План лекції . Тема 1. Вступ до системного моніторингу.

- Визначення системного моніторингу та його роль у сучасних інформаційних технологіях.
- Основні принципи та цілі системного моніторингу.
- Види метрик, що вимірюються при системному моніторингу.

Визначення системного моніторингу та його роль у сучасних інформаційних технологіях.

Наш предмет присвячений моніторингу серверів та комп'ютерних мереж.

Будь-яка людина, пов’язана з інформаційними технологіями знає, що моніторинг є важливим. Іноді — дуже важливим. Є, звичайно, крайність, коли фахівець сподівається дізнатися про аварійну ситуацію за дзвінками розлючених клієнтів, але ця крайність швидко переходить або на розуміння попередньої фрази, або на швидке розлучення з цим фахівцем. Можу провести аналогію: «Або системний адміністратор використовує моніторинг роботи серверів та мереж, або у нього з'являється дуже багато вільного часу та дуже мало грошей». Тож зупиняємось на тому, що моніторинг має бути. Але тут є безліч розгалужень у виборі підходу до створення системи моніторингу, її архітектури, вартості ну і нарешті глибини. І ось ми наблизилися до поняття що ж таке той самий моніторинг, які його види існують, на яких принципах він будується.

Рис. 01.01. «Спостерігачі» на «об’єкті моніторингу»

Мені дуже подобається опис ситуації на картинці з двома «спостерігачами» та «об’єктом моніторингу». На жаль я так і не знайшов першоджерело цього коміксу – власники телеграм каналів люблять щось поцупити без згадки автора. На рис.01.01 спостерігачі живуть на об’єкті, але через невірно налаштований моніторинг, чи скоріше його відсутність, мають хибне та часткове уявлення про своє місце проживання☺ чи у випадку системного адміністратора – місце своєї роботи.

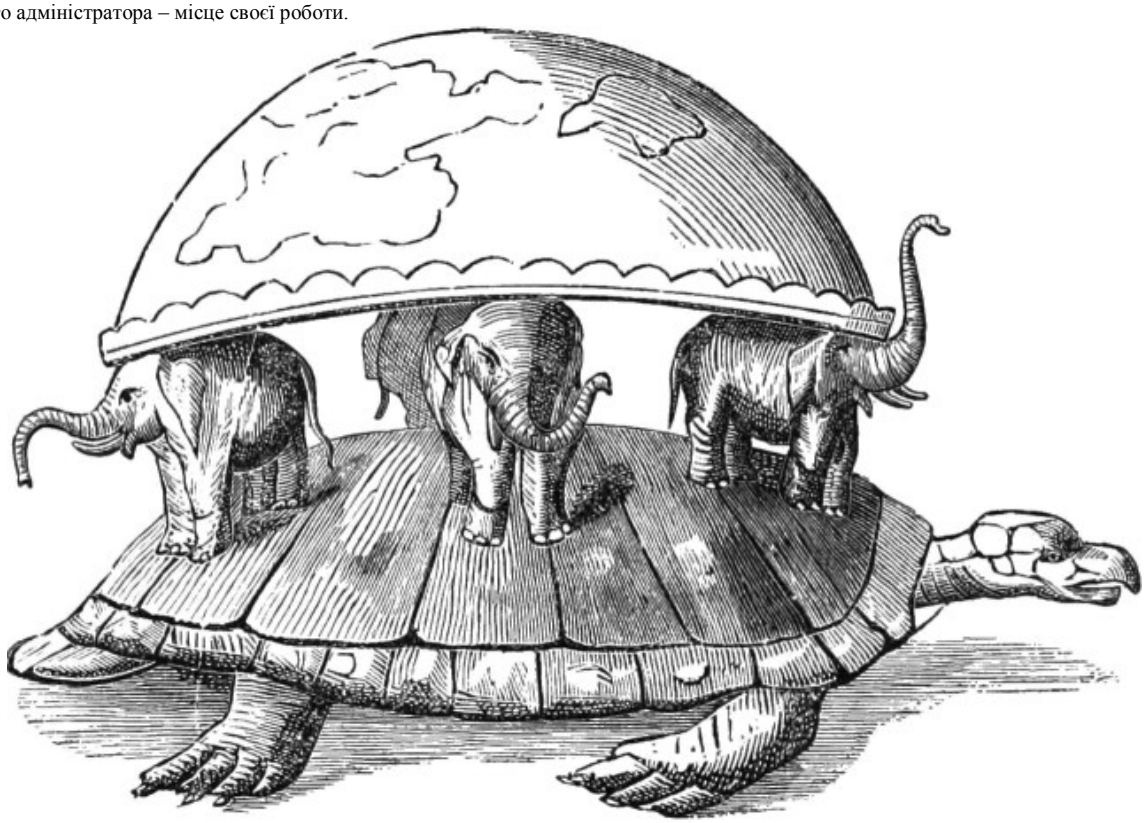


Рис. 01.02. Малюнок 1877 року, що зображує світ, що тримається на спинах чотирьох слонів, що стоять на спині черепахи.

Якщо ми почали з коміксу, буде доречним навести ще і таку ілюстрацію. Це концепція світу, що стоїть на слонах і черепасі. Вона належить до міфологічних уявлень різних культур. Найбільш відомий її варіант походить з давньоіндійської міфології, де світ зображується як диск, який тримають слони, що стоять на спині велетенської черепахи (а іноді й на спині змії або дракона). Зображення рис.01.02 є малюнком –ілюстрацією 1877 року до європейських філософськихтекстів, які популяризували ці міфи. Зображення такого типу часто публікували в енциклопедіях чи книгах XVIII–XIX століть.

Ця міфологічна концепція, хоча й далека від сучасного наукового розуміння, добре ілюструє важливість опорних структур, які забезпечують стабільність системи. Подібні принципи ми можемо побачити і в організації системного моніторингу.

Подібно до того, як на зображенні світ тримається на черепасі та слонах, система моніторингу має бути побудована на надійних 'опорах' — вірно обраних точках спостереження та ключових елементах (items). Проте важливо пам'ятати, що точка спостереження визначає наше сприйняття. Спостерігачі, які знаходилися 'всередині' системи, не могли побачити її цілком, що й призвело до помилкового уявлення про будову світу. Аналогічно, вибір неправильних або обмежених точок спостереження у системі моніторингу може створити хибне уявлення про її стан. Тому потрібно забезпечувати різнобічний та актуальний погляд на всю систему, адаптуючи моніторинг до змін у середовища.

Моніторинг є ключовою складовою управління та підтримки інформаційних систем та технологій. Існує кілька видів моніторингу, кожен з яких має свої характеристики та важливість для специфічних цілей та потреб.

Якщо ми відкриємо статтю моніторинг у Вікіпедії, то прочитаємо, що моніторинг або моніторинг (укр. спостереження) — система постійного спостереження за явищами і процесами, що проходять в навколишньому середовищі, суспільстві, результати якого слугують для обгрунтування управлінських рішень по забезпеченню безпеки людей та об'єктів/суб'єктів (наприклад, економіки).

У широкому сенсі моніторинг — це процес безперервного або регулярного (періодичного) збору інформації про стан певних параметрів об'єкту або суб'єкту спостереження (моніторингу).

Метою моніторингу може бути накопичення інформації для її подальшого аналізу та прийняття управлінського рішення, або постійне відслідковування стану об'єкту моніторингу без збереження попередньої інформації про об'єкт з метою своєчасного реагування (прийняття управлінського рішення) при певних кількісних або якісних змінах об'єкта.

Здійснення моніторингу може бути автоматизоване: при автоматичному контролі відбувається отримання і обробка інформації про стан об'єкта/суб'єкта та зовнішніх умов для виявлення подій, що визначають управлінські дії. Такою подією може бути будь-який заздалегідь заданий параметр: поява деталі з розмірами, що виходять за допустимі межі, коротке замикання електричної мережі, вихід температури за встановлене значення, аварія обладнання та інші.

Звичайно, що ми не будемо вивчати моніторинг метеорологічних явищ, чи моніторинг артеріального тиску і насиченості крові киснем у хворих на COVID – дуже актуальні види моніторингу у останні роки. Предмет вивчення присвячений тільки системному та мережевому видам моніторингу. Але, якщо розглядати сучасні види моніторингу в інформаційних системах, то їх доволі багато. Всі ці види моніторингу носять загальну назву інфраструктурний моніторинг(Infrastructure monitoring) Основні види моніторингу інформаційних систем включають:

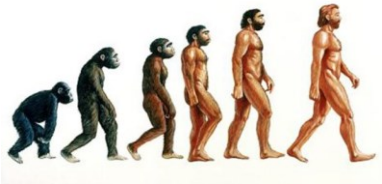
Таблиця 01.01.

Вид моніторингу	**Опис**	**Ціль моніторингу**
Системний моніторинг (System Monitoring)	Відстеження параметрів та показників, що стосуються апаратного та програмного забезпечення системи (операційна система, процесор, пам'ять, мережа тощо).	Оцінка продуктивності, надійності та ефективності системи, виявлення аномалій та проблем для швидкого реагування.
Мережевий моніторинг (Network Monitoring)	Моніторинг мережевих компонентів, трафіку та з'єднань, щоб виявити незвичайну або неправильну активність.	Забезпечення безпеки, виявлення і вирішення проблем у мережевій інфраструктурі.
Додатковий моніторинг (Application Monitoring)	Спостереження за додатками, оцінка їх продуктивності, надійності та відгуку на дії користувачів.	Оцінка роботи додатків, виявлення та усунення проблем, покращення відповідності до вимог користувачів.
Безпековий моніторинг (Security Monitoring)	Спостереження за подіями та активністю, що можуть вказувати на потенційні кіберзагрози та порушення безпеки.	Забезпечення безпеки, виявлення та запобігання кібератак, захист від несанкціонованого доступу.
Журналювання (Logging)	Запис подій, дій та стану системи та додатків для подальшого аналізу та виявлення аномалій.	Забезпечення можливості аналізу та виявлення незвичайної активності, вирішення проблем та безпеки.

Різниця між цими видами моніторингу полягає в тому, що кожен з них спрямований на відстеження та аналіз певних аспектів системи та її екосистеми. Системний моніторинг орієнтований на апаратну та програмну частину системи, мережевий - на мережеву інфраструктуру, додаткОвий - на програмні додАтки, безпековий - на виявлення загроз та захист від них, а журналювання - на реєстрацію та збереження подій для аналізу. Ці види моніторингу є однаково важливими для забезпечення ефективності, надійності та безпеки систем та додАтків. Нагадаю, що ми з Вами розглянули види інфраструктурного моніторингу (Infrastructure monitoring)

Системний моніторинг - це комплексний процес автоматичного або ручного нагляду, аналізу та оцінки параметрів та функцій певної системи або групи систем. Цей процес організується для надання повної та об'єктивної інформації про стан системи в реальному часі або на певних етапах її роботи. Основна мета - забезпечити вчасне виявлення та реагування на проблеми або відхилення в роботі системи для забезпечення її стабільності та ефективності.

Для кращого розуміння, що таке сучасний системний моніторинг необхідно коротко розглянути його еволюцію в сучасному світі IT:



- **Період зародження.**
  Початково системний моніторинг був обмеженим та базувався на мінімальних засобах.
  Основний фокус був на моніторингу апаратного забезпечення (процесор, пам'ять, диск) та базових операційних параметрів, що забезпечувалося системою агентів. Агент - це програмний компонент, що встановлюється на контрольованому об'єкті (системі, сервері, мережевому пристрої), щоб збирати та передавати метрики про його стан. Такий підхід вимагав великого обсягу адміністративної роботи для управління та підтримки системи. Пізніше ми детально розглянемо, і не тільки теоретично, поняття агентів моніторингу, метрик та інші, що зустрічаються у цій лекції.

- **Ера мереж та комп'ютерних систем.**

З поширенням мереж та зростанням складності систем з'явилися інструменти для моніторингу мережевої активності та обміну даними між системами.
Розвиток агентної та безагентної (agentless) архітектур для збору метрик на першому етапі призвів до появи централізованих систем управління агентами, що дозволяли керувати та оновлювати їх масово.
Звичайно, що використання агентів дає величезні бонуси завдяки глибокій інтеграції та доступу до детальної інформації на рівні кожної системи, а також можливість використання локальних ресурсів для обробки та аналізу даних. Є і мінуси, а саме велика кількість агентів може призвести до додаткового навантаження на систему та зменшення продуктивності.
У випадку використання агент-лесс архітектури, збір та аналіз метрик відбувається без встановлення спеціальних агентів на кожному об'єкті. Замість цього, дані можуть збиратися з централізованих джерел або використовуватися агенти, які вже присутні на об'єкті (наприклад SNMP (Simple Network Management Protocol) та WMI (Windows Management Instrumentation) протоколи, що використовуються для моніторингу та керування комп'ютерними системами та мережами).

- **Сучасні тенденції.**
  Зростання величини даних і обчислювальної потужності призвело до необхідності розвивати системи моніторингу для масштабованості.
  Поява хмарних технологій призвело до необхідності моніторингу ресурсів у віртуальних оточеннях.
  Автоматизація та використання штучного інтелекту для прогнозування та управління ресурсами.

- **Зосередження на бізнес-метриках.**
  Замість виключно технічних параметрів ставиться акцент на метриках, що впливають на бізнес-показники.
  А саме враховуються показники доступності для кінцевих користувачів і взаємозв'язку з фінансовими результатами.

- **Розширення Функціональності**.
  Розвиток інтеграції з іншими системами, такими як системи логування, моніторинг безпеки, та іншими елементами IT-екосистеми.
  Аналіз даних для прогнозування та попередження проблем заздалегідь.

Зараз системний моніторинг - це не просто інструмент для виявлення технічних неполадок, але і стратегічний елемент, що сприяє покращенню ефективності, забезпеченню надійності, та відповідності бізнес-цілям компанії.

Визначення системного моніторингу та його роль у сучасних інформаційних технологіях.

Давайте зупинимось на ролі системного моніторингу у сучасних інформаційних технологіях, а саме на значенні системного моніторингу для бізнесу та організацій:
Системний моніторинг представляє собою ключовий елемент в управлінні та забезпеченні ефективності інформаційних технологій (IT) в сучасних бізнес-середовищах. Ми пам’ятаємо, що цей процес включає систематичний нагляд за функціональністю, продуктивністю та надійністю IT-систем, дозволяючи забезпечити безперебійну роботу інфраструктури та уникнути багатьох проблем для бізнесу за порівняно невеликі кошти.
Уявімо, що Ви оволоділи навичками системного моніторингу, відчуваєте наснагу до узагальнення отриманих метрик та бажання оптимізувати за допомогою системного моніторинг інфраструктуру свого підприємства, але на Ваш жах на підприємстві він відсутній як поняття. Ну може, як залишок потуг попереднього персоналу десь «крутиться» покритий мохом сервер MRTG або покритий кактусами сервер Cacti. Це я згадав дві популярні на початку 2000-х системи вимірювання завантаженості та доступності каналів зв’язку. Їх широко використовували для перевірки т.з. білінгу з провайдером каналу зв’язку.
Ну це лірика, хоча і дуже сумна і може з Вами трапитися. Які будуть Ваші аргументи бізнес керівництву для розгортання чи удосконалення системного моніторингу:

Таблиця 01.02.

Забезпечення безперебійності роботи.	❖ Моніторинг дозволяє оперативно виявляти та вирішувати технічні проблеми, запобігаючи перебоям у роботі систем та сервісів. ❖ Передбачення можливих збоїв та їх усунення до того, як вони вплинуть на бізнес-процеси.
Підвищення продуктивності.	❖ Визначення слабких місць у системі та оптимізація ресурсів для максимальної продуктивності. ❖ Аналіз метрик дозволяє ефективно розподіляти ресурси та уникати перевантажень.
Зменшення витрат та підвищення вартості.	❖ Ефективний моніторинг може допомогти уникнути непланованих витрат на ремонт або відновлення після аварій. ❖ Оптимізація роботи системи дозволяє зменшити витрати на енергію та ресурси.

Ви маєте чітко розуміти, що стратегія IT і системний моніторинг взаємодіють для досягнення більшої ефективності та досягнення бізнес-цілей організації. І ці речі – Ваш «залізний» аргумент перед керівництвом.

Таблиця 01.03.

Вирішення стратегічних завдань.	Системний моніторинг адаптується під стратегічні цілі IT, спрямовуючи свою діяльність на вимірювання параметрів, які важливі для стратегічного успіху. Як найпростіший приклад наводимо прогнозування витрат ресурсів: Вимірювання витрат ресурсів (процесор, пам'ять, мережа) дозволяє адекватно вирахувати, які ресурси будуть потрібні для забезпечення планової доступності при зростанні користувацького попиту.
Визначення ключових показників ефективності.	Метрики, які збираються системним моніторингом, стають основою для визначення ключових показників ефективності (KPI - Key Performance Indicator) IT-стратегії. Приклад: підвищення ефективності обробки транзакцій у фінансовому додатку -визначаємо навантаження на складові фінансового додатку (application, базу даних, WEB-сервер) і у найпростішому випадку перерозподіляємо ресурси.
Прискорення прийняття рішень.	Моніторинг надає звіти у реальному, або близькому до реального часі, які допомагають приймати обгрунтовані стратегічні рішення. Тут навіть не потрібно наводити приклади – всі бачили як виглядає ситуаційна кімната, де на великих екранах малюються діаграми, а за їх динамікою слідкує персонал.

Сприяння інноваціям.	Моніторинг дозволяє вчасно виявляти нові можливості та впроваджувати інноваційні рішення, що відповідають стратегії організації, а саме оновлювати програмне забезпечення, змінювати складові «заліза», удосконалювати захист.

Зупинимось на принципах збору даних при системному моніторингу, що включають в себе наступні аспекти:

Таблиця 01.04.

Визначення ключових метрик (KPIs)	Визначте основні параметри та метрики, які ви хочете моніторити. Це можуть бути продуктивність, швидкість реакції, завантаження системи, обсяги даних тощо.
Вибір засобів моніторингу	Оберіть інструменти та програмне забезпечення, які дозволяють збирати, аналізувати та візуалізувати дані. Це можуть бути спеціальні моніторингові системи або власноруч розроблені рішення.
Налаштування моніторингу	Сконфігуруйте інструменти моніторингу для збору даних з обраних метрик та параметрів. Встановіть правила та порогові значення, за якими буде виявлено аномалії.
Збір та агрегація даних	Систематично збирайте дані з обраного спектру метрик. Це може включати отримання інформації про ресурси системи, вхідні та вихідні дані, відгуки користувачів тощо.
Аналіз та інтерпретація даних	Проводьте аналіз отриманих даних для виявлення аномалій, прогнозування проблем та визначення можливих шляхів вирішення. Порівнюйте зі значеннями KPIs та пороговими значеннями.
Візуалізація результатів	Використовуйте графіки, діаграми та інші засоби візуалізації для наглядного представлення результатів моніторингу. Це полегшить розуміння стану системи та дозволить приймати обгрунтовані рішення.
Звітність та документація	Ведіть детальну документацію процесу моніторингу, результати аналізу та прийняті рішення. Це стане важливим джерелом інформації для подальших удосконалень та оптимізацій.
Автоматизація та оптимізація	Розгляньте можливість автоматизації процесу моніторингу для ефективності та точності збору даних. На основі аналізу результатів вдосконалюйте стратегію моніторингу та параметри аналізу.

Системний моніторинг включає в себе наступні елементи:

Таблиця 01.05.

Збір даних	Це включає збір інформації про параметри системи, такі як продуктивність, використання ресурсів, стан мережі, загрози та інші важливі параметри.
Аналіз та обробка даних	Отримані дані аналізуються для виявлення аномалій, трендів, прогалин у продуктивності, вказівок на можливі проблеми або вдосконалення ефективності системи.
Візуалізація та звітність	Результати аналізу даних подаються у вигляді зрозумілих графіків, діаграм, панелей інформації, які допомагають операторам та управлінцям легше розуміти стан системи та приймати відповідні рішення.
Сповіщення та автоматизація	Системний моніторинг може включати автоматизовані процеси сповіщення про проблеми або виявлені аномалії. Це дозволяє оперативно реагувати на негативні явища та запобігати можливим збоям.
Оцінка та оптимізація	Отримані результати аналізу використовуються для оцінки ефективності системи та прийняття рішень щодо її оптимізації, покращення продуктивності та забезпечення стабільності роботи.

Сучасні інформаційні технології є невід'ємною складовою діяльності бізнесу та організацій у всіх сферах. У цьому контексті системний моніторинг має критичне значення для забезпечення надійності, ефективності та безпеки цих технологічних екосистем. Ось докладний опис ролі системного моніторингу у сучасних інформаційних технологіях:

Основні принципи та цілі системного моніторингу.

Ціль системного моніторингу полягає в забезпеченні надійності, ефективності та безпеки системи шляхом постійного спостереження за її функціонуванням та негайної реакції на будь-які невідповідності або проблеми.

Системний моніторинг грунтується на кількох ключових принципах, спрямованих на ефективне та ефективне спостереження, аналіз та управління інформаційними системами та їхніми компонентами.

Необхідно згадати таке поняття, як проактивність — уявлення про природу психіки людини. Згідно з уявленнями про проактивність психіки людини, між подразниками, що впливають на людину і її реакцією на ці подразники лежить вільна незалежна воля. Тобто ми самі вибираємо свою реакцію на ті чи інші дії. Протилежністю проактивності є реактивність, коли вибір визначається зовнішніми обставинами, стимуляцією.

Чому я згадав наче б то далеке від нашого предмету поняття психоогії? А тому, що воно використовується також і у моніторингу як антипод пасивного спостереження за об’єктами.

Перелічимо основні принципи проактивного моніторингу та реагування на проблеми. Це узагальнені принципи, які справедливі для більшості видів моніторингу:

Таблиця 01.06.

Проактивність	❖ Системний моніторинг передбачає постійний нагляд за параметрами системи для виявлення можливих проблем чи відхилень ще до того, як вони стануть критичними. ❖ Проактивність дозволяє адміністраторам та інженерам уникати серйозних збоїв та реагувати на відхилення задовго до впливу на користувачів чи бізнес-процеси.
Автоматизоване сповіщення	❖ Використання систем автоматичного сповіщення для оперативного повідомлення адміністраторів про виявлені аномалії чи проблеми. ❖ Автоматичне сповіщення дозволяє вчасно реагувати та вирішувати проблеми, навіть якщо адміністратор не постійно на зв'язку.
Прогнозування проблем	❖ Використання аналітики та алгоритмів прогнозування для виявлення тенденцій та передбачення можливих проблем на основі зібраних даних. ❖ Прогнозування проблем дозволяє приймати запобіжні заходи та уникнути можливих негативних наслідків.

Деякі джерела надають більш розгорнутий перелік принципів системного моніторингу. Він виглядає наступним чином:

Таблиця 01.07.

Цільова орієнтованість (Goal-Oriented)	Моніторинг повинен бути спрямований на досягнення конкретних цілей та задач. Цілі можуть включати покращення продуктивності, забезпечення безпеки, забезпечення надійності, оптимізацію ресурсів тощо. Вся система моніторингу повинна бути адаптована до цих цілей.
Реалізація метрик та показників (Metrics and Indicators)	Моніторинг повинен включати визначення та вимірювання ключових метрик та показників, які відображають стан системи. Це може бути продуктивність, завантаження, швидкість відгуку, використання ресурсів та інші важливі параметри.
Континуїтет та постійність (Continuous Monitoring)	Системний моніторинг повинен бути постійним та безперервним процесом. Це дозволяє вчасно виявляти зміни, аномалії та проблеми у системі, щоб оперативно реагувати та уникнути серйозних наслідків.
Автоматизація та інтеграція (Automation and Integration)	Автоматизація збору та аналізу даних є ключовим принципом. Це дозволяє оптимізувати час та ефективність процесу моніторингу. Інтеграція моніторингу з іншими інструментами та системами теж важлива для забезпечення повноцінного управління системою.
Виявлення та попередження (Detection and Alerting)	Система моніторингу повинна бути здатна вчасно виявляти аномальні стани, відхилення та проблеми. Крім цього, важливо мати систему сповіщень, яка негайно повідомляє відповідальних осіб про виникнення проблем.
Скорочення "шуму" (Noise Reduction)	Моніторинг повинен бути спрямований на виділення суттєвих змін та проблем, уникання зайвого "шуму" в інформації. Це дає можливість концентруватися на дійсно важливих подіях та проблемах.
Скалабельність та гнучкість (Scalability and Flexibility)	Системний моніторинг повинен бути побудований таким чином, щоб ефективно працювати як для невеликих, так і для великих систем, а також бути гнучким та адаптованим до змін у вимогах та конфігураціях систем

А тепер коротко про цілі системного моніторингу, такі як покращення доступності, продуктивності та безпеки систем:

Таблиця 01.08.

Ціль системного моніторингу	Мета цілі	Заходи забезпечення
Покращення доступності Ensuring continuous availability.	Забезпечення неперервної доступності систем та послуг для користувачів.	Моніторинг функціональності та виявлення точок можливого збою, щоб уникнути перебоїв у роботі.
Підвищення продуктивності Increasing task execution efficiency.	Максимізація ефективності використання ресурсів та оптимізація продуктивності системи.	Моніторинг ресурсів, виявлення перевантажень, оптимізація алгоритмів та розподіл ресурсів для максимальної продуктивності.
Забезпечення безпеки систем Ensuring system security.	Захист системи від потенційних загроз та вразливостей.	Моніторинг активності, виявлення підозрілих або нестандартних взаємодій, вдосконалення системи безпеки на основі зібраних даних.
Оптимізація ресурсів Optimization of resource utilization.	Раціональне використання ресурсів для максимальної продуктивності при мінімальних витратах.	Моніторинг використання ресурсів (процесор, пам'ять, мережа), розподіл завдань, ідентифікація ефективних алгоритмів роботи.

Ці принципи та цілі системного моніторингу допомагають забезпечити стабільність, ефективність та безпеку інформаційних систем у сучасному IT-середовищі.

Види метрик, що вимірюються при системному моніторингу.

Метрика у контексті системного моніторингу є стандартизованим способом вимірювання певних характеристик та параметрів системи, щоб оцінити її продуктивність, надійність, ефективність та інші аспекти функціонування. Це ключовий елемент для аналізу та оцінки роботи системи та прийняття обґрунтованих управлінських рішень.

Технічні метрики

Зрозуміло, що метрика у моніторингу це свого роду лінійка для вимірювання деяких показників чи параметрів. Якщо говорити про види метрик, то "**Технічні метрики**", "**Метрики доступності**" і "**Бізнес метрики**" є основними та ключовими категоріями метрик, але є ще декілька інших важливих видів метрик, які можна врахувати в класифікації.

- **Споживання ресурсів.** Оцінює використання ресурсів, таких як електроенергія, батарея, простір для зберігання, та інші.
- **Метрики безпеки.** Визначають рівень безпеки системи, включаючи виявлення загроз, управління доступом та аудиторію.
- **Метрики ефективності.** Вимірюють ефективність процесів та робочих потоків в організації чи системі.
- **Метрики відновлення (Recovery Metrics).** Оцінюють час відновлення послуги або системи після виникнення збоїв.
- **Метрики користувацького досвіду.** Визначають якість та задоволення користувача при використанні системи або сервісу.
- **Метрики навантаження (Load Metrics).** Моніторять обсяг роботи, який система чи сервіс повинен обробити в певний період часу.
- **Метрики вартості (Cost Metrics).** Визначають витрати та ефективність з точки зору фінансового аспекту.

До речі, кожна метрика, у міру своїх характеристик, може одразу входити у кілька різних класів. Як наприклад основні технічні метрики є також базовими метриками у метриках споживання ресурсів.
Детальніше зупинимось на технічних метриках.

Технічні метрики - це конкретні вимірювання технічних параметрів чи характеристик в інформаційних технологіях та комп'ютерних системах. Ці метрики використовуються для кількісної оцінки та відстеження різних аспектів функціонування технічних систем з метою покращення їхньої продуктивності, надійності, ефективності та безпеки. Технічні метрики включають в себе вимірювання різних ресурсів (таких як процесор, пам'ять, диск) і параметрів мережі, часу реакції системи, завантаження серверів, швидкості передачі даних тощо. Вони є ключовим інструментом у системному моніторингу та управлінні IT-системами.

При виборі технічних метрик для моніторингу важливе значення відіграють граничні значення технічних метрик, що визначаються для вчасного виявлення аномалій, попередження можливих проблем та ефективного управління ресурсами системи. Встановлення граничних значень базується

на специфікаціях системи, її вимогах та типі діяльності. Загальний підхід до визначення граничних значень для типових технічних метрик наведено у таблиці 01.09. Перелічимо основні технічні метрики

Таблиця 01.09.

Технічна метрика	Опис метрики	Значення метрики	Граничні (порогові) значення метрики
Використання процесора	Визначає, який відсоток обчислювальної потужності процесора використовується.	Високе використання процесора може вказувати на перевантаження, що може призвести до зниження продуктивності.	**Ultra Low**: Less than 10% CPU usage. **Normal**: 10-70% usage. **Warning**: 70-90% usage. **Critical**: More than 90% utilization.
Використання пам'яті	Відображає відсоток доступної оперативної пам'яті, яка використовується системою	Високе використання пам'яті може свідчити про неефективне використання ресурсів або потребу в додатковій пам'яті.	**Ultra Low**: Less than 20% memory usage. **Normal**: 20-70% usage. **Warning**: 70-90% usage. **Critical**: More than 90% utilization.
Використання дискового простору	Вимірює, який обсяг дискового простору використовується на системному диску.	Високе використання може сигналізувати про недостатність місця та необхідність оптимізації або розширення простору.	**Ultra Low**: Less than 30% disk space usage. **Normal**: 30-70% usage. **Warning**: 70-90% usage. **Critical**: More than 90% utilization.
Пропускна здатність мережі	Вимірює кількість даних, які можуть бути передані через мережу за певний час.	Зменшення пропускної здатності може вказувати на проблеми з мережею, що впливають на швидкість передачі даних.	**Ultra Low**: More than 80% available bandwidth. **Normal**: 50-80% usage. **Warning**: 30-50% usage. **Critical**: Less than 30% usage.
Відповідь сервера	Час, який сервер витрачає на обробку та відповідь на запити.	Довгий час відповіді може призвести до низької продуктивності та погіршення враження користувачів.	**Ultra low**: Response less than 100ms. **Normal**: 100-500 ms. **Warning**: 500-1000 ms. **Critical**: More than 1000 ms.
Кількість запитів до бази даних	Кількість запитів, які виконуються в базі даних за певний час.	Збільшення цього показника може вказувати на підвищений обсяг роботи з базою даних та потребу в оптимізації.	**Ultra Low**: Less than 100 requests per minute. **Normal**: 100-500 requests. **Warning**: 500-1000 requests. **Critical**: More than 1000 requests.
Швидкість передачі даних	Визначає швидкість передачі даних між компонентами системи чи зовнішніми ресурсами.	Повільна швидкість передачі може впливати на продуктивність та реакцію системи на користувацькі запити.	**Ultra Low**: More than 1 Mbps of free bandwidth. **Normal**: 500 kbps - 1 Mbps of used bandwidth. **Warning**: 200 Kbps - 500 Kbps of used bandwidth. **Critical**: Less than 200 kbps of free bandwidth.

Наведені у таблиці 01.09 граничні значення технічних метрик є лише прикладом, який базується на «чистій теорії» та аналізі трендів. Тому необхідно відмітити три моменти при встановленні граничних значень метрик

- **Контекст застосування**: Граничні значення слід визначати, враховуючи конкретні вимоги та характеристики системи.
- **Аналіз трендів**: Застосування аналізу трендів та історичних даних для визначення оптимальних граничних значень.
- **Поглиблений моніторинг**: Для деяких систем може бути необхідно використовувати більш детальні граничні значення для конкретних компонентів.

Установлення граничних значень метрик моніторингу - це ітеративний процес, який вимагає постійного відстеження та аналізу, оскільки вони можуть змінюватися в залежності від потреб системи та змін у її навколишньому середовищі.

Як приклад зі своєї практики можу згадати, що метрики використання ЦП необхідно підбирати для кожного серверу індивідуально. Для деяких систем завантаження 91-92% (особливо хмарних серверів) це нормально і дозволяє суттєво економити бюджет на цих серверах. Також є сенс виключати якісь некритичні для функціонування системи об'єкти з моніторингу: DVD-приводи (фізичні або змонтовані), підключені мережеві диски, які відслідковуються на своїх серверах, тимчасові диски хмарних серверів.
Тепер, коли ми розглянули основні технічні метрики, зрозуміло, що вони відіграють ключову роль у системному моніторингу, допомагаючи забезпечити ефективність, надійність та оптимальне використання ресурсів у IT-інфраструктурі.

Метрики доступності

Тепер зупинимось на такому класі метрик, як метрики доступності у відношенні системного моніторингу.

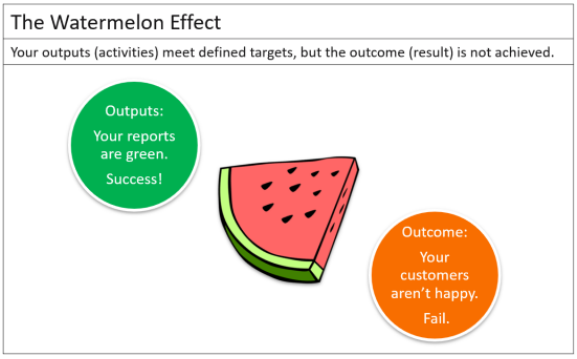
Метрики доступності в системному моніторингу визначаються як конкретні вимірювання, які оцінюють доступність та надійність інформаційної системи чи сервісу. У контексті системного моніторингу ці метрики визначають ступінь готовності та працездатності системи для виконання своїх завдань. Додатково, ці метрики дозволяють визначати і враховувати час відмов та час відновлення.

Що ж таке та сама доступність? Доступність означає здатність елемента конфігурації або IT-послуги виконувати узгоджену функцію, коли це необхідно. Доступність розраховується за допомогою рівняння:

$$Availability\% = \frac{(Agreed\ Service\ Time - DownTime)}{Agreed\ Service\ Time}$$

Agreed Service Time - узгоджений час обслуговування – це очікуваний час, коли послуга працюватиме. Якщо ваш рівень обслуговування визначає, що користувачі повинні мати доступ до системи хмарного бекапу з 6:00 ранку до півночі в робочі дні, узгоджений час обслуговування становить 18 годин/1080 хвилин/64 800 секунд на робочий день.
DownTime - час простою – це час, протягом якого послуга недоступна протягом узгодженого часу.
Доступність вимірюється як відсоток часу, протягом якого послуга або елемент конфігурації доступні. Він звітує про минуле та оцінює майбутнє служби. Він говорить, наскільки добре послуга працювала протягом періоду вимірювання.
Показники доступності також оцінюють, наскільки добре послуга працюватиме в майбутньому. У нашому прикладі доступності системи хмарного бекапу середня доступність 99,99% передбачає, що ми можемо очікувати середній час безвідмовної роботи нашої служби 17,9982 годин/1079,892 хвилин/64 793,52 секунд на день. Ми можемо порівняти розраховані дані з обіцяною доступністю, щоб визначити, чи досягаємо ми своїх бізнес-цілей.

Дуже дивно, але класна статистика доступності не завжди перетворюється на хороші результати для клієнтів. Тут може мати місце маркетингово-психологічний термін, що носить назву «ефекту кавуна», коли постачальник послуг досягає мети вимірювання, але не підтримує бажані результати клієнта.
Припустімо, ви постачальник телекомунікаційних послуг із щотижневою доступністю 99,9% (0,1% або 10 хвилин простою на тиждень). Але цей простой у 0,1% відбувається під час інтенсивних подій, таких як звітний день, коли необхідно перелити по каналам велику кількість даних, або під час відеоконференції у момент заключення дуже вигідного контракту. Цільові показники доступності досягнуто, але ваші клієнти незадоволені. Це класичний візерунок кавуна, зелений (добре) зовні, червоний (погано) всередині.



Виділяють три основних метрики доступності:

Таблиця 01.10.

Назва метрики	Визначення метрики	Опис метрики
Доступність системи System Availability	Доступність системи визначає, як часто система знаходиться в стані готовності та працездатності без відмов.	Ця метрика вимірюється у відсотках та вказує на частоту, з якою система може виконувати свої функції без перебоїв.
Час відмови Downtime	Час відмови представляє собою період, протягом якого система або сервіс не доступний або не працює належним чином.	Вимірюється в одиницях часу (години, хвилини), ця метрика вказує на тривалість відмов та ступінь впливу на доступність.
Час відновлення Recovery Time	Час відновлення вказує, як швидко система може бути відновлена до нормальної робочої діяльності після виникнення відмови.	Ця метрика вимірюється у відсотках або конкретних одиницях часу та вказує на ефективність процесів відновлення.

Ці метрики дозволяють визначити рівень надійності та готовності системи, її доступність для користувачів та взаємозв'язок з продуктивністю. Зрозуміло, що метрики доступності відіграють роль для споживача лише поки система в цілому зберігає працездатність. Тут можна навести безліч прикладів. Самий яскравий, та життєвий приклад, з яким ми всі регулярно маємо справу – доступність інтернету. Вам, як клієнту, провайдер може розповідати про час відновлення 30 хв, але якщо зв'язок зник у важливий для нас відрізок часу, значення метрик доступності відіграє якусь роль лише для самого провайдера.
А тепер розглянемо ще дві метрики, а саме
MTBF (Mean Time Between Failures) та
MTTR (Mean Time To Recovery)
Вони тісно пов'язані з метриками доступності, але вони представляють інші сторони оцінювання надійності та швидкості відновлення системи.

Таблиця 01.11.

Назва метрики	Визначення метрики	Опис метрики
Час безвідмовної роботи системи (MTBF) Mean Time Between Failures Середній час між відмовами	Час безвідмовної роботи (MTBF) вимірює середню тривалість часу між виникненням двох послідовних відмов системи чи компонента.	MTBF вказує на середню тривалість, протягом якої система очікується, що буде функціональною перед тим, як виникне нова відмова. Вищий показник MTBF вказує на більшу надійність системи.
Час відновлення послуги (MTTR) Mean Time To Recovery Середній час відновлення	Час відновлення послуги (MTTR) вимірює час, необхідний для відновлення системи чи послуги після виникнення відмови.	MTTR оцінює ефективність та швидкість відновлення системи після перебоїв. Менший MTTR свідчить про більшу ефективність відновлення та менший вплив відмови на користувачів.

Ці метрики грають ключову роль у вимірюванні та управлінні доступністю системи, допомагаючи прогнозувати та зменшувати відмови та час відновлення для забезпечення найкращого можливого рівня обслуговування для користувачів.

Таблиця 01.12.

Назва метрики	Відношення до доступності	Пов'язаність зі списком метрик
MTBF Середній час між відмовами	Обернено пропорційний до частоти відмов системи. Високий MTBF вказує на низьку частоту відмов, що, в свою чергу, підвищує загальну доступність системи.	MTBF може розглядатися як компонент доступності, але більше відображає ймовірність безвідмовної роботи протягом певного періоду.
MTTR Середній час відновлення	Прямо пропорційний до швидкості відновлення системи після відмови. Має велике значення для скорочення часу відмови та покращення доступності.	MTTR є важливою частиною оцінки доступності, оскільки відображає, як швидко система може повернутися до нормальної роботи після виникнення проблеми.

Іншими словами, MTBF та MTTR не є прямими включеннями до списку метрик доступності, але вони є критичними компонентами для визначення, наскільки доступна та надійна система. Загальний підхід може виглядати так: високий MTBF сприяє підвищенню доступності, а коротший MTTR допомагає зменшити час відмови та покращити загальну доступність системи.

Бізнес-метрики

Тепер згадаю таку начеб то зовсім не технічну річ, як бізнес-метрики.

Бізнес-метрики - це конкретні кількісні та якісні вимірювання, які використовуються для оцінки впливу інформаційних технологій та інших бізнес-процесів на стратегічні та фінансові результати організації. Ці метрики допомагають визначити, наскільки ефективно використовуються ресурси, як вони впливають на задоволення клієнтів, фінансові показники та інші аспекти діяльності компанії.

Визначальні риси бізнес-метрик включають:

Таблиця 01.13.

Орієнтованість на стратегічні цілі	Бізнес-метрики повинні бути прив'язані до стратегічних цілей організації та допомагати визначити, наскільки успішно вони досягаються.
Кількісний та якісний характер	Метрики можуть бути числовими (наприклад, прибуток, витрати) або якісними (наприклад, задоволення клієнтів).
Взаємозв'язок з бізнес-процесами	Вони повинні відображати результати та ефективність ключових бізнес-процесів організації.
Відстеження змін в часі	Метрики можуть використовуватися для відстеження змін в часі, що дозволяє організації визначати тенденції та аналізувати ефективність за період.
Орієнтованість на кінцевого користувача	Вони часто відображають вплив на клієнтів, які можуть бути замовниками, споживачами, чи іншими зацікавленими сторонами.
Порівняння та бенчмаркінг	Метрики можуть використовуватися для порівняння результатів зі стратегічними цілями, або з результатами подібних організацій (бенчмаркінг).

Ось деякі типові бізнес-метрики:

Таблиця 01.14.

Назва бізнес-метрики	**Характеристика**	**Розрахунок**
ROI (Return on Investment)	Вимірює відношення прибутку від вкладеного капіталу або інвестицій до їхньої вартості.	$$ROI = \frac{(\text{Прибуток} - \text{Вартість інвестицій})}{\text{Вартість інвестицій}} \times 100\%$$
TCO (Total Cost of Ownership)	Визначає загальну вартість володіння та утримання IT-системи протягом всього періоду експлуатації.	$$TCO = \text{Вартість придбання} + \text{Вартість експлуатації} + \text{Вартість обслуговування}$$
Customer Lifetime Value (CLV)	Визначає прибуток, який очікується від одного клієнта протягом всього його перебування в системі.	$$CLV = \text{Середній дохід на клієнта} \times \text{Середній термін обслуговування клієнта}$$
Conversion Rate	Визначає відсоток користувачів, які здійснили бажану дію, наприклад, покупку, реєстрацію чи завантаження.	$$Conversion\ Rate = \frac{(\text{Кількість бажаних операцій})}{\text{Загальна кількість відвідувачів}} \times 100\%$$
Churn Rate	Визначає відсоток користувачів, які припинили використання послуг або продуктів компанії.	$$Churn\ Rate = \frac{(\text{Кількість відтоку клієнтів})}{\text{Загальна кількість клієнтів на початку періоду}} \times 100\%$$

Ці метрики допомагають бізнес-лідерам розуміти вартість та вплив IT-систем на стратегічні та фінансові аспекти діяльності компанії.

Необхідно згадати ще дві важливі бізнес-метрики, які допомагають оцінити ефективність IT-інфраструктури та визначити стратегії її вдосконалення. Це

- **Витрати на технічне обслуговування та відновлення після збоїв** та
- **Втрати доходу внаслідок перерв у роботі системи**

- Таблиця 01.15.

Витрати на технічне обслуговування та відновлення після збоїв.	• **Визначення витрат на технічне обслуговування.** Витрати на технічне обслуговування можуть включати в себе витрати на утримання та обслуговування обладнання, витрати на віддалене адміністрування, зарплати технічного персоналу, витрати на оновлення програмного забезпечення тощо. • **Визначення витрат на відновлення після збоїв.** Витрати на відновлення включають в себе витрати на роботу збійної системи, вартість втраченого часу праці персоналу, витрати на відновлення даних, витрати на відновлення та поновлення служб та інфраструктури.
Втрати доходу внаслідок перерв у роботі системи	• **Визначення втрат доходу.** Втрати доходу можна розрахувати, враховуючи втрати прибутку за час перерви у роботі системи. Це може включати втрати від простою обслуговування клієнтів, можливі втрати партнерів, іміджеві втрати та інші фінансові втрати. • **Визначення тривалості перерви.** Дані про тривалість перерви можуть бути зібрані через системний моніторинг, журнали відмов, інформаційні системи для керівництва або від звітів технічного персоналу. • **Визначення втрат прибутку.** Втрати доходу можна розрахувати, помноживши тривалість перерви на прогнозований або фактичний обсяг прибутку на одиницю часу.

	• **Оцінка впливу на клієнтів та імідж компанії.** Дані про вплив на клієнтів та імідж можуть бути отримані через відгуки клієнтів, соціальні мережі, або інші канали комунікації з клієнтами.

Ці метрики можна відстежувати та розраховувати, використовуючи системи моніторингу, логи подій, аналітичні інструменти та внутрішні дані компанії. Важливо враховувати потреби бізнесу та налаштовувати системний моніторинг для збору необхідних даних для ефективного визначення цих величин.
І на завершення лекції, хотілося б підсумувати, що метрики в системному моніторингу охоплюють різні аспекти системи та її функціонування. Вони дозволяють вимірювати та оцінювати різноманітні параметри, які є ключовими для надійності, ефективності та безпеки систем. Основні типи метрик у системному моніторингу включають:

- Таблиця 01.16.

Продуктивність **Performance Metrics**	• Час відгуку (Response Time): Час, який система витрачає на обробку запиту та надсилання відповіді. • Кількість оброблених запитів на одиницю часу (Requests per Second): Кількість запитів, які система може обробити протягом секунди. • Тривалість виконання операцій (Operation Duration): Середній час, який витрачається на виконання конкретних операцій.
Використання ресурсів **Resource Utilization Metrics**	• Використання центрального процесора (CPU Utilization): Відсоток використання обчислювальної потужності процесора. • Використання оперативної пам'яті (Memory Utilization): Відсоток використання доступної оперативної пам'яті. • Використання мережевого трафіку (Network Traffic Utilization): Кількість переданих даних через мережу в порівнянні з доступною пропускною спроможністю.
Надійність та доступність **Reliability and Availability Metrics**	• Час доступності (Uptime): Відсоток часу, протягом якого система була доступною для користувачів. • Кількість збоїв (Number of Failures): Кількість виявлених проблем або відмов системи.
Безпека **Security Metrics**	• Кількість виявлених кібератак (Number of Detected Cyber Attacks): Кількість спроб несанкціонованого доступу до системи. • Рівень захисту (Security Posture): Оцінка загального рівня захищеності системи та дотримання правил безпеки.
Масштабованість **Scalability Metrics**	• Розмір та обсяг даних (Data Size and Volume): Кількість та обсяг даних, які система може ефективно обробляти та зберігати. • Масштабованість додатку (Application Scalability): Ефективність додатку при збільшенні навантаження та обсягу користувачів.
Витрати **Cost Metrics**	• Витрати на обслуговування (Maintenance Costs): Сума грошей, витрачених на підтримку та обслуговування системи протягом певного періоду.
Інші метрики **Other Metrics**	• Скарги користувачів (User Complaints): Кількість та характер скарг від користувачів щодо функціонування системи.

Ці метрики важливі для ефективного моніторингу та управління системою, дозволяючи оцінювати різні аспекти її роботи та вживати заходів для покращення продуктивності, надійності та безпеки.

Висновки.
У ході лекції ми занурювались у світ системного моніторингу, розкриваючи його визначення, роль у сучасних інформаційних технологіях та основні принципи та цілі. Системний моніторинг виявився ключовим елементом сучасного IT-пейзажу, забезпечуючи нагляд та управління найважливішими аспектами інфраструктури та сервісів.

Визначивши системний моніторинг як процес збору та аналізу даних про стан системи, виявилось, що його роль в сучасних IT-технологіях непереоціненна. Цей інструмент дозволяє не лише реагувати на поточні проблеми, а й передбачати їх, щоб уникнути серйозних відмов та оптимізувати ресурси.

Основні принципи та цілі системного моніторингу виявилися спрямованими на забезпечення доступності, надійності та ефективності інфраструктури. Ми розглянули важливість вчасного виявлення аномалій, моніторингу різних аспектів, таких як продуктивність, безпека та використання ресурсів.

Окрему увагу ми приділили видам метрик, які вимірюються при системному моніторингу. Використовуючи технічні метрики, такі як використання процесора, пам'яті, дискового простору та інші, системи можуть отримати повний обсяг інформації про свій стан та продуктивність.

Системний моніторинг - це не тільки інструмент для виявлення проблем, але і стратегічний ресурс для вдосконалення та оптимізації роботи IT-інфраструктури. Правильне впровадження та налагодження системного моніторингу є важливим етапом для забезпечення стабільності та ефективності сучасних інформаційних систем.

Закінчу цю лекцію так само, як і почав.
Будь-який системний адміністратор знає, що моніторинг є важливим. Іноді — дуже важливим.