу гнучкість і короткі строки монтажу, що дозволяє задовольняти швидко зростаючі потреби компаній, що займаються зберіганням і обробкою даних.

Переваги

Швидке розгортання завдяки високій масштабованості

- Підходить для малого й середнього бізнесу.
- Гнучкість і швидка адаптуємість.
- Швидкий монтаж.
- Оплата в міру росту.

Висока надійність завдяки використанню стандартних модулів

- Модульна конструкція.
- Стандартизація.
- Висока інтеграція.
- Висока надійність системи.
- Вибір конфігурації (N, N+1 або 2N) відповідно до потреб клієнта.
- Відповідність вищому рівню сертифікації ЦОД Tier 4 по стандарті TIA-942.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

Комплексне й з високим ступенем інтеграції

- Інтеграція ДБЖ, кабінетів розподілу живлення, батарей, пристроїв охолодження, стійок і іншого встаткування.
- Висока ефективність використання простору завдяки невеликим габаритам.

Висока ефективність і екологічність

- Кондиціонери RowCool задовольняють вимогам по щільності потужності (низьк, середньої й високої) і заощаджують простір.
- Система гарячих і холодних коридорів підвищує ефективність охолодження.
- Модульні ДБЖ забезпечують високий ККД навіть при низькому навантаженню.
- При відповідних погодних умовах можна використовувати природне охолодження.

Контейнерний ЦОД

Швидке розгортання ЦОД для периферійних обчислень у світі Інтернету речей

В ІТ-сферах з інтенсивними потоками даних ЦОД для периферійних обчислень (edge datacentre) служить проміжним пунктом кешування й нагромадження даних між користувачами й більшими ЦОД, що дозволяє полегшити величезні ІТ-навантаження. У зв'язку з поширенням периферійних обчислень, Delta представляє нове покоління контейнерних ЦОД із гнучкими системами живлення й охолодження, можливістю швидкого розгортання й масштабування для будь-яких сфер застосування. Комплексне рішення забезпечує не тільки зручність придбання всього необхідного в одному місці, але й високу системну інтеграцію й надійність.

Застосування

- Хмарні обчислення.
- Телекомунікації.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

- Периферійні обчислення.
- Мережа доставки контенту.

Переваги

Швидке розгортання й оплата по факті

Будівництво традиційного ЦОД займає від 1,5 до 2 років. Завдяки модульній конструкції контейнерний ЦОД Delta забезпечує високу гнучкість і масштабованість, а також короткі строки розгортання (кілька тижнів), що дозволяє задовольняти швидко зростаючі потреби в нарощуванні потужності.

Висока інтегрованість і надійність

- Використання готових, попередньо протестованих і повністю зконфігурованих компонентів забезпечує високу мобільність.
- Інтеграція ДБЖ, кабінетів розподілу живлення, батарей, пристроїв охолодження, стійок і іншого встаткування.

Енергоефективність і низький коефіцієнт ефективності енергоспоживання

- Можливості керування швидкістю обертання вентиляторів RowCool забезпечують значну економію енергії.
- Система гарячих коридорів підвищує ефективність охолодження.
- ДБЖ забезпечує ККД перетворення АС-АС 95% навіть при навантаженні 30%.

Повна керованість

Система керування інфраструктурою ЦОД Delta надає комплексне рішення для керування й моніторингу таких аспектів роботи ЦОД, як живлення, енергоспоживання, ресурси, робочі замовлення, безпека, керування продуктивністю й ін.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

Delta InfraSuite Manager – керування інфраструктурою центру обробки даних (DCIM)

Система Моніторингу й Керування (EMS) є зразком системи DCIM і дозволяє відслідковувати різні параметри навколишнього середовища, такі як температура, вологість, влучення води, сигналізація вогню, диму, несанкціонованого проникнення.

Пристрій EnviroProbe дозволяє здійснити моніторинг температури й вологості як одного кабінету, так і певного сегмента дата-центру, а за допомогою EnviroStation дані обстеження передаються по мережі. Датчики EnviroProbe реагують на повінь, задимлення, пожежу, проникнення й інші фактори.

Система DCIM від Delta Electronics дозволяє оперативно управляти центром обробки даних і відправляти повідомлення в режимі реального часу. Висока ефективність керування забезпечується зручним графічним інтерфейсом і хронологічним записом подій. EMS відрізняється гнучкістю й дозволяє встановлювати різні рівні тривоги залежно від потреб дати-центру. Крім того, DCIM має багаторівневу систему доступу й може бути легко інтегрована в будь-яку систему керування підприємством.

Центральна станція контролю й моніторингу EnviroStation

Система моніторингу й керування (EMS) дозволяє відслідковувати параметри мікроклімату (температуру й вологість), а також такі події, як витік води, поява вогню й диму, несанкціонований доступ. EMS пропонує IT-менеджерам інтегровану платформу для більше зручного моніторингу й керування сучасним ЦОД. EnviroStation поєднує дані моніторингу навколишнього середовища й інших параметрів, і передає їх по мережі диспетчерові. Установлювані користувачем тривожні сигнали гарантують безпеку центру обробки даних.

Датчик параметрів навколишнього середовища EnviroProbe

EnviroProbe контролює температуру й вологість усередині стійки або шафи, а також передає сигнали від інших датчиків параметрів навколишнього

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

середовища (наприклад, дверних контактів, датчиків диму, полум'я, витоку води й ін.) у систему керування по мережі. Якщо EnviroProbe оснащений дискретними й аналоговими виходами, то він інформує ІТ-менеджера про всі зміни в навколишній середовищі за даними, отриманим від убудованих і зовнішніх датчиків. EnviroProbe подає сигнали тривоги, у тому числі звуковий сигнал убудованого зумера при виявленні витоку води, а також контролює активацію й деактивацію зовнішніх пристроїв (наприклад, магнітного замка).

Охолодження ЦОД

Рішення Delta по прецизійному охолодженню відрізняються високої холодопродуктивністю й здатні винятково точно підтримувати задану температуру й вологість повітря усередині ЦОД. Професійне рішення по охолодженню для ЦОД Delta поєднує повну лінійку агрегатів охолодження, у яку входять: повітроохолоджувачі серії RowCool, установлені поруч із джерелом тепла для ліквідації зон температурного максимуму; повітроохолоджувачі серії RowCool з подачею повітря нагору й долілиць; повітророзподільний блок (ADU), використовуваний разом з повітроохолоджувачем RoomCool з подачею повітря долілиць для ефективного видалення тепла із зон температурного максимуму. Крім точної підтримки заданої температури й вологості рішення по охолодженню для ЦОД від Delta Electronics забезпечують високу енергоефективність, сприяючи тим самим скороченню витрат на експлуатацію й технічне обслуговування.

Підвищення щільності потужності в сучасних ЦОД привело до того, що традиційні прецизійні кондиціонери вже не можуть забезпечити охолодження в наступних ситуаціях:

- Коливання навантаження в періоди пікового й звичайного споживання.
- Висока щільність потужності.
- Нерівномірний розподіл тепла.

Тому так важливо підібрати комплексні рішення по охолодженню для ЦОД. Міжрядні прецизійні кондиціонери RowCool у сполученні з повітророзподільним блоком InfraSuite ADUB забезпечать оптимальне

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

охолодження ЦОД. Як правило, у центрах обробки даних з фальшполами охолоджене повітря від кондиціонера подається до кожної стійки через канали під підлогою. Однак у міру видалення стійки від кондиціонера надходження до неї охолодженого повітря зменшується. Крім того, під підлогою часто прокладені кабелі й труби, що перешкоджають проходженню охолодженого повітря й сприяють утворенню зон температурних максимумів.

ДБЖ

Клієнти зацікавлені в якісному енергопостачанні без зникнень напруги, провалів і кидків, зниження або підвищення напруги, відхилень частоти, гармонійних перекручувань і перешкод. Компанія Delta Electronics, що спеціалізується в області безперебійного живлення, регулювання напруги й пристроїв захисту, розробила чотири сімейства джерел безперебійного живлення – Agilon, Amplon, Ultron і Modulon. Джерела живлення компанії Delta забезпечують максимальну економію при винятковій компактності. Вони володіють найвищим ККД і винятковою стабільністю параметрів. Ці характеристики вказують на придатність систем безперебійного живлення Delta для найбільш відповідальних додатків. У таблиці нижче наведені їхні діапазони потужності, а також короткі описи архітектури й області застосування.

Номенклатура випускається продукції, що, дозволяє нашим замовникам вибирати системи безперебійного живлення, повністю відповідним їхнім вимогам по забезпеченню безперебійної роботи і які забезпечують довгострокову конкурентну перевагу. Також клієнти можуть замовляти ДБЖ, виходячи з початкових потреб свого бізнесу, а потім нарощувати їх у міру необхідності. Дане рішення забезпечує максимум переваг при одночасному скороченні сукупної вартості володіння системою безперебійного живлення.

На додаток до вискоєфективних і надійних джерел безперебійного живлення, компанія Delta Electronics пропонує програмне забезпечення UPSentry і InsightPowerUPS, значно розширювальної можливості керування ДБЖ. Установивши підтримувані мережні карти, користувачі, можуть дистанційно

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

контролювати роботу джерела безперебійного живлення, виконувати початкову діагностику при аномальних відхиленнях, а також включати або виключати системи якщо буде потреба.

Переваги Систем Безперебійного Живлення Delta:

- Високий ККД перетворення АС-АС.
- Повністю резервуєма конструкція й конфігурація.
- Високий коефіцієнт потужності на вході й на виході.
- Простота розширення без використання додаткового встаткування.
- Простота експлуатації при низькій сукупній вартості володіння.

Гібридні системи живлення

Компанія Eltek (входить до складу Delta Group) представляє гібридні системи живлення – рішення для забезпечення живлення ЦОД нового покоління. Нове рішення забезпечує неперевершену надійність, масштабованість і компактність у порівнянні із традиційними системами, а також більше низьку загальну вартість володіння. Це можливості забезпечення живлення майбутнього, доступні вже сьогодні. Гібридні системи живлення надають гнучку модульну інфраструктуру, що задовольняє всі потреби ЦОД по живленню в галузях ІТ, телекомунікацій, хмарних обчислень і банківських операцій. Рішення з високою щільністю потужності не має можливості, що мають аналоги, забезпечення живлення для телекомунікаційного й ІТ-устаткування, а також пристроїв охолодження.

Проста й недорога експлуатація:

- Усунення необхідності в складних розподільних пристроях, пов'язаних з виникненням ризиків.
- Масштабування під потреби будь-якого ЦОД, від 100% змінного струму до 100% постійного струму в кращій комбінації.
- Базовий блок напруги постійного струму природно вирівнює навантаження, включає паралельну роботу й виконує синхронізацію.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

- Одна архітектура для тренування для всіх застосувань і ремонт без останова.
- Убудовані контролери, можливості підключення системи керування інфраструктурою ЦОД.
- Модульна конструкція із фронтальним завантаженням з використанням квадратних кабінетів розміром 600 мм, що відповідають компоновчій сітці приміщення.
- Тестування генераторної установки в реальному часі в будь-який час.
- Високий стандарт готовності до роботи забезпечує час на відновлення після відмови або модернізацію у власному темпі.

Оригінальна гібридна система живлення

Основою гібридної системи живлення є система збірних шин напругою 380 В постійного струму й батареї, що відповідають новому стандарту ДБЖ високої напруги постійного струму для ЦОД і ІКТ. У своїй базовій конфігурації гібридна система живлення являє собою випрямляч постійного струму 380 В з батареями, що подає постійний струм у серверні приміщення з мінімумом втрат на електропровідність і перетворення. Випрямляч, що має модульну масштабовану конфігурацію, заснований на добре зарекомендувала себе високоефективної технології Eltek.

Зважаючи на те, що стандарт 380 В постійного струму поки не одержав широкого поширення, гібридну систему можна розширити модульними ДБЖ на базі інвертора, підключеними до шини/батареїному блоку 380 В постійного струму через гальванічно розв'язаний вхідний каскад постійного струму. Клієнт може вибрати конфігурацію тільки з виходом змінного струму, тільки з виходом постійного струму або будь-які комбінації змінний і постійний токи, не жертвуючи ефективністю й надійністю й маючи можливість розширення рішення в будь-якому напрямку після монтажу.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

Що стосується входу змінного струму, гібридна система пропонує унікальну альтернативу традиційному автомату включення резерву між мережею й дизель-генератором.

Автомат включення резерву – єдина точка відмови в традиційній конфігурації ДБЖ. При використанні гібридної системи живлення клієнт може зовсім відмовитися від автомата включення резерву, підключивши другий випрямляч прямо до генератора. Таке рішення особливо привабливо у випадках, коли очікується часте застосування генератора через нестабільну напругу в електромережі або обмежень пікового навантаження. Під час запланованих експлуатаційних випробувань генератора підключена до електромережі система залишається в режимі очікування й забезпечує безперебійну подачу живлення на критичні навантаження у випадку відмови генератора.

4 варіанти перетворення зі зниженням

– Пряма подача постійного струму на виділені джерела живлення фронтального сервера (наприклад, при відкритих обчисленнях).

– Пряма подача змінного струму на звичайні джерела живлення фронтального сервера, коли основна частина загального навантаження харчується змінним струмом.

– подача постійного струму на кабінети інверторів, які забезпечують перетворення в змінний струм, коли невелика частина загального навантаження харчується змінним струмом.

– подача постійного струму 380 В на кабінети перетворювачів постійного струму, які забезпечують перетворення в постійний струм 48 В для живлення телекомунікаційного встаткування колишніх поколінь. Також доступні більше компактні внутрішні рішення.

Міні-варіант гібридної системи живлення

Повністю масштабовану інфраструктуру забезпечення живлення можна одержати й при використанні міні-варіантів гібридної системи живлення. Це

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

більш компактні, але повноцінні рішення, розмір яких розрахований на підтримку одного ряду серверних шаф.

Вони надають всі переваги повномасштабної системи. Крім того, міні-рішення мають високу гнучкість, оскільки інфраструктуру забезпечення живлення можна розширювати в міру росту бізнесу, а також адаптувати системи живлення до вимог у кожному ряді шаф.

Rectiverter – це здвоєний модуль перетворення електричної енергії з 3 портами. Пристрій сполучає функції випрямляча, інвертора й статичного перемикача уведення. Це ідеальне рішення для змішаних середовищ із живленням змінний і постійний токи.

Основні можливості

- Джерело безперебійного живлення змінного й постійного (48 В) струму загальною потужністю до 100 кВт.
- Двошкафне рішення з батареями й блоком розподілу живлення.
- Опціонально доступний випрямляч, що підключається до дизель-генератора.

Застосування:

- Система живлення в ЦОД, що харчує встаткування змінним і постійним струмом.
- Контейнерні, модульні ЦОД.

Гібридна система живлення на основі змінного струму

Гібридна система живлення на основі змінного струму являє собою комбінацію перетворювача змінного струму й окремого випрямляча постійного струму.

Це рішення заміняє собою традиційний автомат включення резерву, що часто є єдиною точкою відмови, і дозволяє проводити в реальному часі випробування генератора під максимальним навантаженням без відключення від електричної мережі.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

Гібридна система живлення на основі змінного струму заснована на інверторі Eltek потужністю 25/50 кВт, що забезпечує високий ККД перетворення електроенергії, можливості резервування й гарячої заміни. Потужність кожної шафи можна зконфігурувати до 200/450 кВт, а масштабованість дозволяє підняти потужність до 1000/3600 кВт завдяки паралельному включенню шаф.

Випрямляч, що підключається до дизель-генератора, заснований на випрямлячах Eltek HE, що забезпечують ККД перетворення світового класу, і дозволяє використовувати батареї для подачі живлення постійного струму на інвертор при тривалих перебоях енергопостачання.

Основні можливості:

- Перетворювач змінного струму з опціональним випрямлячем, що підключається до генератора, для підвищення надійності й безпечного випробування генератора.
- Економічне, високоякісне рішення для застосування в системах з ДБЖ змінного струму.
- Сполучимо із системою керування будинками Infrasuite.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – це потужна мова програмування, яка проста у вивченні. Він має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис і динамічна типізація Python разом з його інтерпретованим характером роблять його ідеальною мовою для створення сценаріїв і швидкої розробки додатків у багатьох сферах на більшості платформ.

Інтерпретатор Python і обширна стандартна бібліотека доступні у вихідному або двійковому вигляді для всіх основних платформ на веб-сайті Python <https://www.python.org/> і можуть вільно поширюватися. Цей же сайт також

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

містить дистрибутиви та вказівники на багато безкоштовних сторонніх модулів Python, програм і інструментів, а також додаткову документацію.

Інтерпретатор Python легко розширюється за допомогою нових функцій і типів даних, реалізованих у C або C++ (або інших мовах, які можна викликати з C). Python також підходить як мова розширення для налаштовуваних програм.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

В процесі розробки випускної кваліфікаційної роботи за першим (бакалаврським) 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;

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

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) сформулювати висновки про виконаний обсяг робіт та одержані результати.

К6ПЗ_2026

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Як периферійні обчислення змінюють центр обробки даних

Найбільша зміна в тому, що ми завжди розуміли як центр обробки даних, є концептуальною. Центри обробки даних більше не є централізованими «скляними будинками», що розташовані десь у штаб-квартирі. Натомість, центри обробки даних стають аморфними утвореннями, що охоплюють традиційні центри обробки даних, численні хмари та ланцюг мікроцентрів обробки даних на віддалених периферійних сайтах.

Для реалізації цієї концепції розширеного центру обробки даних ІТ-відділ повинен:

1. Встановить сервери, стійки для зберігання даних та мережеве обладнання в кожному периферійному мікроцентрі обробки даних.
2. Перемістити інші ІТ-активи (наприклад, програмне забезпечення, засоби зв'язку, обладнання для резервного копіювання) на віддалені периферійні сайти, щоб вони могли працювати незалежно, але з дотриманням правил та безпекою.

Існує три сфери викликів, з якими ІТ-відділ має зіткнутися під час реструктуризації центрів обробки даних:

Прогалини у стандартизації Інтернету речей: основним компонентом розгортання периферійних мереж є апаратне забезпечення у вигляді серверів, мережевого обладнання, стійок для зберігання даних, а також датчиків і пристроїв Інтернету речей. ІТ-відділам складно підтримувати всі ці компоненти як частину глобального корпоративного центру обробки даних, якщо немає встановлених спеціальних стандартів для придбаного обладнання та операційних систем.

У цьому сценарії централізовані закупівлі стають ключовим гравцем, як і

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

повне схвалення політики стандартизації обладнання та ОС генеральним директором та іншими керівниками рівня вищої ланки. Слід уникати тенденції цивільних ІТ-користувачів самостійно купувати обладнання, несумісне з ІТ-інфраструктурою підприємства.

Стандартизацію необхідно особливо суворо застосовувати до телефонів, планшетів, зчитувачів RFID (радіочастотної ідентифікації), датчиків та інших пристроїв Інтернету речей. Саме Інтернет речей становить найбільший ризик для несумісності та підтримки ІТ, оскільки постачальники в цій сфері часто використовують власні операційні системи та надають мало або взагалі не надають підтримки продуктів.

Узгодженість контейнерів між сайтами: Програмне забезпечення, якщо його мініатюризувати та розповсюджувати по мікроцентрах обробки даних, має залишатися сумісним по всьому підприємству. На кожному периферійному місці ІТ-відділ надає контейнеризовані «мікросистеми» операційних систем, компонентів ІТ-інфраструктури та програм. Однак, коли відбувається зміна базового компонента ІТ-інфраструктури, операційної системи чи програми, ця зміна має бути однаково встановлена на всіх контейнерах, що використовуються на периферії, щоб підтримувати сумісність підприємства. Це робить ІТ-відділ.

Нульова довіра та мережі ідентифікації: у 2025 році 60% порушень безпеки підприємств були результатом людської діяльності, згідно зі звітом DeepStrike «Людський злом: статистика, тенденції та майбутні загрози соціальної інженерії за 2025 рік». Внутрішні користувачі продовжують ставати жертвами фішингових атак, коли вони відкривають вкладення в шахрайських електронних листах, які виглядають як від законної особи, а тепер, завдяки штучному інтелекту, зростає кількість відео з дідфейками та телефонних дзвінків.

Відділи кадрів та ІТ підприємств знають про це та навчають користувачів протоколам корпоративної безпеки, але кіберзлочинці також хитрі. Ці зловмисники знають, що область атак на безпеку розширилася зі зростанням мікроцентрів обробки даних на периферії та широким використанням вразливих

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

до безпеки пристроїв Інтернету речей.

Компанії реагують, інвестуючи в мережі з нульовою довірою, про що свідчить очікуване зростання ринку мереж з нульовою довірою в США до 4,18 мільярда доларів до 2030 року з 1,34 мільярда доларів (складений річний темп зростання 25%).

Мережі з нульовою довірою дозволяють ІТ-фахівцям спостерігати за будь-якими ІТ-активами, які додаються, видаляються або змінюються в мережах будь-де, і вони є незамінною технологією, якщо ІТ-фахівці мають контролювати всі ІТ, незалежно від того, де вони знаходяться.

Не менш важливим є забезпечення належних посвідчень користувачів та їх авторизації для мережевих ресурсів, які вони використовують. Окремий користувач може переходити з одного периферійного центру до іншого та мати різні рівні авторизації доступу на кожному периферійному сайті.

Існують технології, які відстежують ідентифікаційні дані та дії користувачів в ІТ-мережах. Для мереж центрів обробки даних для відстеження користувачів використовується програмне забезпечення для керування доступом до ідентифікаційних даних. У хмарі ту саму функцію відстеження користувачів виконує програмне забезпечення для керування правами доступу до хмарної інфраструктури. На жаль, ці два рішення функціонують незалежно одне від одного. Щоб об'єднати їх усі в одному пакеті, необхідно використовувати комплексне програмне забезпечення, таке як управління та адміністрування ідентифікаційних даних, яке може забезпечити загальну структуру.

Економіка реструктуризації

Концепція центру обробки даних змінюється від центрального скляного будинку до широко розподіленої ІТ-парасольки, яка охоплює периферійні сайти, хмари та традиційний центр обробки даних. Ця реструктуризація центру обробки даних також змусить ІТ-відділ реструктуризувати способи розгортання, обслуговування та захисту ІТ-активів.

Для ІТ-директорів та менеджерів центрів обробки даних реструктуризація

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

центрів обробки даних призведе до витрат у таких сферах, як мережі з нульовою довірою та безпека, а з боку додатків та ІТ-інфраструктури ми побачимо більше контейнеризації.

Разом ці тенденції змусять ІТ-відділи впроваджувати нові способи розгортання, обслуговування та безпеки ІТ-активів, оскільки від ІТ-відділів все ще очікуватиметься виконання всього цього.

3.2 Розробка структурної схеми

Нижче наведемо вісім тенденцій, які змінюють інфраструктуру центрів обробки даних, і чому вони важливі для вашого планування на 2026 рік.

1. Проектування центрів обробки даних, орієнтованих на штучний інтелект

Це головне. Об'єкти, орієнтовані на штучний інтелект, зі стійками з великою кількістю графічних процесорів та прискорювачів стають основною ціллю проектування, а не нішевим робочим навантаженням. Ми вже пройшли фазу «пілотного проекту зі штучним інтелектом». Зараз організації проектують цілі об'єкти навколо навчальних кластерів та високооб'ємного логічного виводу.

Цей зсув призводить до змін усюди: розподіл електроенергії, топологія мережі, архітектура сховищ. Центр обробки даних, який був побудований для традиційних корпоративних навантажень п'ять років тому, не був розроблений з урахуванням цього. Якщо ваша стратегія об'єкта досі розглядає штучний інтелект як ще одне робоче навантаження, ви плануєте світ, якого більше не існує.

2. Висока щільність живлення та вдосконалене охолодження

Традиційні стійки центрів обробки даних споживають від 7 до 15 кВт. Саме на це було розроблено більшість установ. Кластери для навчання штучного інтелекту? Йдеться про 40-100+ кВт на стійку. Деякі конфігурації з високою щільністю графічних процесорів мають ще більшу потужність.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

Це не поступова зміна. Це фундаментальне переосмислення розподілу електроенергії та управління температурою. Не можна просто замінити кілька нових серверів. Сама будівля не була побудована для цього.

Що я бачу в цій галузі: рідинне охолодження пройшло шлях від «цікава технологія, яку ми оцінюємо» до «як швидко ми можемо це впровадити?». Безпосередньо охолодження чіпів, теплообмінники із задніми дверцятами, навіть повноцінне занурення в охолодження переходять від пілотних проектів до виробництва. Виробничі потужності перепроєктуються з урахуванням більш потужного розподілу електроенергії та нових теплових оболонок. Якщо дорожня карта вашого об'єкта не включає стратегію рідинного охолодження, ви вже відстаєте.

3. Високошвидкісні мережі наступного покоління

400G стає головним пріоритетом. Розгортання 800G прискорюється. А перші комутатори 1.6T з'являться в середовищах штучного інтелекту та високопродуктивних обчислень, починаючи з 2026 року.

Але ось що люди не помічають у зміні мереж: справа не лише у вищих швидкостях між стійками. Робочі навантаження ІІІ генерують зовсім іншу схему трафіку. Традиційний північно-південний трафік (користувачі звертаються до серверів) поступається східно-західному трафіку (сервери спілкуються один з одним під час навчальних запусків). Архітектури листового хребта, які добре працювали для веб-застосунків, потребують серйозного переосмислення для розподілених робочих навантажень ІІІ.

Оптика та роз'єми з більшою щільністю всюди. Якщо ви плануєте оновлення, врахуйте, що мережевий рівень може потребувати такої ж уваги, як і обчислювальний рівень.

4. Операції, керовані штучним інтелектом, та цифрові двійники

Роками цифрові двійники інфраструктури центрів обробки даних здавалися приємним доповненням. Саме це й зробили гіперскейлери. Це швидко змінюється.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

Коли ви використовуєте стійки потужністю понад 50 кВт з контурами рідинного охолодження та робочими навантаженнями штучного інтелекту, які можуть непередбачувано зростати, вам потрібно моделювати зміни, перш ніж їх вносити. Оператори використовують машинне навчання для оптимізації охолодження та живлення в режимі реального часу, прогнозування збоїв та планування розгортання високої щільності без дорогих несподіванок.

Все більше об'єктів створюють цифрових двійників систем живлення, охолодження та ІТ, щоб імітувати зміни перед їх впровадженням. Ця можливість стає важливою, а не обов'язковою, для тих, хто керує серйозною інфраструктурою штучного інтелекту.

5. Сталий розвиток, енергетична стратегія та інтеграція з мережею

Кожне підприємство, з яким я спілкуюся, має цілі щодо викидів вуглецю. Більшість із них взяли на себе публічні зобов'язання. Ось у чому полягає суперечність: інфраструктура штучного інтелекту неймовірно енергоємна, і є зацікавлені сторони, які вимагають як можливостей штучного інтелекту, так і скорочення викидів.

Відповідь стає дедалі складнішою, ніж просто «купувати кредити на відновлювану енергію». Розумні оператори прагнуть укласти прямі угоди про купівлю електроенергії з відновлюваних джерел, генерувати енергію на місці та накопичувати її. Але справді цікавий зсув відбувається в бік «інтерактивних мережевих» об'єктів, які можуть брати участь у реагуванні на попит, масштабувати робочі навантаження на основі вуглецевої інтенсивності мережі та демонструвати перевірені показники ефективності.

Це не просто екологічна відповідальність. Це дедалі частіше стає вимогою закупівель. Запити пропозицій ставлять складніші питання щодо сталого розвитку, і фраза «ми над цим працюємо» вже не є достатньою.

6. Розширення периферії та гібридні обчислення

Пам'ятаєте рух "все перенесено в публічну хмару"? А потім контррух "репатріації"?

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

Насправді ситуація дещо складніша. Гібридна модель, що поєднує гіпермасштабовану хмару, колокейшн та локальну інфраструктуру, закріпилася як архітектура, що має сенс для більшості підприємств. Центри обробки даних на периферії масштабуються для використання з низькою затримкою, таких як Інтернет речей, 5G та автономні системи, тоді як основні сайти займаються інтенсивним навчанням та агрегацією ШІ.

Тенденція до повернення хмарних ресурсів реальна, але цілеспрямована. Організації скорочують певні робочі навантаження, де витрати або контроль мають сенс, не відмовляючись від хмарних ресурсів повністю. Розумний підхід полягає в розміщенні ресурсів відповідно до робочого навантаження, а не в релігійному дотриманні якоїсь єдиної моделі.

7. Модульна, швидша у розгортанні інфраструктура

Ось тенденція, якій не приділяється достатньо уваги: підприємства, які перемагають у розвитку інфраструктури штучного інтелекту, – це ті, хто може найшвидше розгорнути потужності.

Модульні, збірні зали обробки даних та блоки живлення/охолодження стають рішенням. Коли попит на технології, що базуються на штучному інтелекті, не можна чекати від 18 до 24 місяців на традиційне будівництво. В середині приміщень модульні високощільні підключення та блоки шаф дозволяють операторам швидко змінювати конфігурацію макетів у міру зміни поколінь обладнання. А вони змінюються швидко.

Якщо ваша інфраструктурна стратегія передбачає стабільне, передбачуване зростання, ви плануєте світ, якого більше не існує.

8. Консолідоване управління та зрілий DCIM

Платформи DCIM нарешті стали корисними. Платформи другого покоління стають справжньою єдиною скляною панеллю, яка об'єднує живлення, охолодження, IT-ресурси, хмарні ресурси та системи продажу квитків.

Таке консолідоване представлення даних є критично важливим для точного планування потужностей, управління кількома сайтами та звітності про

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

відповідність вимогам у гібридних середовищах з високим вмістом штучного інтелекту. Якщо ви досі використовуєте окремі системи для кожного з них, ви створюєте сліпі зони саме там, де не можете собі їх дозволити.

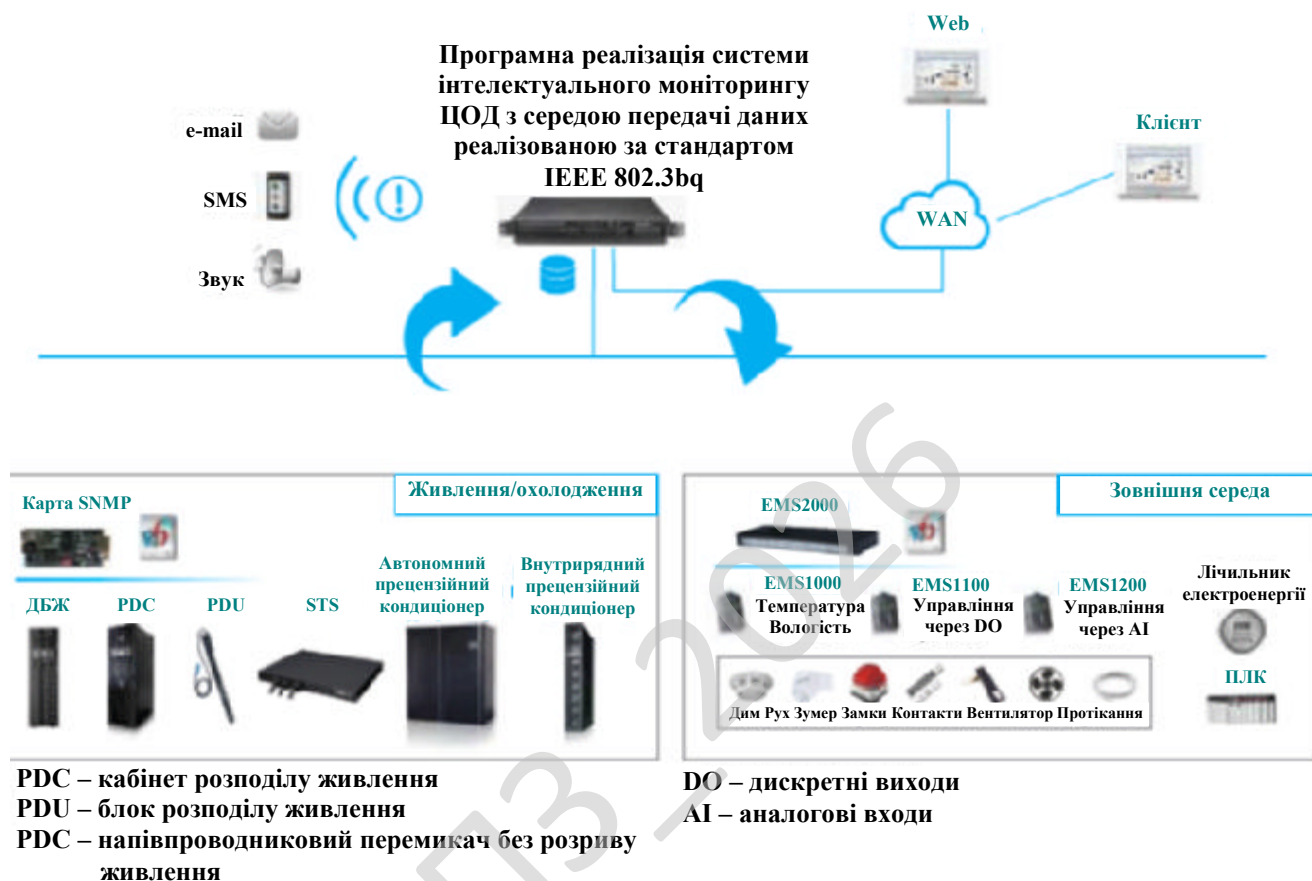


Рисунок 3.1 – Структурна схема системи

Моніторинг мережі більше не є простим процесом на серверній частині, а основою продуктивності та надійності мережі в сучасному багатогранному ІТ-ландшафті. Оскільки мережі поширюються на локальні, хмарні та гібридні середовища, сфера моніторингу значно розширюється.

Ефективний моніторинг мережі тепер означає забезпечення її справності, максимізацію часу безвідмовної роботи та швидке вирішення таких проблем, як втрата пакетів, до їх загострення.

З появою нових технологій та зростанням вимог, ця дисципліна продовжує адаптуватися, що робить життєво важливим для організацій бути в курсі останніх досягнень.

Моніторинг мережі та його важливість у сучасному складному ІТ-ландшафті

Мережевий моніторинг стосується постійного спостереження та аналізу мережевої інфраструктури, яка включає всі підключені мережеві пристрої, потоки даних та залежності мережевих даних.

Цей процес моніторингу є критично важливим для сучасних мереж, особливо враховуючи, що організації все більше покладаються на складні топології та хмарні сервіси. Він забезпечує видимість мережевого трафіку, продуктивності програм та використання ресурсів, дозволяючи мережевим адміністраторам контролювати та підтримувати доступність мережі.

Сучасні організації залежать від надійного підключення для ведення бізнесу, що робить управління мережею стратегічним пріоритетом. Збій у мережі може призвести до дорогого простою, втрати продуктивності та навіть репутаційної шкоди.

Згідно з галузевими даними, лише одна година простою може коштувати великим підприємствам понад 300 000 доларів. Проактивний моніторинг мережі дозволяє виявляти проблеми з мережею на ранній стадії та надає дієву інформацію, яка допомагає запобігти збоям.

Використовуючи передове програмне забезпечення для моніторингу мережі, ІТ-команди можуть оптимізувати продуктивність мережі, покращити моніторинг продуктивності програм, підтримувати ефективний потік даних та забезпечувати безперервне надання послуг. Отже, що таке моніторинг мережі та чому він важливий? Це ключ до підтримки стійкої та високопродуктивної мережевої інфраструктури для будь-якої сучасної організації.

2026 рік сигналізує про значні зміни в мережевому моніторингу, оскільки майбутні тенденції формують те, як ІТ-фахівці керують продуктивністю та

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

безпекою. Програмне забезпечення для моніторингу швидко інтегрує нові інструменти для забезпечення видимості в режимі реального часу та розширеної аналітики в традиційних, хмарних та гібридних середовищах. Оскільки організації впроваджують хмарні сервіси у великих масштабах, потреба в єдиному управлінні продуктивністю стає все більш критичною.

Поява рішень на основі штучного інтелекту, автоматизації та моделей машинного навчання переосмислює методи виявлення та усунення аномалій. Ці досягнення дозволяють отримувати проактивне розуміння продуктивності, автоматизоване виправлення та прогнозне оповіщення – все це надзвичайно важливо для управління дедалі складнішими мережами. ІТ-команди повинні бути в курсі цих тенденцій, щоб мати змогу вирішувати нові проблеми та підтримувати безперебійну роботу.

З огляду на зростання популярності гібридних ІТ, ІТ-фахівцям слід готуватися до майбутнього, впроваджуючи системи моніторингу, які надають комплексну аналітику в режимі реального часу та використовують автоматизацію для зменшення ручного навантаження. Тенденції, що формують 2026 рік, обіцяють не лише кращу продуктивність, але й більш стійке та адаптивне ІТ-середовище.

Зростання штучного інтелекту та машинного навчання в мережевому моніторингу

Значні досягнення у сфері штучного інтелекту та машинного навчання змінюють методи моніторингу мережі, дозволяючи ІТ-командам проактивно вирішувати проблеми продуктивності. Ці технології сприяють автоматизованому аналізу першопричин, надаючи інформацію про продуктивність мережі та моделі трафіку, що раніше було неможливо.

Удосконалене програмне забезпечення для моніторингу використовує історичні дані та аналітику в режимі реального часу для оптимізації стану мережі, забезпечуючи безперебійну взаємодію з користувачами в різних середовищах. Завдяки налаштовуваним інформаційним панелям ці рішення дозволяють

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

мережевим адміністраторам фіксувати критичні показники продуктивності, що зрештою підвищує операційну ефективність у складних інфраструктурах.

Прогнозна аналітика та виявлення аномалій

Штучний інтелект та машинне навчання відкривають шлях для прогнозної аналітики в моніторингу продуктивності. Аналізуючи величезні обсяги історичних даних та даних у реальному часі, ці технології вивчають, як виглядає «норма» для продуктивності мережі. Коли моделі трафіку або продуктивність програм відхиляються від цих базових значень, алгоритми виявлення аномалій миттєво попереджають ІТ-фахівців про потенційні проблеми.

Такий підхід означає, що моніторинг мережі більше не є реактивним, а передбачає проблеми до їх загострення. Прогнозна аналітика сприяє ранньому втручанню, зменшуючи час простою та підтримуючи безперервність бізнесу. Наприклад, якщо програмне забезпечення для моніторингу виявляє незвичне зростання мережевого трафіку, воно може запропонувати цілеспрямовані дії для запобігання вузьким місцям.

Вплив цих досягнень виходить за рамки простого оповіщення. Машинне навчання постійно вдосконалює своє розуміння динаміки мережі, роблячи майбутні висновки ще точнішими. Як результат, моніторинг продуктивності мережі стає стратегічним активом, що дозволяє організаціям випереджати збої та підтримувати оптимальний рівень обслуговування.

Автоматизований аналіз та усунення першопричин

Ефективне вирішення мережевих проблем значною мірою залежить від автоматизованого аналізу та усунення першопричин. Використовуючи передові алгоритми машинного навчання, ці системи можуть аналізувати історичні дані, щоб виявити закономірності та точно визначити джерело зниження продуктивності.

Завдяки оптимізації процесу діагностики, ІТ-команди отримують можливість швидко реагувати на аномалії мережевого трафіку та проблеми з продуктивністю програм, що значно покращує стан мережі. Такий проактивний

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

підхід не лише зменшує час простою, але й покращує загальний користувацький досвід, що робить його важливою функцією сучасних рішень для моніторингу мережі.

Посилена безпека

Сучасний мережевий моніторинг тепер інтегрує потужні можливості моніторингу безпеки, що робить виявлення загроз основною функцією. Сучасне програмне забезпечення для моніторингу постійно сканує мережеву активність на предмет незвичайної поведінки, швидко виявляючи ознаки потенційних порушень, витоку даних або несанкціонованого доступу. Співвідносячи моделі трафіку з відомими індикаторами загроз, ці системи допомагають захищати мережеву безпеку з кількох фронтів.

Оскільки кіберзагрози стають дедалі складнішими, інтегрований моніторинг безпеки є надзвичайно важливим. Автоматизоване оповіщення та поглиблений аналіз аномалій дозволяють ІТ-командам швидко реагувати на нові ризики. Наприклад, сплеск вихідного трафіку з певного пристрою може сигналізувати про компрометацію кінцевої точки, що спонукатиме до негайного розслідування.

Поєднання моніторингу продуктивності з розширеними функціями безпеки означає, що організаціям більше не потрібні окремі інструменти для забезпечення справності та безпеки мережі. Такий цілісний підхід підвищує стійкість усіх компонентів мережі, допомагає підтримувати відповідність вимогам та зменшує ризик дороговартісних інцидентів безпеки.

Зміна архітектур та парадигм моніторингу

Архітектура мережі розвивається, як і очікування від сучасної системи моніторингу. Оскільки організації переходять до хмарних середовищ та гібридних інфраструктур, вимоги до моніторингу стають складнішими та динамічнішими.

Традиційні локальні рішення замінюються гнучкими інструментами, що адаптуються до хмарних та багатохмарних налаштувань. Ці зміни вимагають

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

стратегій моніторингу, які можуть безперешкодно інтегруватися в розподілені середовища, забезпечувати видимість мережі та надавати узгоджені дані про продуктивність незалежно від того, де знаходяться програми та ресурси.

Хмарний та гібридний/багатохмарний моніторинг

Моніторинг хмарних, гібридних та мультихмарних середовищ створює унікальні труднощі для ІТ-фахівців. На відміну від традиційних мереж, ці середовища охоплюють локальні центри обробки даних, публічні хмарні платформи та приватні хмари, кожна з яких має свої дані про продуктивність та вимоги до програмного забезпечення для моніторингу. Забезпечення безперебійної видимості мережі в усіх компонентах є головним пріоритетом.

Одним із головних викликів є інтеграція різнорідних систем моніторингу та джерел даних. Дані про продуктивність мають бути нормалізовані та візуалізовані на єдиних інформаційних панелях, що дозволить ІТ-командам швидко виявляти проблеми незалежно від їхнього походження. Крім того, програмне забезпечення для моніторингу має адаптуватися до швидких змін у розподілі ресурсів, масштабі та підключенні, характерних для гібридних середовищ.

Ще однією перешкодою є потреба в налаштовуваних інформаційних панелях та інструментах мережевого картографування, які надають аналітику в режимі реального часу як хмарних, так і локальних компонентів. Подолання цих проблем вимагає передових рішень для моніторингу, здатних усувати розриви між середовищами, забезпечуючи оптимальну справність мережі та продуктивність програм.

Моніторинг периферійних обчислень та Інтернету речей

Досягнення в периферійних обчисленнях та моніторингу Інтернету речей революціонізують управління мережами. Ці технології пропонують обробку даних у режимі реального часу ближче до джерела даних, що значно скорочує час відгуку та підвищує загальну продуктивність мережі.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

Розгортаючи системи моніторингу, що використовують алгоритми машинного навчання, організації можуть отримувати уявлення про моделі трафіку та виявляти потенційне зниження продуктивності в розподілених середовищах.

Ефективне керування мережевими пристроями має вирішальне значення для підтримки взаємодії з користувачем, оскільки пристрої Інтернету речей генерують величезні обсяги мережевого трафіку, що вимагає надійних рішень для моніторингу продуктивності для забезпечення оптимального стану мережі.

Мережа як послуга (NaaS) та програмно-визначені мережі (SDN)

Інтеграція мережі як послуги (NaaS) та програмно-визначених мереж (SDN) революціонує спосіб управління продуктивністю мережі в організаціях. Використовуючи хмарні сервіси, компанії можуть динамічно налаштовувати пропускну здатність та засоби керування доступом, оптимізуючи доступність та продуктивність мережі.

NaaS забезпечує масштабовані рішення, тоді як SDN покращує видимість мережі завдяки аналізу трафіку в режимі реального часу та моніторингу продуктивності. Разом вони забезпечують налаштовувані панелі інструментів, які дозволяють ІТ-командам проактивно вирішувати проблеми з мережею. Ця синергія не лише оптимізує управління мережею, але й покращує взаємодію з користувачем, забезпечуючи ефективний потік даних у різних середовищах.

Комплексна спостережуваність проти традиційного моніторингу

Спостережуваність переосмислює підхід організацій до моніторингу мережі. Замість того, щоб зосереджуватися виключно на метриках продуктивності, сучасні системи моніторингу тепер інтегрують журнали, трасування та дані про потоки. Ця еволюція забезпечує глибоку видимість мережі та практичну аналітику в різноманітній ІТ-інфраструктурі.

Традиційний моніторинг, з його обмеженим обсягом, часто не враховує складні взаємозалежності та ледь помітні аномалії, які можуть впливати на продуктивність. Завдяки впровадженню комплексної спостережливості, ІТ-

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

команди отримують цілісне розуміння стану мережі, продуктивності програм та взаємодії з користувачем, що дозволяє їм проактивно керувати та швидше вирішувати проблеми.

За межами метрик: інтеграція інструментів моніторингу мережі

Спостережуваність у мережевому моніторингу означає вихід далеко за рамки простих показників продуктивності. Комплексні системи моніторингу тепер збирають та співвідносять журнали, трасування та дані про потоки, щоб забезпечити повну видимість мережі. Такий підхід дозволяє ІТ-фахівцям зрозуміти не лише те, що щось пішло не так, але й точно де і чому.

Журнали фіксують детальні події, такі як зміни конфігурації або інциденти безпеки. Трасування відстежує шлях пакетів даних мережею, виявляючи затримку або проблеми з підключенням.

Дані потоку аналізують моделі трафіку та споживання пропускну здатності, допомагаючи точно визначити вузькі місця та потенційні загрози. Коли ці джерела даних об'єднуються, програмне забезпечення для моніторингу може реконструювати інциденти та виявляти першопричини набагато ефективніше, ніж традиційні інструменти.

Моніторинг цифрового досвіду (DEM)

Моніторинг цифрового досвіду (DEM) підкреслює важливість розуміння поведінки користувачів у різних програмах та мережах. Використовуючи передові інструменти моніторингу мережі, організації можуть отримати уявлення про продуктивність програм та взаємодію з користувачами, забезпечуючи оптимальну реакцію. Цей проактивний підхід виявляє потенційні проблеми в усій мережевій інфраструктурі, дозволяючи ІТ-командам покращувати надання послуг. Завдяки налаштовуваним інформаційним панелям DEM спрощує аналіз мережевого трафіку в режимі реального часу, що дозволяє ефективно відстежувати показники продуктивності. Оскільки бізнес все більше покладається на цифрове середовище, безперешкодна інтеграція DEM в управління мережею стає важливою для підтримки надійного стану мережі.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

Автоматизація та оркестрація: переосмислення моніторингу в режимі реального часу

Автоматизація та оркестрація стають основою сучасних ІТ-операцій. Автоматизуючи рутинні завдання моніторингу та оркеструючи складні робочі процеси, організації можуть підвищити ефективність, зменшити ручне навантаження та реагувати на проблеми з мережею з безпрецедентною швидкістю.

Ці технології дозволяють програмному забезпеченню для моніторингу обробляти все: від управління продуктивністю до моніторингу серверів та реагування на інциденти, що звільняє ІТ-фахівців від необхідності зосереджуватися на більш цінних ініціативах. Зі зростанням складності мереж автоматизація та оркестрація забезпечують гнучкість, масштабованість та стійкість операцій.

Автоматизація рутинних завдань моніторингу

Автоматизація рутинних завдань моніторингу є важливою для ефективного управління продуктивністю. Сучасне програмне забезпечення для моніторингу тепер обробляє повторювані перевірки, сповіщення на основі порогових значень та стандартні виправлення без ручного контролю. Цей перехід дозволяє ІТ-командам витрачати менше часу на моніторинг серверів і більше часу на стратегічні інновації.

Найкращі практики моніторингу продуктивності корпоративних мереж у 2025 році включають використання автоматизації для зменшення людських помилок та стандартизації відповідей.

Наприклад, інструменти моніторингу можуть автоматично перезапускати служби, переналаштовувати пристрої або ескалювати проблеми на основі попередньо встановлених критеріїв. Налаштовувані робочі процеси розширюють автоматизацію відповідно до індивідуальних потреб бізнесу, забезпечуючи послідовне дотримання операційних політик.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		39

Мережа на основі намірів (IBN) та моніторинг

Мережі на основі намірів (IBN) – це революційний підхід, який інтегрує розширені політики в системи моніторингу мережі. Цей метод використовує алгоритми машинного навчання для аналізу показників продуктивності та динамічного налаштування конфігурацій мережі.

Зосереджуючись на поведінці користувачів та моделях трафіку, IBN підвищує продуктивність мережі та зменшує її зниження.

Це надає IT-командам можливість контролювати стан мережі в режимі реального часу та автоматично реагувати на неї, забезпечуючи оптимальний стан мережі. Завдяки налаштовуваним інформаційним панелям та покращеній доступності мережі, застосування IBN для моніторингу спрощує управління мережею, зрештою покращуючи взаємодію з користувачами в хмарних середовищах та сучасних мережах.

Інтеграція кібербезпеки в мережевий моніторинг

Кібербезпека тепер невіддільна від моніторингу мережі. Сучасне програмне забезпечення для моніторингу інтегрує розширений моніторинг безпеки для виявлення, розслідування та реагування на загрози в усій інфраструктурі. Аналіз мережевого трафіку, поведінки програм та активності пристроїв у режимі реального часу дозволяє командам швидко виявляти вразливості та порушення.

Оскільки організації надають пріоритет мережевій безпеці та відповідності вимогам, системи моніторингу повинні забезпечувати постійну перевірку дотримання політик та надавати практичну інформацію для захисту конфіденційних даних у режимі реального часу. Така тісна інтеграція є критично важливою в сучасному динамічному середовищі загроз.

Архітектура нульової довіри та безперервна перевірка

Нульова довіра – це модель безпеки, яка передбачає, що жоден користувач чи пристрій не є надійним за своєю суттю, навіть у корпоративній мережі. У мережевому моніторингу нульова довіра вимагає постійної перевірки всіх

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

доступів та активності, забезпечуючи суворе дотримання політик на кожному рівні.

Програмне забезпечення для моніторингу відіграє центральну роль у цій архітектурі. Воно забезпечує видимість мережевої безпеки в режимі реального часу, відстежує поведінку користувачів та виявляє будь-які відхилення від встановлених політик.

Така постійна пильність дозволяє організаціям швидко виявляти несанкціонований доступ або горизонтальне переміщення, зменшуючи вікно можливостей для кіберзагроз.

SASE (Secure Access Service Edge) та уніфіковані платформи безпеки

Конвергенція SASE та уніфікованих платформ безпеки революціонізує управління мережею. Інтегруючи функції безпеки безпосередньо в рівень доступу, організації можуть досягти повної видимості мережевого трафіку та продуктивності програм. Ця синергія покращує взаємодію з користувачем, одночасно спрощуючи виявлення загроз та реагування на них.

Завдяки системам моніторингу в режимі реального часу ІТ-команди мають можливість проактивно вирішувати потенційні проблеми безпеки, оптимізуючи використання пропускну здатності та покращуючи загальний стан мережі.

Крім того, масштабовані хмарні інфраструктури забезпечують безперебійне управління в розподілених середовищах, що робить SASE важливим компонентом сучасних мережевих стратегій.

Реагування на кіберзагрози, що розвиваються

Ландшафт кіберзагроз постійно змінюється, що спонукає організації адаптувати свої стратегії моніторингу безпеки. Сучасне програмне забезпечення для моніторингу повинно йти в ногу з часом, надаючи комплексну аналітику стану мережі, даних про продуктивність та підозрілу активність у режимі реального часу.

Автоматизовані сповіщення та виявлення аномалій допомагають ІТ-командам швидко виявляти нові загрози. Інтеграція з каналами інформації про

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

загрози та поведінковою аналітикою ще більше розширює можливості виявлення складних атак, таких як програми-вимагачі або внутрішні загрози.

Системи моніторингу також відіграють вирішальну роль у дотриманні вимог, зберігаючи журнали та докази для судово-медичної експертизи та перевірки регуляторними органами.

Рішення для хмарного та гібридного моніторингу мереж

Оскільки організації розгортають додатки в хмарних та гібридних середовищах, рішення для моніторингу повинні розвиватися, щоб забезпечувати послідовну аналітику в режимі реального часу.

Сучасне програмне забезпечення для моніторингу усуває розрив між застарілими системами та динамічними хмарними ресурсами. Ці рішення пропонують уніфіковані панелі інструментів, мережеве картографування та налаштовувані сповіщення, адаптовані для розподілених інфраструктур.

Незалежно від того, чи йдеться про керування даними про продуктивність у хмарі, чи про підтримку видимості в гібридних мережах, правильне рішення для моніторингу є важливим для максимізації часу безвідмовної роботи, оптимізації використання ресурсів та безпеки цифрових операцій.

Адаптація до мультихмарних та гібридних середовищ

Керування продуктивністю мережі в багатохмарних та гібридних середовищах є складним процесом. Рішення для моніторингу повинні інтегруватися з кількома платформами, нормалізувати дані про продуктивність та представляти практичну інформацію в єдиному, уніфікованому вигляді.

Такий підхід дозволяє IT-командам орієнтуватися в умовах мінливих робочих навантажень, оптимізувати розподіл ресурсів та швидко виявляти мережеві проблеми в різних інфраструктурах.

Ключовою стратегією є використання інструментів мережевого картографування, які візуалізують зв'язки між локальними, хмарними та віддаленими ресурсами. Налаштовувані інформаційні панелі об'єднують

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

аналітику в режимі реального часу, що дозволяє легко виявляти аномалії або погіршення роботи.

Удосконалене програмне забезпечення для моніторингу підтримує безперебійний перехід між середовищами, забезпечуючи безперервне надання послуг.

Захист розподілених робочих сил за допомогою хмарного моніторингу

Моніторинг хмарних технологій є критично важливим для захисту розподілених працівників, забезпечуючи прозорість і контроль, необхідні для управління мережевою безпекою та віддаленим доступом для глобальних команд. Оскільки співробітники працюють з різних місць, ІТ-команди стикаються з унікальними викликами:

- Моніторинг віддалених з'єднань на наявність незвичайної активності або спроб несанкціонованого доступу.
- Захист конфіденційних даних за допомогою шифрованого мережевого трафіку та безпечної автентифікації.
- Забезпечення послідовного застосування політик на особистих та корпоративних пристроях.
- Швидке виявлення та вирішення проблем продуктивності, що впливають на віддалених користувачів.

Сучасне програмне забезпечення для моніторингу інтегрується з хмарною інфраструктурою, щоб забезпечити картографування мережі в режимі реального часу, налаштовувані сповіщення та комплексний моніторинг безпеки. Це гарантує організаціям підтримку справності мережі та відповідності вимогам, незалежно від того, де підключаються співробітники.

Забігаючи наперед, до 2026 року, організації повинні надавати пріоритет адаптивності, автоматизації та комплексній аналітиці у своїх стратегіях моніторингу мережі.

З огляду на швидкі темпи технологічних змін, рішення для моніторингу повинні враховувати майбутні тенденції в управлінні мережами, такі як аналітика

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

на основі штучного інтелекту, розширений моніторинг безпеки та підтримка багатохмарних розгортань.

Вибір інструментів, які усувають прогалини в навичках, оптимізують витрати та відповідають бізнес-цілям, є надзвичайно важливим. Ці міркування допоможуть ІТ-фахівцям максимізувати продуктивність мережі та випереджати нові виклики.

Розрив у навичках та ШІ-копілоти

Нові тенденції підкреслюють дефіцит навичок в ІТ-командах, особливо в управлінні мережами та їхніх можливостях моніторингу. Оскільки продуктивність мережі стає дедалі складнішою, команди зі штучним інтелектом стають важливими для подолання цього розриву.

Ці інтелектуальні інструменти підвищують операційну ефективність, автоматизуючи виснажливі завдання, такі як аналіз першопричин та моніторинг продуктивності.

Завдяки аналітиці на основі штучного інтелекту команди можуть зосередитися на стратегічних ініціативах, а не зациклюватися на проблемах продуктивності, забезпечуючи покращення стану мережі. З розвитком технологій співпраця між ІТ-фахівцями та штучним інтелектом забезпечить оптимальну продуктивність мережі.

Оптимізація витрат та рентабельність інвестицій

Оптимізація витрат є ключовим питанням під час оцінки програмного забезпечення для моніторингу мережі. Організації повинні враховувати загальну вартість володіння – не лише ліцензійні збори, але й витрати на впровадження, обслуговування та навчання. Рішення, що забезпечують надійні показники продуктивності та автоматизацію, можуть знизити експлуатаційні витрати, зменшуючи час простою та ручне втручання.

Оцінюючи рентабельність інвестицій (ROI), зосередьтеся на впливі швидшого вирішення проблем, покращення часу безвідмовної роботи та зменшення кількості інцидентів безпеки.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

Розширені інструменти моніторингу пропонують налаштовувані інформаційні панелі та автоматизовану звітність, що оптимізує зусилля з управління дотриманням вимог та ефективністю.

Короткий зміст ціннісної пропозиції

Моніторинг мережі пропонує переконливу ціннісну пропозицію для організацій, які інвестують у ІТ-операції наступного покоління.

Забезпечуючи повну видимість, проактивне покращення продуктивності та виявлення загроз на основі штучного інтелекту, ці системи зменшують час простою та експлуатаційні витрати.

Ключові переваги включають покращене планування потужностей, стратегічне узгодження з бізнес-цілями та підвищену гнучкість у гібридних середовищах.

Завдяки автоматизації та штучному інтелекту, що надає ІТ-командам можливості, рішення для моніторингу мережі допомагають організаціям випереджати виклики та створювати стійкі, масштабовані та безпечні інфраструктури.

Покращена продуктивність завдяки проактивному та прогнозному моніторингу

Акцент на проактивних та прогнозних механізмах моніторингу змінює спосіб управління продуктивністю мережі. Аналіз історичних даних та використання алгоритмів машинного навчання допомагає виявляти моделі трафіку та потенційні проблеми, перш ніж вони переростуть у серйозні мережеві проблеми.

Таке передбачення дозволяє ІТ-командам оптимізувати розподіл ресурсів та підвищити продуктивність додатків.

Налаштовувані інформаційні панелі надають аналітику стану мережі в режимі реального часу, що дозволяє ІТ-фахівцям швидко реагувати на погіршення продуктивності, забезпечуючи таким чином чудовий користувацький досвід.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

Зрештою, такий підхід гарантує покращену доступність послуг у всій мережевій інфраструктурі.

Посилений рівень безпеки завдяки виявленню загроз на основі штучного інтелекту

Виявлення загроз на основі штучного інтелекту трансформує моніторинг безпеки. Сучасне програмне забезпечення для моніторингу мережі використовує машинне навчання для виявлення підозрілої активності, аномальних моделей трафіку та потенційних порушень у мережі.

Ці системи співвідносять різноманітні сигнали, від невдалих спроб входу до системи до витоку даних, позначаючи загрози задовго до їхньої ескалації.

Автоматизоване виявлення загроз скорочує час реагування та допомагає ІТ-командам зосередитися на найважливіших інцидентах. Замість того, щоб бути перевантаженими гучними сповіщеннями, адміністратори отримують дієву аналітику, яка виявляє ризики з високим пріоритетом.

Інтегровані інформаційні панелі та звіти відстежують поточні загрози та зусилля щодо їх усунення, підтримуючи відповідність вимогам та журнали аудиту.

Зменшення простоїв та експлуатаційних витрат

Скорочення простоїв – це прямий шлях до зниження експлуатаційних витрат. Удосконалене програмне забезпечення для моніторингу мережі виявляє та вирішує проблеми з продуктивністю до того, як вони спричинять збої, захищаючи організації від дорогих перебоїв.

Оповіщення в режимі реального часу, автоматизоване виправлення та оптимізовані робочі процеси сприяють швидшому реагуванню на інциденти.

Коротший час простою означає, що співробітники залишаються продуктивними, а клієнти мають безперебійний доступ до послуг. Історичні дані та аналіз першопричин також допомагають командам навчатися на минулих інцидентах, удосконалювати майбутні стратегії та мінімізувати повторювані проблеми.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

Краще планування потужностей та стратегічне узгодження

Ефективне планування потужностей спирається на точні та детальні дані про продуктивність. Рішення для моніторингу мережі збирають показники використання пропускної здатності, завантаження пристроїв та моделей трафіку, допомагаючи організаціям передбачати зростання та розумно розподіляти ресурси.

Аналітика в режимі реального часу та історичні тенденції допомагають у прийнятті рішень щодо інвестицій та модернізації інфраструктури.

Стратегічне узгодження стає досяжним, коли ІТ-лідери можуть впевнено підтримувати бізнес-цілі за допомогою масштабованих та надійних мереж.

Програмне забезпечення для моніторингу перетворює технічну інформацію на практичні бізнес-ідеї, що спрощує обґрунтування витрат та демонстрацію рентабельності інвестицій.

Підвищена гнучкість та масштабованість у гібридному/хмарному середовищі

Гнучкість та масштабованість є невід'ємними елементами в гібридних та хмарних середовищах. Сучасні інструменти моніторингу мережі забезпечують видимість у режимі реального часу та швидку адаптацію до змін робочих навантажень, сприяючи безперешкодному масштабуванню локальних та хмарних ресурсів.

Автоматизоване виявлення, динамічне зіставлення та налаштовувані інформаційні панелі забезпечують, що постачальники ІТ-послуг можуть відстежувати нові пристрої або програми під час їх розгортання.

Показники продуктивності та сповіщення залишаються незмінними, незалежно від того, де знаходяться ресурси. Така гнучкість дозволяє організаціям швидко реагувати на зміну бізнес-вимог, запускати нові послуги або розширювати потужності, не жертвуючи контролем.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

Розширення можливостей ІТ-команд за допомогою автоматизації та штучного інтелекту як копілотів

Автоматизація та штучний інтелект дозволяють ІТ-командам впевнено керувати складними мережами. Програмне забезпечення для моніторингу, яке автоматизує рутинні перевірки, управління порогами та усунення інцидентів, дозволяє персоналу зосередитися на стратегічних проектах, а не на ручному усуненні несправностей.

Копілоты на базі штучного інтелекту ще більше підвищують продуктивність, надаючи контекстні рекомендації, керовані робочі процеси та аналітичні дані в режимі реального часу на основі даних про продуктивність. Ці віртуальні помічники допомагають командам інтерпретувати аномалії, визначати пріоритети проблем та ефективно вирішувати інциденти, навіть коли мережеві середовища стають дедалі складнішими.

Перспективи на майбутнє / Що подивитися

Новітні технології суттєво змінять підхід організацій до моніторингу мережі. Акцент слід зробити на інтеграції передових алгоритмів машинного навчання, що пропонують безпрецедентне розуміння продуктивності мережі та потенційних проблем. Крім того, зростаюче впровадження гібридних середовищ вимагатиме вдосконалених рішень для моніторингу, які можуть безперешкодно адаптуватися до різноманітних мережевих компонентів. Аналіз трафіку в режимі реального часу та покращені показники взаємодії з користувачем стануть важливими для ІТ-команд, які прагнуть забезпечити доступність мережі. У міру продовження цифрової трансформації, пріоритетність цих тенденцій дозволить компаніям ефективно оптимізувати свої методи управління мережею.

Вкрай важливо, щоб організації адаптувалися та впроваджували ці досягнення

Адаптація до нових технологій моніторингу більше не є необов'язковою – вона є важливою для організацій, які прагнуть підтримувати високопродуктивні ІТ-операції. Темпи змін в управлінні мережами, моніторингу безпеки та хмарних

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		48

сервісах означають, що вчорашні найкращі практики можуть не відповідати потребам завтрашнього дня.

Впровадження моніторингу, автоматизації та розширеної аналітики на основі штучного інтелекту дозволяє організаціям встигати за зростаючою складністю та масштабом. Проблеми впровадження часто включають прогалини в навичках, перешкоди в інтеграції та опір змінам. Однак переваги – зменшення часу простою, покращення стану мережі та більша гнучкість – значно переважають ризики.

Перспективи на майбутнє: шлях до все більш автономних та інтелектуальних мереж

У майбутньому еволюція автономних та інтелектуальних мереж змінить те, як організації контролюють та керують своїми ІТ-ландшафтами. Штучний інтелект та машинне навчання будуть рушійними силами цієї трансформації, дозволяючи мережам самовідновлюватися, самооптимізуватися та динамічно адаптуватися до нових вимог і загроз.

Ці інтелектуальні системи автоматично виявлятимуть проблеми з продуктивністю, визначатимуть потенційні порушення безпеки та вживатимуть коригувальних заходів без ручного втручання. Моделі машинного навчання ставатимуть більш досконалішими, постійно вдосконалюючи своє розуміння поведінки мережі та адаптуючись до останніх загроз або вимог бізнесу.

З наближенням 2026 року ландшафт мережевого моніторингу стрімко розвивається завдяки розвитку штучного інтелекту, хмарних технологій та інтеграції кібербезпеки.

Організації повинні бути в курсі цих тенденцій, щоб покращити свої можливості моніторингу та забезпечити надійну безпеку, зберігаючи при цьому операційну ефективність. Впровадження таких концепцій, як автоматизований аналіз першопричин, комплексна спостережуваність та архітектура нульової довіри, не лише покращить продуктивність, але й надасть ІТ-командам можливість швидко реагувати на кіберзагрози, що розвиваються, та операційні

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

виклики. Майбутнє за інтелектуальними автономними мережами, які можуть адаптуватися до змінних вимог. Слідкуйте за цими розробками та вживайте проактивних заходів для вдосконалення ваших стратегій моніторингу мережі на наступні роки.

3.3 Розробка функціональної схеми

Прискорення росту ринку систем керування інфраструктурою ЦОД у сполученні з їх реальними й відчутними перевагами підвищує важливість DCIM не тільки для начальника інженерно-технічної служби, але й для IT-менеджера й директора по IT. Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq – це повнофункціональне програмне забезпечення керування інфраструктурою ЦОД. Воно являє собою комплексну платформу автоматичного збору, реєстрації й відображення даних для полегшення керування ЦОД. Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq оптимізує продуктивність і керування життєвим циклом ЦОД.

Переваги системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq:

– Єдина платформа для централізованого відображення даних. Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq є єдиною платформою централізованого надання всієї важливої інформації про ЦОД у масштабі реального часу.

– Економічна ефективність. Організації, що реалізують корпоративні ініціативи по підвищенню економічної ефективності, можуть скористатися DCIM для оптимізації керування, ефективного використання ресурсів всієї

інфраструктури й зниження її впливу на навколишнє середовище. Коефіцієнт використання енергії (PUE) зменшується й, відповідно, скорочуються витрати.

– Підвищена готовність. Можливість перегляду критично важливої інформації підвищує готовність центру обробки даних. Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq пропонує розширені алгоритми оповіщення по всій інфраструктурі, що допомагає знизити ризик простоїв ЦОД.

– Керування стійкістю експлуатації. Уміння оцінювати перспективи експлуатації ЦОД і розуміння того, яким образом можна оптимізувати його ресурси, неоціненні для успішного ведення бізнесу. Програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq не тільки поліпшує керування потужностями й активами, але й підвищує загальну продуктивність ЦОД, сприяючи продовженню строку його служби.

Дані й функції, доступні для фахівців з керування ЦОД:

1. Для начальника інженерно-технічної служби:

- Загальна схема ЦОД.
- Розподіл значень і профіль.
- Параметри ЦОД.
- Стан усього встаткування.
- Стан і режим роботи чіллера.
- Діаграми потужності.
- Повідомлення про тривоги й звітність.

**Програмна реалізація системи інтелектуального моніторингу ЦОД з
середною передачею даних реалізованою за стандартом IEEE 802.3bq**

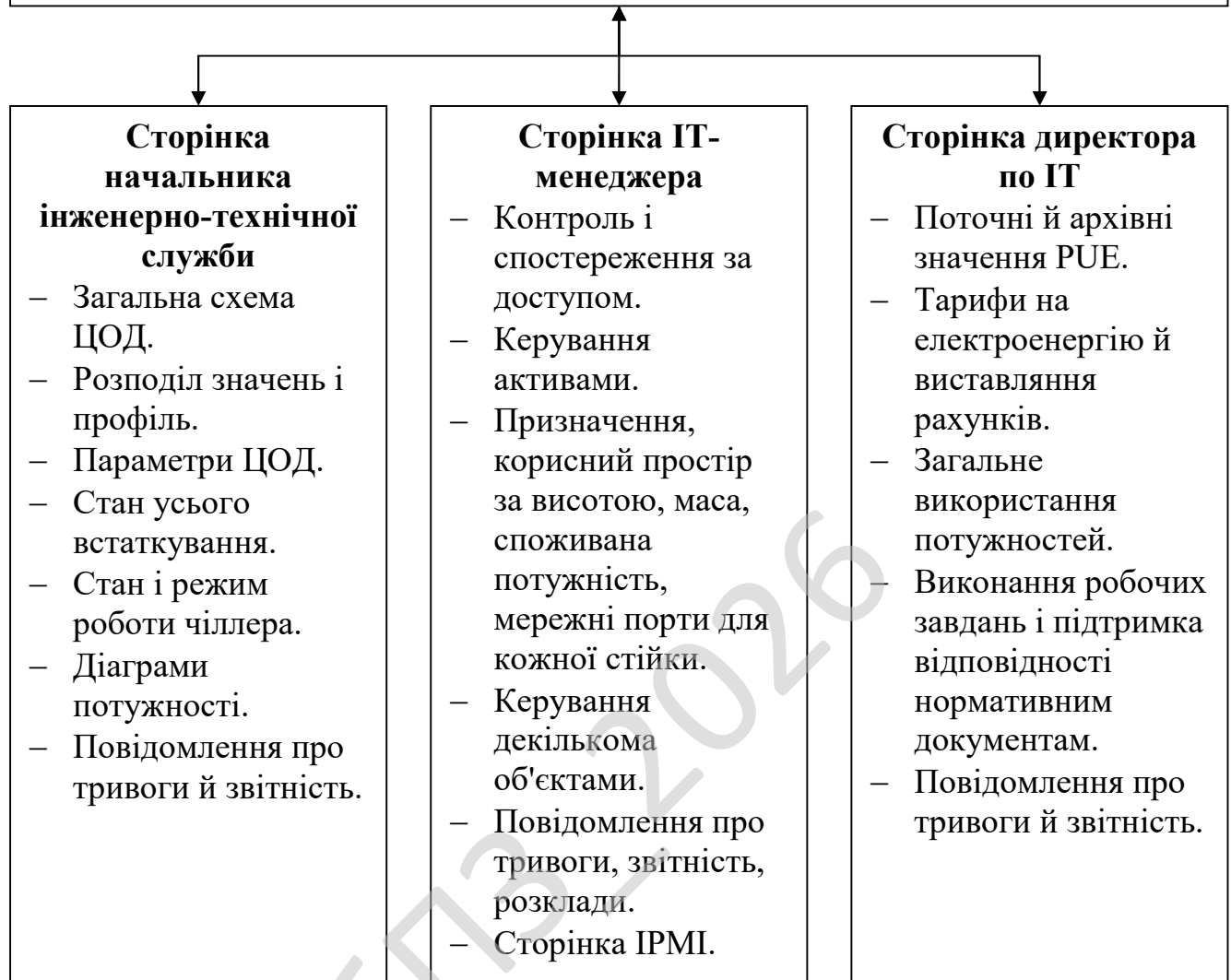


Рисунок 3.2 – Функціональна схема системи

2. Для ІТ-менеджера:

- Контроль і спостереження за доступом.
- Керування активами.
- Призначення, корисний простір за висотою, маса, споживана потужність, мережні порти для кожної стійки.
- Керування декількома об'єктами.
- Повідомлення про тривоги, звітність, розклади.
- Сторінка IPMI.

3. Для директора по ІТ:

- Поточні й архівні значення PUE.
- Тарифи на електроенергію й виставляння рахунків.
- Загальне використання потужностей.
- Виконання робочих завдань і підтримка відповідності нормативним документам.
- Повідомлення про тривоги й звітність.

Усього лише п'ять років тому ринок систем керування інфраструктурою дата-центру (DCIM) тріпотів від захвату: першим adeptам була надана можливість скористатися функціями моделювання й перегляду у високому дозволі по-поверхових планів і стійок, розташованих усередині дата центру.

На першому етапі розвитку ринку DCIM це було воістину вражаючим досягненням: створити точну модель дата-центру за допомогою одного лише зображення, яким можна маніпулювати на екрані монітора й виводити в різних формах залежно від цілей документування. Більш ніж десяток розроблювачів перших DCIM видавали на-гора одну демоверсію за іншою, при цьому головним критерієм якості в рекламних проспектах вказувався ступінь реалістичності зображення стійок.

Кінцеві користувачі оцінили результати візуалізації, надані ранніми версіями DCIM, але проте, вони чекали більшого: нова технологія повинна була допомагати в рішенні комерційних завдань. У деяких випадках можливість легко моделювати й документувати свою ІТ-структуру була сама по собі достатньою, і рішення купувався винятково як засіб візуалізації, але ринок чекав, коли ж виявить себе комерційна цінність цієї концепції.

У другій, сучасній фазі розвитку технології DCIM завдання з'єднання DCIM-моделі із зовнішнім миром у реальному часі стала ключовий. Основна комерційна цінність будь-якого рішення DCIM полягає в тому, наскільки добре воно інтегрується із загальною системою керування дата-центром (що включає керування будинком). Мова йде не тільки про джерела живлення й датчиках

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

температури, але й про повний процес керування інформаційними сервісами й системами (ITSM). Чим більше інформації, тим якісніше прийняті на її основі рішення. У світі, орієнтованому на створення рентабельних Каталогів Сервісів, можливість такого підключення стає єдиним способом розрахувати реальні витрати, пов'язані з наданням тих або інших послуг.

Націлена на зниження експлуатаційних витрат, система DCIM сьогодні – чи не краще рішення по оптимізації дата-центру і його поточних операцій. DCIM використовується для забезпечення й реалізації найкращих методів, а також стандартизації роботи підприємства й всіх його дата-центрів. DCIM створює найбільш експлуатаційно-придатні структури, де всі використовувані процеси створення й підтримки інформаційних систем можуть бути оптимізовані, захищені й відтворені незалежно від того, хто їх створив і де вони перебувають на будь-якому етапі розвитку підприємства.

Сьогодні можна спостерігати деякі ключові тенденції в комплексі DCIM. Тут я приведу десять із них.

1. Два аспекти керування

На сьогоднішній момент сформувалися дві основні групи пропозицій у сегменті ринку DCIM:

- керування інформаційними ресурсами в стійках протягом тривалих тимчасових проміжків;
- керування механічними, електричними елементами й водопровідною арматурами, або керування енергопостачанням і охолодженням об'єкта.

Більшість розроблювачів починають визнавати наявність обох груп і необхідність розробляти такі рішення, які стерли б границю між ними. Сьогодні кожний вендор, працюючи над рішенням, фокусується, як правило, на одному аспекті, у більшості випадків лише несміливо переборюючи границю між ними, щоб в обмеженому обсязі задовольнити потреби іншої сторони. Чи вдасться звести ці аспекти воедино? Час покаже. Надія є, але поки створити реальне рішення для такої єдиної платформи DCIM не вдається жодному із гравців.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

2. DCIM як інструмент стратегії

У міру того як відношення до технології мінялося (від опції до предмета першої необхідності), більшість кінцевих користувачів зрозуміли, що DCIM повинна стати не просто ще одним тактичним інструментом, але й частиною стратегії керування.

Дата-центри протягом останнього років росли, поступово розширюючи свого функціонала з появою кожного нового інструмента. Сьогоднішній тренд – мислити стратегічно й знаходити більше продуктивні рішення для всіх зацікавлених осіб. Найбільш успішні проекти показали, що від впровадження DCIM починають вигравати широкі шари користувачів багатьох галузей, внаслідок чого відношення до DCIM міняється від «непогано б мати» до «необхідно мати». Деякі з нині діючих впроваджених DCIM-моделей використовуються сотнями клієнтів зі сфери інформаційних технологій, фінансів, інфраструктурних проектів, навіть управлінського сектора вищої ланки. DCIM проявляє себе щонайкраще, якщо вона розглядається як стратегічний інструмент, і її ефективність прямо може бути пов'язана з витратами на будівництво й зміст дати-центру.

3. Статус Системи Зберігання Даних

У міру посилення взаємного проникнення цифрових технологій у дата-центрі споживачі мають потребу у всі меншій кількості інструментів. Стало тенденцією шукати більше зроблені рішення, у яких використовується принцип обміну даними. Інструменти, що вимагають дублювання даних, поступово відмирають. Інтеграція на рівні конвергентної інфраструктури (CI) має критичне значення. У найбільш успішних DCIM-інсталяціях інтеграція репозиторія DCIM з іншими системами настільки висока, що DCIM сама по собі стала розглядатися як «система записів», або «база даних» активів дати-центру.

Фактично DCIM стає самою точною моделлю дата-центру, у багатьох випадках навіть більше точною, ніж бухгалтерські реєстри.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

4. Зміни в дата-центрі через реінжиніринг процесів

Дата-центри завжди були площадками, на яких відбуваються зміни: там увесь час щось міняється. Бездоганно-прозорий дизайн дати-центру швидко перетворюється в хаотичне накопичення відновлень, які погано задокументовані й часто зовсім неефективні. Сьогоднішній тренд – перспективне планування всіх змін, які відбудуться в даті-центрі.

По ідеї, ефективність дата-центру не буде падати, якщо використовується стругаюча система керування змінами. Якщо зміни параметрів виробляються за допомогою системи керування змінами (яка є частиною DCIM), ця модель завжди буде залишатися точним відбиттям стану самого дата-центру й дозволить підтримувати його в оптимізованому стані. Таким чином, сьогодні тенденція полягає в тому, щоб шукати рішення комерційних питань шляхом аналізу DCIM-моделі, а не в процесі блукання між рядами стійок дата-центру в надії одержати відповіді лише на підставі спостереження за тим, що відбувається в серверному залі.

5. Ріст популярності SaaS

Хоча впровадження DCIM спочатку розглядалося як рішення локальне, багато розроблювачів уже тоді почали пропонувати програмне забезпечення як сервіс (SaaS). Можливості DCIM як сервісу стають ідентичними локальному рішенням окремого розроблювача.

Причина цього тренда, тобто використання SaaS-версії DCIM, криється в тому, у тім, що пропозиція у вигляді сервісу SaaS-можна віднести в статтю операційних витрат, а не капітальних витрат. Хоча процес прийняття ринком цих сервісів може бути однаковий, проте існує думка, що пропозиції SaaS більше відкриті й гнучкі. Важливо помітити, що в той час як DCIM традиційно відносять до сегмента сервісів, підхід до реалізації DCIM безпосередньо на площадці, або у вигляді SaaS-варіанта повинен бути однаковим, якщо ви хочете успішно впровадити цю систему.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

6. DCIM – більше не «річ у собі»

У той час як раніше функціональність досягалася за рахунок окремо взятих можливостей, нині особливо важливою є інтеграція в системи керування IT-інфраструктурою (ITSM), включаючи керування змінами й керування конфігураційними базами даних (CMDBs). Сьогоднішня тенденція – побудувати більше високий рівень інтеграції на етапі вибору DCIM-провайдеру. Інтеграція в системи ITSM необхідна для того, щоб зробити DCIM стратегічною частиною інфраструктури керування дата-центром. Взагалі, підхід до впровадження DCIM без обліку подальшої інтеграції залишився далеко в минулому.

Перспективи використання DCIM у співвідношенні з іншими ключовими інструментами керування тепер повністю прогнозуються з першого дня розробки проекту.

7. Тісна інтеграція із засобами віртуалізації

На сьогоднішній день уже більше половини серверів у світі віртуалізовані. Таким чином, має сенс тісно інтегрувати найбільш успішні DCIM-рішення з топовими галузевими віртуальними платформами.

Тенденція сьогодні – шукати рішення, що дозволяють одержати в реальному часі подання про статус віртуального сервера на кожному з фізичних пристроїв. DCIM повинна забезпечувати зображення контрольованого вузла і його операційних систем у режимі реального часу. Зараз прагнуть використовувати зв'язану картину віртуалізації для планування навантаження від операційної системи до сервера, і, в остаточному підсумку, до необхідних фізичних ресурсів (приміщення, енергопостачання, охолодження).

8. Ріст використання вбудованих датчиків

Завдання контролювати параметри середовища в дата-центрі існували завжди, але рішення були громіздкими й дорогими. Сьогодні виробники IT-устаткування шукають рішення, що дозволяють вбудовувати апаратні датчики в кожний пристрій промислового класу, що випускається ними. Ці датчики можуть

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

надавати звіт про енергоспоживання, про температуру усередині різних зон дата-центру й про фізичну безпеку.

Тенденція полягає в тому, щоб найбільше ефективно використовувати убудовані датчики й комбінувати їх з додатковими (звичайно бездротовими) для тих пристроїв, які не перебувають на площадці основного встаткування.

9. Точна оцінка активів конвергентної інфраструктури

Серед корпоративних дата-центрів простежується тенденція до забезпечення процесів перевірки й балансування з метою увесь час зберігати впевненість у тім, що DCIM-модель точно відбиває ситуацію в серверному залі. Такий подвійний контроль приймає різні форми, від перевірки вручну з використанням електронних таблиць, до використання бездротового зчитувача штрихкода й/або локальних технологій, заснованих на автоматизованому використанні радіочастотних міток (RFID). Можлива навіть комбінація інформації, отриманої візуальним способом, з даними від системи виявлення або від коннекторів конфігураційної бази CMDB.

У кожному разі, є тенденція до підвищення точності відображення моделей дата-центрів будь-якими можливими засобами, через ITSM-інтеграцію, інтеграцію із системою віртуалізації, а також за допомогою технологій, наявних на самій площадці.

10. Загальнокорпоративне впровадження DCIM

Рішення DCIM спочатку пропонувалися як засіб візуалізації десятка стійок. З ростом комерційної ефективності зі стратегічної точки зору масштаб впровадження DCIM значно розширився, аж до того, що деякі постачальники DCIM-рішень тепер обслуговують десятки тисяч стійок у десятках дата-центрів.

Не варто забувати, що в рамках DCIM-пропозиції всі об'єкти, включаючи ті що розташовано усередині іншого будинку, модульні, а також комерційні ЦОДи із сервісами колокейшен, розглядаються як площадки дати-центру. Іноді можна зустріти десятки площадок, які потрібно сукупно представити в єдиному

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

DCIM-рішенні. Сьогоднішні рішення прагнуть охопити все компоненти, у будь-якому масштабі, незалежно від їхнього фізичного розташування.

У цей час ми спостерігаємо розвиток технології DCIM, що відбуває в основному завдяки зрушенню від ідеї дата-центру як тактичного набору функцій до дата-центру – добре осмисленому стратегічному інструменту. Постачальники DCIM розуміють, що їм потрібно фокусуватися на високоефективній послугі в декількох підсистемах, а не заспокоюватися на досягненнях у сфері підвищення деталізації картини. Кінцеві користувачі тепер повинні формувати свої індивідуальні вимоги до DCIM набагато більш докладно, ніж коли-або в минулому. Фактично, від IT-організацій тепер вимагають чітко роз'яснити склад портфеля сервісів, виділяючи кожний сервіс в окремий рядок каталогу. Система DCIM стає життєво важливим компонентом у створенні таких елементів каталогів сервісів, оскільки її завдання зрештою зводиться до керування витратами.

Отже, як же виглядає наступна фаза розвитку DCIM? Очевидно, це буде контроль і оркестровка. Це зрівноважить моделювання й зв'язність, удосконалені в перших двох фазах, і привнесе новий рівень автоматизації з використанням електронних систем керування, що замінюють участь людини при прийнятті рішень.

У більшості випадків пристрою автоматизації стають засобом виконання складних наборів правил, заснованих на великих обсягах метричної інформації. Незважаючи на те, що наступна фаза буде визрівати набагато довше внаслідок різноманітності середовища провайдерів послуг дата-центрів, саме ця фаза DCIM дозволить знизити рівень витрат до бажаного.

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

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

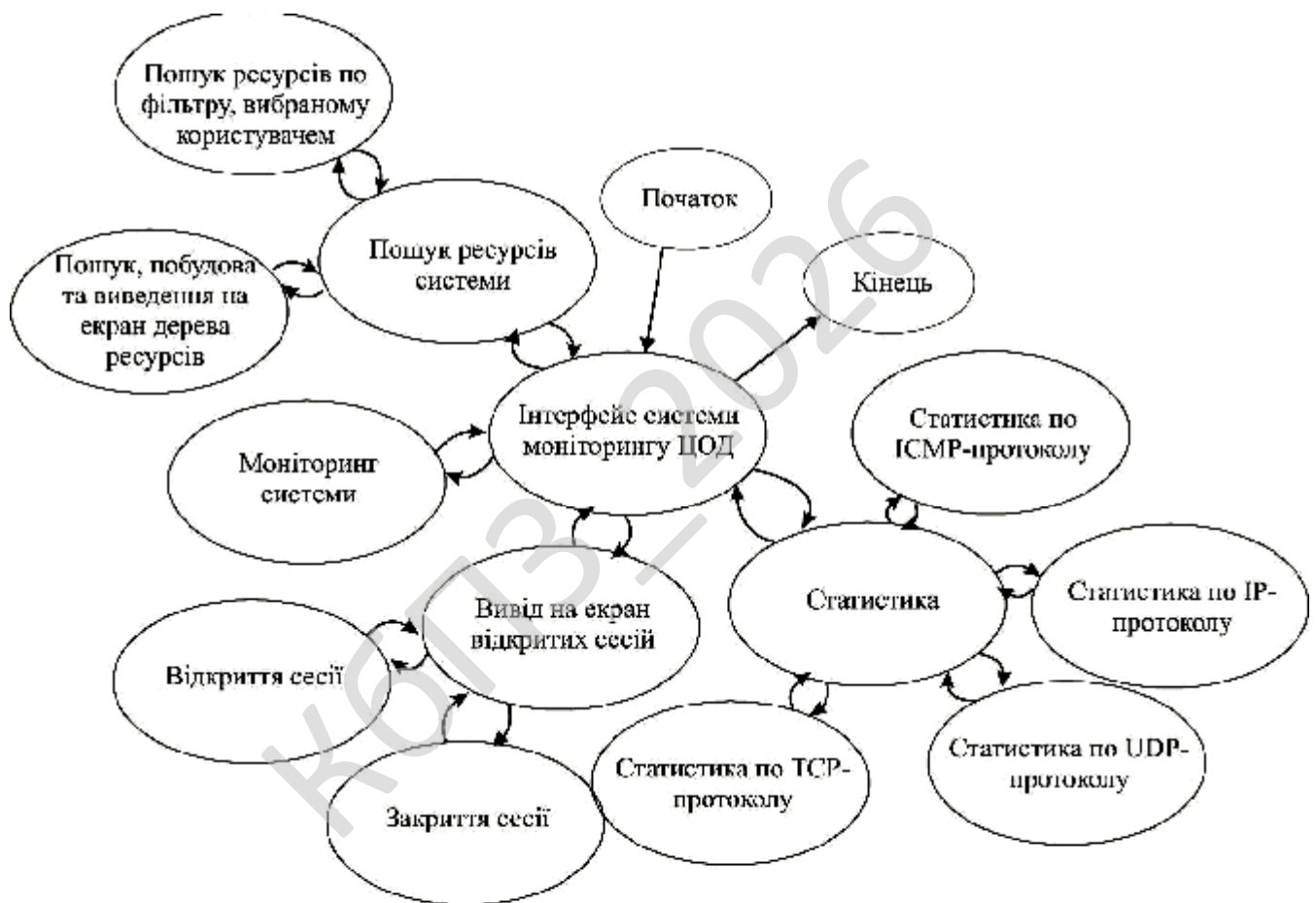


Рисунок 3.3 – Діаграма взаємодії процесів

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.

При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).

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.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень.

Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. 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 високого рівня декомпозиції задач на класи.

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 підсистеми 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.

Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

стандарт, що використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

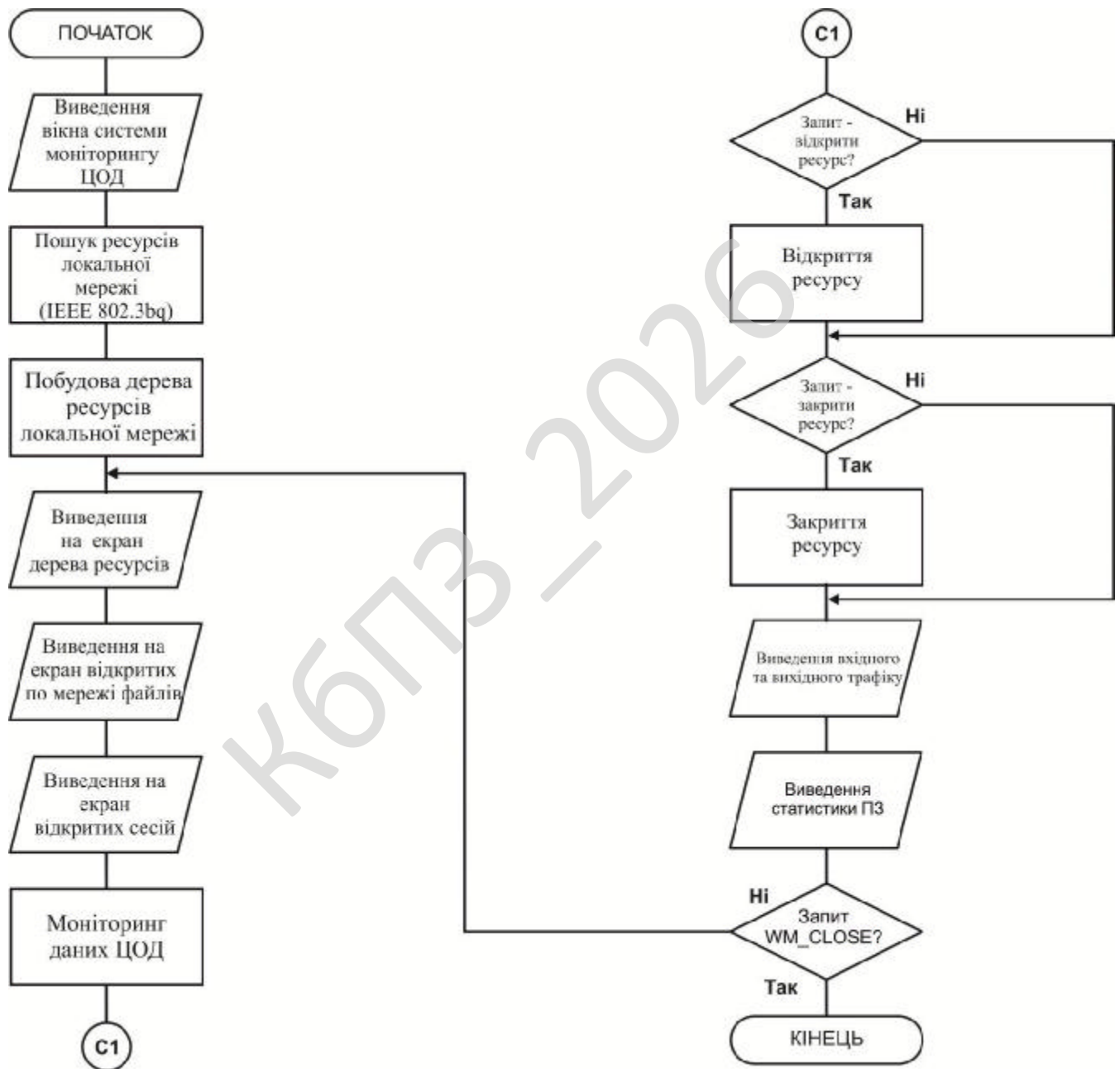


Рисунок 4.1 – Блок-схема основної програми

Хоча я реалізовував програму сам, було використано підходи Scrum для саморозвитку та пришвидшенню розробки, розглянемо цей метод. Scrum – підхід управління проектами для гнучкої розробки програмного забезпечення. Скрам чітко робить акцент на якісному контролі процесу розробки.

Підхід вперше описали Гіротакі Такеучі та Ікуджіро Нонака в статті The New New Product Development Game (Гарвардський Діловий Огляд, січ–лют 1986). Вони відзначили, що проекти, над якими працюють невеликі, крос-функціональні команди, зазвичай систематично продукують кращі результати, і пояснили це, як «підхід регбі». У 1991 році Деґрейс та Шталь у книжці Злі проблеми, справедливі рішення послалися на цей підхід, як на Scrum (штовханина; сутичка навколо м'яча (у регбі)), спортивний термін, згаданий в статті Такеучі і Нонака. Кен Швабер на початку 1990-х використовував підхід який привів Scrum в його компанію.

Вперше метод Scrum було представлено на загальний огляд задокументованим, чітко сформульованим та описаним спільно Сазерлендом та Швабером на OOPSLA'96 в Остіні. Швабер та Сазерленд протягом наступних років працювали разом щоб обробити та описати весь їхній досвід та найкращі практичні зразки для індустрії в одне ціле, в ту методологію, що відома сьогодні як Scrum. Швабер об'єднав зусилля з Майком Бідлом в 2001, щоб детально описати метод в книжці Agile Software Development with SCRUM. Не зважаючи на те, що для Scrum нарікли долю управління проектами з розробки ПЗ, він може також використовуватися в роботі команд обслуговувань програмного забезпечення (software maintenance teams), або як підхід управління розробкою і супроводом програм: Scrum of Scrums.

Scrum – це кістяк процесу, який включає набір методів і попередньо визначених ролей. Головні дійові особи – ScrumMaster, той хто опікується процесами, веде їх і працює як керівник проекту, Власник Продукту, людина, що представляє інтереси кінцевих користувачів та інших зацікавлених в продукті сторін, та Команду, яка включає розробників.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		64

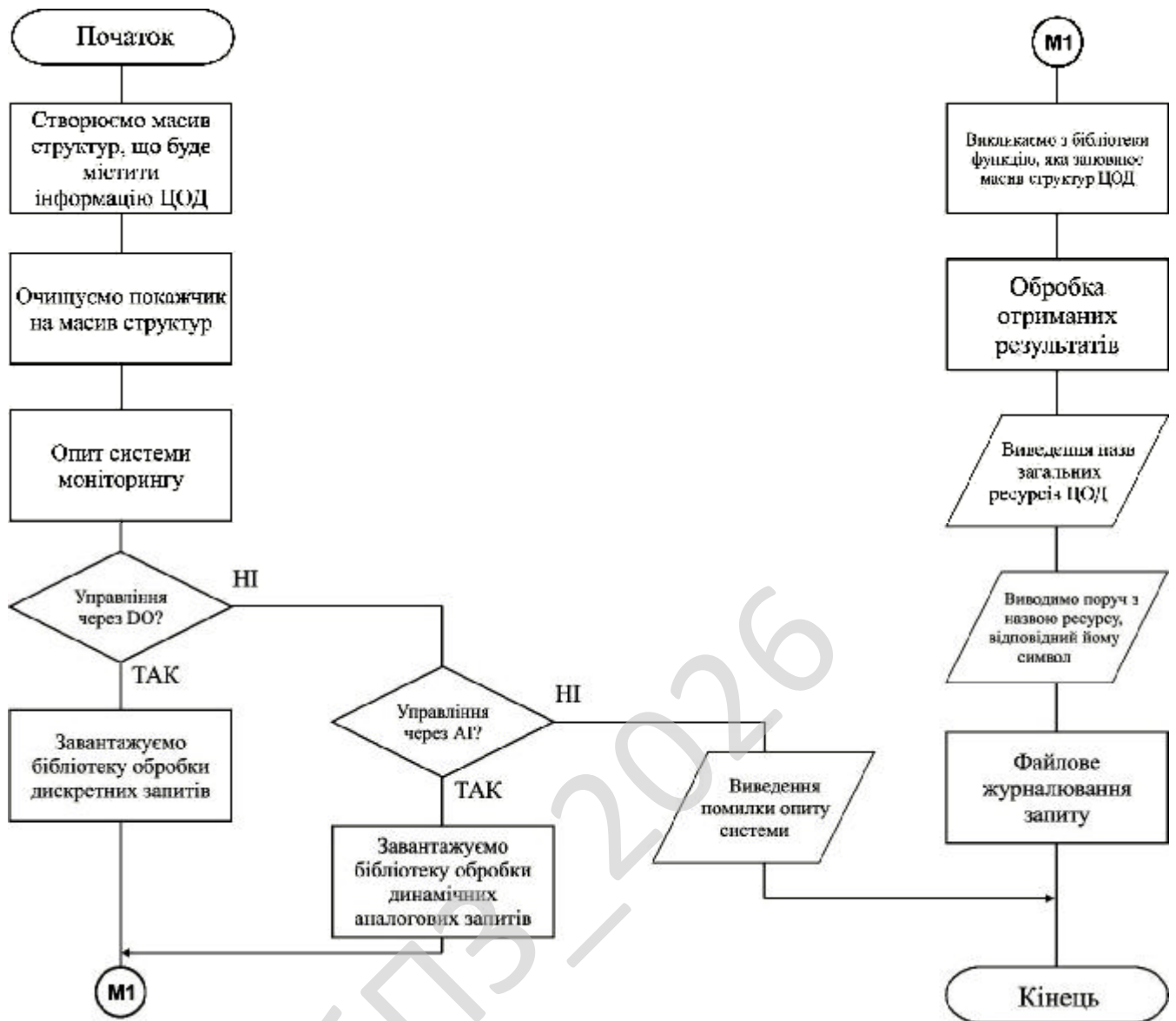


Рисунок 4.2 – Блок-схема роботи підпрограми

Протягом кожного спринту, 15-30 денного періоду (тривалість визначається командою), працівники створюють функціональний ріст програмного забезпечення.

Набір можливостей, які імплементуються кожного спринту, приходять з етапу, що має назву product backlog (документація запитів на виконання робіт), який має найвищу пріоритетність за рівнем вимог до роботи, що повинна бути виконана.

Запити на виконання робіт (backlog items), що визначені протягом наради з планування спринту (sprint planning meeting), переміщуються в етап спринту. Протягом цієї наради Власник Продукту інформує про завдання, які він хоче, аби були виконані. Тоді Команда визначає, скільки з бажаного вони можуть зробити, щоб завершити необхідні частини протягом наступного спринту. Протягом спринту команда виконує визначений фіксований список завдань (т.з. backlog items). Впродовж цього періоду ніхто не має права змінювати перелік запитів на виконання робіт, що слід розуміти, як заморожування вимог (requirements) протягом спринту.

Product backlog – це документ, який має список вимог до функціональності, які упорядковані згідно зі ступенем важливості. Product backlog представляє список того, що повинно бути реалізовано. Елементи цього списку називається «історіями» (user story) або елементами backlog-у (backlog items). Product backlog відкритий для редагування усім учасникам Scrum-процесу.

Обов'язкові поля:

1. ID – унікальний ідентифікатор, порядковий номер, який використовується для ідентифікації історій у разі їх перейменування.

2. Назва (Name) – стислий опис історії. Він повинен бути однозначним, щоб і розробники і product owner могли зрозуміти, про що йдеться і відрізнити одну історію від іншої.

3. Важливість (Importance) – ступінь важливості даної історії на погляд product owner'a. Зазвичай являє собою натуральне число, іноді для цієї цілі використовуються числа Фібоначчі. Чим більше значення, тим більше пріоритет.

4. Попередня оцінка (initial estimate) – початкова оцінка об'єму робіт, необхідного для реалізації історії порівняно з іншими історіями. Вимірюється у story point'ax. Приблизно відповідає числу «ідеальних людино-днів».

5. Як продемонструвати (how to demo) – стисле пояснення того, як завершена задача буде продемонстрована у кінці спринта. Дане поле може являти собою код автоматизованого приймального тесту.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

Додаткові поля. Іноді, також, використовуються додаткові поля у product backlog, в основному для того, щоб допомогти product owner'у визначитися з його пріоритетами.

Категорія (track). Наприклад, «панель управління» чи «оптимізація». За допомогою цього поля product owner може легко вибрати усі пункти категорії «оптимізація» і задати їм низький пріоритет.

Компоненти (components) – указує, які компоненти (наприклад, база даних, сервер, клієнт) будуть зачеплені при реалізації історії. Дане поле складається з групи checkbox'ів, які відмічаються, якщо відповідні компоненти потребують змін.

Ініціатор запиту (requestor). Product owner може захотіти зберігати інформацію про усіх замовників, зацікавлених у даній задачі. Це потрібно для того, щоб тримати їх у курсі діла про хід виконання робіт.

ID у системі обліку помилок (bug tracking ID) – якщо ви використовуєте окрему систему обліку помилок, тоді у описі історії корисно зберігати посилання на всі дефекти, які до неї відносяться.

Sprint backlog – містить функціональність, обрану Product Owner із Product Backlog. Всі функції розбиті по задачах, кожна з яких оцінюється командою. Кожен день команда оцінює об'єм роботи, який необхідно провести для завершення задачі.

Burndown chart – показує, скільки вже виконано і скільки ще залишається зробити.

Планування спринта (Sprint Planning Meeting)

Проходить на початку нової ітерації Спринта:

– Із Product Backlog обираються задачі, зобов'язання по виконанню яких за спринт приймає на себе команда.

– На основі обраних задач створюється Sprint Backlog. Кожна задача оцінюється у ідеальних людино-годинах.

– Рішення задачі не повинно займати більше 12 годин або одного дня. При необхідності задача розбивається на підзадачі.

– Обговорюється та визначається, яким чином буде реалізовано цей об'єм робіт.

– Тривалість наради обмежена зверху 4–8 годинами в залежності від тривалості ітерації, досвіду команди тощо.

– (Перша частина наради) Беруть участь Product Owner + Команда: обирають задачі із Product Backlog.

– (Друга частина наради) Бере участь лише команда: обговорюють технічні деталі реалізації, наповнюють Sprint Backlog.

Щоденна нарада (Daily Scrum Meeting)

Відбувається кожен день протягом спринта. Є «пульсом» ходу спринта.

Нараді властиві наступні обмеження:

– починається точно вчасно;

– всі можуть спостерігати, але говорять тільки обрані;

– триває не більш ніж 15 хвилин;

– проводиться в одному і тому ж місці протягом одного спринта.

Протягом наради кожен член команди відповідає на 3 запитання:

– Що зроблено з моменту попередньої щоденної наради?

– Що буде зроблено з моменту поточної наради до наступної?

– Які проблеми заважають досягненню цілей спринта? (Над рішенням цих проблем працює ScrumMaster. Зазвичай це рішення проходить за рамками щоденної наради і у складі осіб, що безпосередньо займаються даною перешкодою.)

Демонстрація (Sprint Review Meeting):

– Проходить у кінці ітерації (спринта).

– Команда демонструє внесок функціональності до продукту всім зацікавленим особам.

– Залучається максимальна кількість глядачів.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		68

- Усі члени команди беруть участь у демонстрації (одна людина на демонстрацію або кожен показує, що зробив за спринт).
- Обмежена 4-ма годинами в залежності від тривалості ітерації і змін у продукті.

Ретроспектива (Sprint Retrospective):

- Члени команди висловлюють свою думку про минулий спринт.
- Відповідають на два основних запитання: Що було зроблено добре у минулому спринті?; Що потрібно покращити в наступному?.
- Виконують покращення процесу розробки (вирішують питання та фіксують вдалі рішення).
- Обмежена 1-3ма годинами.

Розглянемо формат що використовується – JSON (JavaScript Object Notation, укр. запис об'єктів JavaScript, вимовляється джейсон) – це текстовий формат обміну даними між комп'ютерами.

JSON базується на тексті, може бути прочитаним людиною. Формат дозволяє описувати об'єкти та інші структури даних. Цей формат головним чином використовується для передачі структурованої інформації через мережу (завдяки процесу, що називають серіалізацією). Розробив і популяризував формат Дуглас Крокфорд.

JSON знайшов своє головне призначення у написанні веб-програм, а саме при використанні технології AJAX. JSON, що використовується в AJAX, виступає як заміна XML (використовується в AJAX) під час асинхронної передачі структурованої інформації між клієнтом та сервером. При цьому перевагою JSON перед XML є те, що він дозволяє складні структури в атрибутах, займає менше місця і прямо інтерпретується за допомогою JavaScript в об'єкти.

JSON з'явився через необхідність обміну даними з сервером у реальному часі без використання плагінів для браузерів, flash-додатків або Java-апплетів, які використовувались скрізь на початку 2000-х років. Дуглас Крокфорд був тим, хто активно просував новий на той час формат. Він з колегами хотів створити

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

технологію, яка використовувала б можливості звичайного браузера давала б веб-розробникам можливість створювати веб-додатки із постійним двостороннім зв'язком із веб-сервером.

JSON вперше був використаний в проєкті в Communities.com для Cartoon Network, він дозволяв обмінюватись повідомленнями і одночасно маніпулювати DHTML-елементами.

Веб-сайт JSON.org було запущено 2002 року. У грудні 2005-го року Yahoo! почав переводити деякі зі своїх веб-сервісів на роботу з JSON. Google взялася до роботи з технологією у своєму веб-протоколі GData у грудні 2006-го року.

Використання

За рахунок своєї лаконічності в порівнянні з XML, формат JSON може бути більш придатним для серіалізації складних структур.

Якщо говорити про веб-застосунки, в такому ключі він доречний в задачах обміну даними як між браузером і сервером (AJAX), так і між самими серверами (програмні HTTP-інтерфейси).

Формат JSON так само добре підходить для зберігання складних динамічних структур в реляційних базах даних або файлового кеші.

Синтаксис

JSON будується на двох структурах:

1. Набір пар назва/значення. У різних мовах це реалізовано як об'єкт, запис, структура, словник, хеш-таблиця, список з ключем або асоціативним масивом.

2. Впорядкований список значень. У багатьох мовах це реалізовано як масив, вектор, список, або послідовність.

Це універсальні структури даних. Теоретично всі сучасні мови програмування підтримують їх у тій чи іншій формі. Оскільки JSON використовується для обміну даними між різними мовами програмування, то є сенс будувати його на цих структурах.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70

У JSON використовуються такі їхні форми:

1. Об'єкт – це послідовність пар назва/значення. Об'єкт починається з символу { і закінчується символом } . Кожне значення слідує за : і пари назва/значення відділяються комами.

2. Масив – це послідовність значень. Масив починається символом [і закінчується символом]. Значення відділяються комами.

3. Значення може бути рядком в подвійних лапках, або числом, або логічними true чи false, або null, або об'єктом, або масивом. Ці структури можуть бути вкладені одна в одну.

4. Рядок – це послідовність з нуля або більше символів юнікода, обмежена подвійними лапками, з використанням escape-послідовностей, що починаються зі зворотної косої риски \. Символи представляються простим рядком. Тип Рядок (String) дуже схожий на String в мовах C і Java. Число теж дуже схоже на C- або Java-число, за винятком того, що вісімкові та шістнадцяткові формати не використовуються. Пропуски можуть бути вставлені між будь-якими двома лексемами.

Використання JSON в AJAX

Наступний фрагмент коду JavaScript показує, як клієнт може використати XMLHttpRequest для запиту об'єктів в форматі JSON з серверу. (Серверна частина коду пропущена, вона просто повертає на запит URL рядок у JSON форматі).

Треба відзначити, що тут використання XMLHttpRequest не є кросс-браузерним (за деталями звертайтеся на сторінку XMLHttpRequest), і код зазнаватиме незначних модифікацій в різних версіях оглядачів Internet Explorer, Opera, Safari або Mozilla. Використання запиту XMLHttpRequest обмежено правилом одного джерела (same origin policy): URL, що відповідає на запит, має посилатися на той же сайт, що обслуговує сторінку, що ініціювала запит.

Оглядачі можуть також використовувати тег <iframe> для асинхронного запиту JSON-даних в кросс-браузерному варіанті, або використати просте перенаправлення <form action="url_to_cgi_script"

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		71

target="name_of_hidden_iframe">. Такий підхід був поширений до приходу популярного нині запиту XMLHttpRequest.

Динамічний тег <script> також можна використати для підвантаження JSON-даних. Ця техніка можлива, щоб обійти надто суворе правило одного джерела, але вона не є безпечною. Запит JSONRequest пропонується, як безпечніша альтернатива.

Питання безпеки

Хоча JSON призначений для передачі даних в серіалізованому вигляді, його синтаксис відповідає синтаксису JavaScript і це створює низку проблем безпеки. Часто для обробки даних, отриманих від зовнішнього джерела у форматі JSON, до них застосовується функція eval() без якої-небудь попередньої перевірки.

JavaScript eval()

Оскільки JSON представляється синтаксично правильним фрагментом коду JavaScript, природним способом розбору JSON-даних в JavaScript-програмі є використання вбудованої в JavaScript функції eval(), яка призначена для обчислення JavaScript-виразів. При цьому підході відпадає необхідність у використанні додаткових парсерів.

Техніка використання eval() робить систему вразливою, якщо джерело JSON-даних, що використовуються, не відноситься до надійних. Такими даними може виступати шкідливий JavaScript-код для атак за допомогою ін'єкції коду. За допомогою цієї вразливості можливо здійснювати крадіжку даних, підробку автентифікації. Проте, вразливість можна усунути за рахунок використання додаткових засобів перевірки даних на коректність. Наприклад, до виконання eval() отримані від зовнішнього джерела дані можуть перевірятися за допомогою регулярних виразів. У RFC, що визначає JSON пропонується використовувати такий код для перевірки його відповідності формату JSON

```
const my_JSON_object = !(/[^\s:}[\]\0-9.\-+Eaeflnr-u \n\r\t]/.test(
text.replace(/"(\\"|\\.|[^\\"\\])"/g, ' ')) &&
eval('(' + testedData + ')');
```

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

Як безпечніша альтернатива eval() була запропонована нова функція parseJSON(), здатна обробляти тільки JSON-дані.

Вбудований JSON

Останні версії веб-браузерів мають вбудовану підтримку JSON і здатні його обробляти без виклику функції eval(), що призводить до описаної проблеми. Обробка JSON у такому разі зазвичай здійснюється швидше. Так у червні 2009 року вбудовану підтримку JSON мали такі браузери: Mozilla Firefox 3.5+; SeaMonkey 2; Thunderbird 3; Microsoft Internet Explorer 8; Opera 10.5; Браузери, засновані на WebKit (наприклад, Google Chrome, Apple Safari).

Принаймні дві популярні бібліотеки JavaScript використовують вбудований JSON у разі його доступності: jQuery; Dojo.

Підробка крос-доменного запиту

Непродумане використання JSON робить сайти вразливими до підробки міжсайтових запитів (CSRF або XSRF). Оскільки тег <script> допускає використання джерела, що не належить до того ж домену, що і використовуваний ресурс, це дозволяє виконувати код даних, представлених у форматі JSON, в контексті довільної сторінки, що робить можливою компрометацію паролів або іншої конфіденційної інформації користувачів, що пройшли авторизацію на іншому сайті.

Це є проблемою тільки у разі вмісту в JSON-даних конфіденційної інформації, яка може бути компрометована третьою стороною і якщо сервер розраховує на політику одного джерела, блокуючи доступ до даних при виявленні зовнішнього запиту. Це не є проблемою, якщо сервер визначає допустимість запиту, надаючи дані тільки у разі його коректності. HTTP cookie не можна використовувати для визначення цього. Виключне використання HTTP cookie використовується підробкою міжсайтових запитів.

Розширення, JSONP

JSONP або «JSON з підкладкою» є розширенням JSON, коли назва функції зворотного виклику вказується як вхідний аргумент. Спочатку ідея була

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

запропонована в блозі MacPython в 2005 році, і в наш час використовується багатьма Web 2.0 застосунками, такими, як Dojo Toolkit Applications, Google Toolkit Applications і zanox Web Services.

Подальші розширення цього протоколу були запропоновані з урахуванням введення додаткових аргументів, як, наприклад, у разі JSONPP за підтримки S3DB вебсервісів.

Оскільки JSONP використовує скрипт-теги, виклики по суті відкриті світові. З цієї причини JSONP може бути недоречними для зберігання конфіденційних даних.

Включення скриптових тегів від віддалених сайтів дозволяє їм передати будь-який контент на сайті. Якщо віддалений сайт має вразливості, які дозволяють виконати ін'єкції JavaScript, то початковий сайт також може бути ними зачеплений.

Розширення, BSON

BSON – це бінарна форма представлення простих структур даних і асоціативних масивів (які називають об'єктами або документами). Назва «BSON» заснована на визначенні JSON і неофіційно означає «Binary JSON» (бінарний JSON).

JSON Reference

Стандарт JSON не описує посилання на інші об'єкти або частини, але існує чернетка стандарту IETF для посилань на об'єкти на основі JSON. Посилання дозволяють здійснювати трансклюзію – вставляти одні документи в інші.

JSON Reference – це JSON-об'єкт з ключем "\$ref" (всі інші ключі ігноруються) і значенням стрічкового типу що містить URI, наприклад:

```
{ "$ref": "http://example.com/example.json#/foo/bar" }
```

Якщо URI містить ідентифікатор фрагмента (в прикладі вище "/foo/bar"), він інтерпретується як JSON Pointer.

Модуль dojox.json.ref в Dojo toolkit, забезпечує підтримку декількох форм JSON Reference.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

Jira – була використана комерційна система відслідковування помилок, призначена для організації взаємодії з користувачами, хоча в деяких випадках використовується і для управління проектами. Розроблено компанією Atlassian, є одним з двох її основних продуктів (поряд з вікі-системою Confluence). Має веб-інтерфейс.

Назва системи отримано шляхом усічення слова «Gojira» – Японського імені монстра Годзилла, що, в свою чергу, є відсиланням до назви конкуруючого продукту – Bugzilla; створювалася в якості заміни Bugzilla і багато в чому повторює її архітектуру. Система дозволяє працювати з декількома проектами. Для кожного з проектів створює і веде схеми безпеки і схеми оповіщення.

До версії 3.13.5 (включно) розрізнялися редакції Enterprise, Professional і Standard, після – Залишилася тільки редакція Enterprise (для великих організацій).

Система заснована на Java EE і працює на кількох популярних системах управління базами даних і операційних системах.

Основний елемент обліку в системі – завдання (ticket або issue). Завдання містить назву проекту, тему, тип, пріоритет, компоненти і зміст. Завдання може бути розширена додатковими полями (також і нові призначені для користувача поля можуть бути визначені), додатками (наприклад – Фотографіями, скріншотами) або коментарями. Завдання може редагуватися або просто змінювати статус, наприклад, з «відкритий» в «закритий». Які переходи між станами можливі, визначається через настраюється потік операцій. Будь-які зміни в задачі записуються в журнал.

Jira має велику кількість можливостей конфігурації: для кожної програми може бути визначений окремий тип завдання з власним workflow, набором статусів, одним або декількома видами уявлення (screens). Крім того, за допомогою так званих «схем» можна визначити для кожного індивідуального Jira-проекту власні права доступу, поведінку і видимість полів і багато іншого.

Завдяки універсальному підходу можна пристосувати Jira для багатьох непрофільних завдань, наприклад, керування вимогами, керування ризиками, аж до реалізації невеликої системи бронювання, автоматизації процесу рекрутингу.

Для інтеграції з зовнішніми системами підтримує інтерфейси SOAP, XML-RPC і REST. Поставляється із засобами інтеграції з такими системами управління версіями, як Subversion, CVS, Git, Clearcase, Team Foundation Server, Mercurial і Perforce.

Існують доповнення, що дозволяють вбудувати Jira в інтегровані середовища розробки, в тому числі Eclipse і IntelliJ IDEA. Перекладена багатьма мовами, включаючи російську, англійську, японську, німецьку, французьку, іспанську.

Для сторонніх розробників надаються кошти розробки розширень системи – плагінів. Розробники розширень можуть викладати плагіни для продажу на спеціальний розділ сайту Atlassian.

Є комерційним продуктом, який може бути ліцензований для роботи на локальному сервері або доступний в якості віддаленого додатки. Ціноутворення залежить від максимального числа користувачів, при цьому близько \$50 за користувача для локального і \$7 на місяць за користувача для віддаленого доступу є типовими цінами.

Для академічних і комерційних клієнтів доступний повний вихідний код під ліцензією розробника.

Для проектів з відкритим вихідним кодом Atlassian надає спеціальну безкоштовну ліцензію при дотриманні наступних правил:

- проект використовує ліцензії, схвалені Open Source Initiative;
- Вихідний код проекту доступний для скачування;
- у проекту є публічно доступна веб-сайт;
- програмне забезпечення від Atlassian є на веб-сайті проекту.

Система керування базами даних (СКБД, Database Management System, DBMS) – набір взаємопов'язаних даних (база даних) і програм для доступу до цих

даних. Надає можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних.

Першим поколінням СКБД прийнято вважати ієрархічні й мережеві системи. Ці системи отримали широке поширення в 1970-х роках, а першою комерційною системою цього типу була система IMS компанії IBM.

У 1980-х роках ці системи були витіснені системами другого покоління – повсюдно використовуваними і донині реляційними СКБД. У цих системах використовувалися непроцедурні мови управління даними (SQL) і передбачався значний ступінь незалежності даних. Реляційні системи внесли значні удосконалення в управління даними: графічний користувацький інтерфейс (GUI), клієнт-серверні застосунки, розподілені бази даних, паралельний пошук даних та інтелектуальний аналіз даних.

Але вже до кінця 1980-х років існуюча тоді реляційна модель перестала задовольняти розробників в силу низки обмежень. Відповіддю на зростаючу складність програм баз даних стали два нових напрямки розвитку СКБД: об'єктно-орієнтовані СКБД і об'єктно-реляційні СКБД.

У 1991 був утворений консорціум ODMG, основною метою якого стало вироблення промислового стандарту об'єктно-орієнтованих баз даних. Між 1993 та 2001 роками ODMG опублікувала п'ять ревізій своїх специфікацій. Остання версія стандарту має індекс 3.0, після чого група розпустилася. До кінця 1990-х існувало близько десяти компаній, що виробляли комерційні продукти, що позиціонуються на ринку як ООСКБД. Найбільш відомими системами даного класу стали Objectivity, Versant виробництва однойменних компаній, а також СКБД Jasmine, випущена компанією CA. Незважаючи на переваги, що дозволяють ефективніше вирішувати певний ряд завдань, об'єктно-орієнтовані системи так і не змогли завоювати значущу частку ринку СКБД, залишившись «нішевим» продуктом.

Постачальниками традиційних реляційних СКБД також була проведена значна робота з об'єднання об'єктно-орієнтованих і реляційних систем.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

Розробники постаралися розширити мову SQL, щоб включити в неї концепції об'єктно-орієнтованого підходу, зберігаючи переваги реляційної моделі (об'єктні розширення мови SQL були зафіксовані в стандарті SQL:1999).

Основний принцип – це еволюційний розвиток можливостей СКБД без поломки попередніх підходів та зі збереженням наступності з системами попереднього покоління.

Поняття СКБД третього покоління, якими, власне кажучи, і є об'єктно-реляційні СКБД, з'явилося після опублікування групою відомих фахівців в області баз даних «Маніфесту систем баз даних третього покоління». Основні принципи СКБД третього покоління, позначені в маніфесті:

Крім традиційних послуг з управління даними, СКБД третього покоління повинні забезпечити підтримку розвиненіших структур об'єктів і правил. Розвинутіша структура об'єктів характеризує засоби, необхідні для зберігання і маніпулювання нетрадиційними елементами даних (тексти, просторові дані, мультимедіа).

СКБД третього покоління повинні включити в себе СКБД другого покоління. Системи другого покоління внесли вирішальний вклад у двох областях – непроцедурний доступ за допомогою мови запитів SQL і незалежність даних. Ці досягнення обов'язково повинні враховуватися в системах третього покоління.

СКБД третього покоління повинні бути відкриті для інших підсистем. Це включає оснащення різноманітними інструментами підтримки прийняття рішень, доступом з багатьох мов програмування, інтерфейсами до існуючих популярних систем і бізнес-застосунків, можливістю запуску програм з бази даних на іншій машині і розподілені СКБД. Весь набір інструментів і СКБД має ефективно функціонувати на різноманітних апаратних платформах з різними операційними системами.

Крім того, СКБД, що розраховує на широку сферу застосування, повинна бути оснащена мовою четвертого покоління (4GL).

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

У середині 1990 років було лише кілька дослідних прототипів СКБД, які поєднали найкращі риси реляційних і об'єктно-орієнтованих СКБД. Першим комерційним продуктом, якому були властиві об'єктно-реляційні риси, став Universal Server компанії Informix(згодом була поглинена IBM). В даний час більшість цих ідей вже втілено в реальних комерційних рішеннях, в тому числі і в продуктах основних постачальників СКБД (Oracle Database і IBM DB2).

Розвиток індустрії систем керування базами даних базується на значних фундаментальних наукових дослідженнях. Найчастіше, між самими дослідженнями та їхньою конкретною реалізацією в прикладних рішеннях минають роки, а іноді й десятиліття. Роботу в області управління даними проводять як університетські дослідницькі групи (MIT, Berkeley), так і центри розробок основних постачальників СКБД (Oracle, IBM, Microsoft). Інвестування в управління даними – це довгострокове, і разом з тим, вигідне вкладення коштів. В даний час дослідники мають у своєму розпорядженні засоби, що дозволяють ефективно реалізувати найскладніші запити, що маніпулюють терабайтами й петабайтами різних даних.

Основними тенденціями, які дали привід для проведення різних масштабних досліджень в області баз даних стали:

Експонентний ріст даних. Обсяг даних, у тому числі синтетичних, що генеруються автоматизованими системами, значно зріс. Збільшилося і число прикладних областей, в яких вимагається обробка великих обсягів даних. До таких областей тепер відносяться не тільки традиційні корпоративні програми, пошук у веб, але також і наукові дослідження, обробка природних мов, аналіз соціальних мереж тощо.

Значне ускладнення структур використовуваних даних. Прості види даних у вигляді чисел і символьних рядків стали доповнятися численною мультимедійною інформацією, просторовими, процедурними даними та великою кількістю інших складних форматів.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

Широке поширення дешевих високопродуктивних апаратних засобів. Щорічно ми спостерігаємо зростання обчислювальних можливостей мікропроцесорів, збільшення ємності і зниження вартості доступних і зручних в експлуатації пристроїв дискової оперативної пам'яті.

Активний розвиток засобів комунікації та «всесвітньої павутини» World Wide Web. WWW стає єдиним інформаційним середовищем, що пронизує весь світ і об'єднує величезне число користувачів та електронних пристроїв.

Поява нових важливих областей застосування СКБД. У першу чергу, це пов'язано з інтелектуальним аналізом даних, сховищами даних, а останнім часом – з паралельними обчисленнями і хмарними технологіями.

Основні характеристики СКБД

1. Контроль за надлишковістю даних.
2. Несуперечливість даних.
3. Підтримка цілісності бази даних (коректність та несуперечливість).
4. Цілісність описується за допомогою обмежень.
5. Незалежність прикладних програм від даних.
6. Спільне використання даних.
7. Підвищений рівень безпеки.

Можливості СКБД

1. Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language)).

2. Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)

3. Можна надавати контрольований доступ до БД за допомогою: Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД; Системи керування паралельною роботою прикладних програм, яка контролює процеси спільного доступу до БД; Система відновлення – дозволяє відновлювати БД до

попереднього несуперечливого стану, що був порушений в результаті збою апаратного або програмного забезпечення.

Основні компоненти середовища СКБД

1. Апаратне забезпечення.
2. Програмне забезпечення.
3. Дані.
4. Процедури – інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.
5. Користувачі: адміністратори даних (керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних); розробники БД; прикладні програмісти; кінцеві користувачі.

Архітектура СКБД

Існує трирівнева система організації СКБД ANSI-SPARC, при якій існує незалежний рівень для ізоляції програми від особливостей представлення даних на нижчому рівні.

Рівні:

1. Зовнішній – представлення БД з точки зору користувача.
2. Концептуальний – узагальнене представлення БД, описує які дані зберігаються в БД і зв'язки між ними. Підтримує зовнішні представлення, підтримується внутрішнім рівнем.
3. Внутрішній – фізичне представлення БД в комп'ютері.

Логічна незалежність – повна захищеність зовнішніх моделей від змін, що вносяться в концептуальну модель.

Фізична незалежність – захищеність концептуальної моделі від змін, які вносяться у внутрішню модель.

4.2 Захист розробленого програмного забезпечення

Дані у програмному забезпеченні я захищаю за допомогою MISTY1. MISTY1 – блоковий алгоритм шифрування, створений для компанії Mitsubishi Electric криптологом Міцурю Мацуї. Назва є аббревіатурою Mitsubishi Improved Security Technology. Алгоритм був розроблений в 1995-1996 рр. Відомі також дві модифікації алгоритму MISTY1: MISTY2 і KASUMI

Шифр став переможцем на Європейському конкурсі NESSIE. У результаті аналізу алгоритму експерти зробили вивід, що ніяких серйозних уразливостей даний алгоритм не має (переважно, завдяки вкладеним мережам Фейстеля, що суттєво утрудняє криптоаналіз). У нього високий запас криптостійкості, алгоритм має високу швидкість шифрування й досить ефективний для апаратної реалізації.

Алгоритм був розроблений на основі теорії «підтвердженої безпеки» проти диференціального й лінійного криптоаналізу. Цей алгоритм був спроектований, щоб протистояти криптоатакам, відомим на момент створення.

З моменту публікації MISTY1 було проведено багато досліджень, щоб оцінити його рівень безпеки.

Диференціальний і неможливий диференціальний криптоаналіз високого порядку ефективно застосовується до блокових шифрів з малим ступенем. Найкращі результати для обох варіантів були отримані для 5-рівневого алгоритму MISTY1 без FL функцій.

Саме FL функції й широкобітні AND/OR операції в сильно утрудняють використання диференціального криптоаналізу, що не заважає проведенню в цьому напрямку всі нових досліджень і досягненню усе більш близьких до розв'язку результатів.

Параметри вихідних даних

MISTY1 – це шифр на основі вкладених мереж Фейстеля з вар'юємим числом раундів. Рекомендоване використання 8-раундової версії, але може

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		82

використовуватися будь-яка кількість раундів, кратне 4-м. Розмір блоку вихідного тексту – 64 біта, розмір ключа – 128 біт.

Для роботи алгоритму також попередньо виконується процедура розширення ключа, яка для 8-мі раундів обчислює 1216 бітів ключової інформації з 128-бітного ключа шифрування.

Структура алгоритму

Для задоволення вимогам конкурсу NESSIE, а також для задоволення завдання мультиплатформеності, в алгоритмі MISTY1 використовувалися наступні методи шифрування:

- Логічні операції.
- Арифметичні операції.
- Операції зрушення.
- Таблиці перестановок.

Як говорилося вище, алгоритм MISTY1 заснований на «вкладених» мережах Фейстеля. Спочатку блок вихідного тексту розбивається на два 32-бітних субблоки, після чого виконується r раундів наступних перетворень[1]:

- У кожному непарному раунді обидва субблоки обробляються операцією FL
- Над обробленим субблоком виконується операція FO.
- Результат цих операцій накладається логічною операцією «, що виключає або» (XOR) на неопрацьований субблок.
- Субблоки міняються місцями. Після заключного раунду обидва субблоки ще раз обробляються операцією FL.

Операція FL

Оброблюваний 32-бітний субблок розбивається на два 16-бітних фрагмента, до яких застосовуються операції, де:

- L і R – вхідні значення лівого й правого фрагментів відповідно;
- L' і R' – вихідні значення;

– i – фрагменти j -го підключа i -го раунду для функції FL (процедура розширення ключа докладно описана далі);

– i – побітові логічні операції «і» і «або» відповідно.

Операція FO

Саме ця функція є вкладеною мережею Фейстеля. Тут, як і раніше, виконується розбивка вхідного значення на два 16-бітних фрагмента, що проходять 3 раунду наступних перетворень:

– На лівий фрагмент операцією XOR накладається фрагмент ключа, де k – номер раунду функції FO.

– Лівий фрагмент обробляється операцією FI.

– На лівий фрагмент накладається операцією XOR значення правого фрагмента.

– Фрагменти міняються місцями.

Після третього раунду операції FO на лівий фрагмент накладається операцією XOR додатковий фрагмент ключа.

Операція FI

Дана операція також представляє собою третій рівень вкладеності мережі Фейстеля. На відміну від двох верхніх рівнів, дана мережа є незбалансованою: оброблюваний 16-бітний фрагмент ділиться на дві частини: 9-бітну ліву й 7-бітну праву. Потім виконуються 3 раунду перетворень, що впливають:

– Ліва частина зазнає обробці S-box. 9-бітна частина (в 1-м і 3-м раундах) обробляється таблицею S9, а 7-бітна (в 2-м раунді) – таблицею S7. Дані таблиці описані нижче.

– На ліву частину операцією XOR накладається поточне значення правої частини. При цьому, якщо праворуч 7-бітна частина, вона доповнюється нулями ліворуч, а в 9-бітної частини віддаляються ліворуч два біти.

– У другому раунді на ліву частину операцією XOR накладається фрагмент ключа раунду, а на праву – фрагмент. В інших раундах ці дії не виконуються.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		84

- Ліва й права частини міняються місцями.

Для оптимального розв'язку завдання мультиплатформеності, таблиці S7 і S9 алгоритму MISTY1 можуть бути реалізовані як за допомогою обчислень, так і безпосередньо таблицями.

Розширення ключа

Для 8 раундів алгоритму результатом процедури розширення ключа буде наступний набір ключових значень:

- 20 фрагментів ключа (), кожний з яких має розмір по 16 бітів;
- 32 16-бітних фрагмента ();
- 24 7-бітних фрагмента (при $k=4$, тобто в 4-м раунді функції FO, операція FI не виконується);
- 24 9-бітних фрагмента.

Виконується дане обчислення в такий спосіб:

1. 128-бітний ключ ділиться на 8 фрагментів ... по 16 бітів кожний.
2. Формуються значення: у якості використовується результат обробки значення функцією FI, яка в якості ключа (тобто сукупності необхідних 7- і 9-бітних фрагментів) використовує значення (якщо індекс n фрагмента ключа перевищує 8, то замість нього використовується індекс $n-8$).

Необхідні фрагменти розширеного ключа «набираються» у міру виконання перетворень із відповідних масивів і згідно з відповідними таблицями 16-бітний фрагмент ділиться на 7-бітний фрагмент і 9-бітний .

Розшифрування

Розшифрування проводиться виконанням тих же операцій, що й при зашифруванні, але з наступними змінами:

- фрагменти розширеного ключа використовуються у зворотній послідовності,
- замість операції FL використовується зворотна їй операція – FLI.

Схеми виконання функції FLI і процедури розшифрування наведено на малюнках 6 і 7 відповідно:

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		85

Методи аналізу

Як говорилося на початку розділу, диференціальний і неможливий диференціальний аналізи виявилися ефективні лише до версій шифру з меншою кількістю раундів і без операції FL [2][3]. Проте, на даний момент цей напрямок аналізу, особливе використання слабких ключів, найбільше перспективно, тому що наближене до реальних можливих допущень при використанні алгоритму.

Так само, ученим з Японії був проведений інтегральний аналіз повного алгоритму, використовуючи відкритих текстів зі складністю обчислення, рівної [4].

Лінійний аналіз дав результати тільки для 7-раундової версії шифру, і також без операції FL[5].

Так як MISTY1 створювався, у тому числі, з розрахунку на апаратну реалізацію, має сенс диференціальний аналіз, заснований на використанні атаки по помилках обчислень, що в цьому випадку наближене до реальності.

Висновок

Таким чином, була докладно описана структура алгоритму шифрування MISTY1 і розглянуті методи його аналізу, найбільш прагматичні напрямки дослідження. Далі має бути створення програмної реалізації для більш детального розгляду алгоритму й набір статистичних даних для повного дослідження й пошуку оптимального підходу до аналізу MISTY1.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблена системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Функціональних кнопок ПЗ.
- Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.
- Розділу виведення результату роботи системи.
- Розділу обрання групи даних.

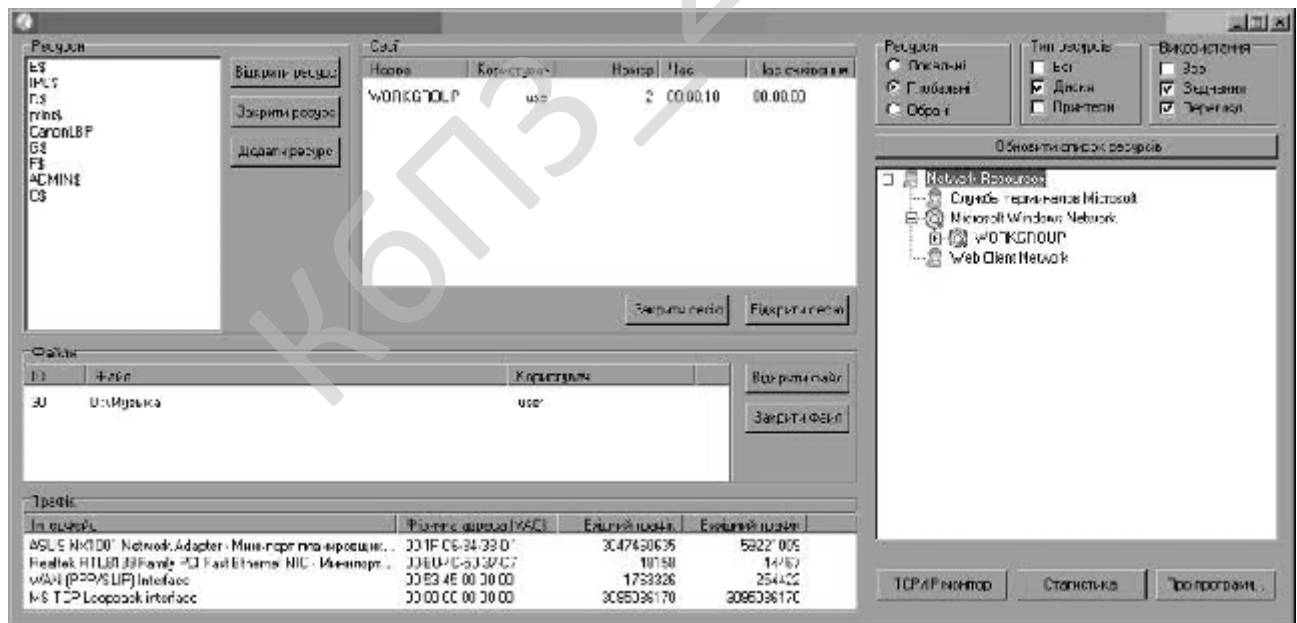


Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і 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.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

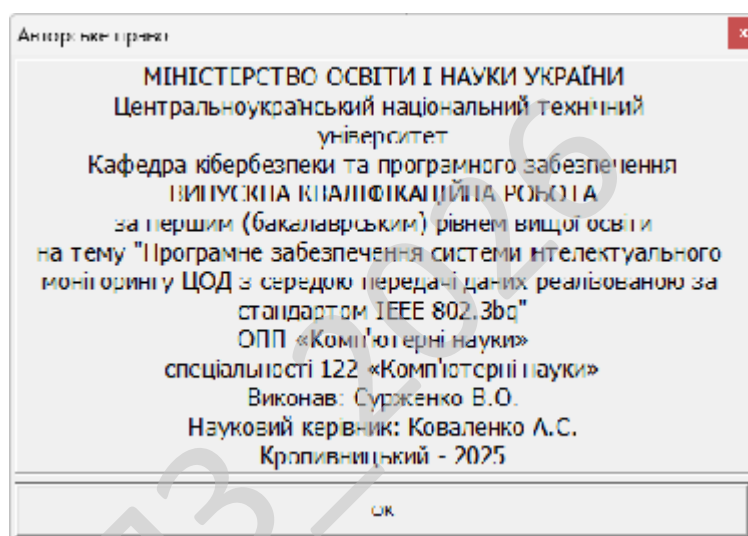


Рисунок 5.2 – Авторське право

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.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		88

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.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

- Випуск.
- Встановлення та активація.
- Деактивація.
- Адаптація.
- Оновлення.
- 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 ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ 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 ІТ 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 чорної скриньки. Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

- Як виконуються функції програми.
- Як приймаються вихідні дані.
- Як виробляються результати.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		90

– Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^{10} . Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чію поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

– Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ІТс).

– Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його ОТ).

Будь-який спосіб тестування «чорної скриньки» повинен:

– Виявити такі вхідні дані, які з високою ймовірністю належать набору ІТс;
– Сформулювати такі очікувані результати, які з високою ймовірністю є елементами набору ОТ.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

– Некоректних чи відсутніх функцій.
– Помилки інтерфейсу.;
– Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		91

- Помилки характеристик (необхідна ємність пам'яті і т.д.).
- Помилки ініціалізації та завершення.

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 спільноті 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 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.
- Досліджена система інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq.

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 створенні 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 призначені для

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		93

системи інтелектуального моніторингу ЦОД з середою передачі даних реалізованою за стандартом IEEE 802.3bq. 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 MISTY1.

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.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		94

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

2. Смірнова Т.В., Коноплицька-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.

3. 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.

4. 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.

5. 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.

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

7. 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.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		95

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools».

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		96

Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.

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

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. Smirnov O. Kuznetsov A., Zaichenko 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.*

31. Smirnov A.A., Kuznetsov 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.

32. 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

33. 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.

34. 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.

35. Смірнов О.А., Коноплицька-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.

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

37. Смірнов О.А., Дреєва Г.М., Дреєв 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.

38. Смірнов О.А., Коноплицька-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.

39. 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).

40. Смірнов О.А., Дреєва 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

41. Дреєва Г.М., Смірнов О.А., Дреєв 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.

42. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дреєв 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.

43. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Коноплицька-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.

44. 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.

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

46. Смірнов О.А., Смірнов С.А., Дідик А.К., Дреєв 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.

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

48. Смірнов О.А., Смірнов С.А., Дідик А.К., Дреєв А.М. Спосіб контролю ліній зв'язку телекомунікаційної системи антивірусу. Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. - 2016. - С. 121-127.

49. Смірнов О.А., Смірнов С.А., Дідик А.К. Метод безпечної маршрутизації метаданих у хмарні антивірусні системи. Системи озброєння та військова техніка. - Випуск 2 (46) - Х.: ХУПС - 2016. - С. 146-149.

50. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.

					ВКРБ-122.26.0029.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		101