



УДК 621.491

ТЕХНОЛОГІЯ ПРОВЕДЕННЯ КОМПЛЕКСНОГО ІТ-МОНІТОРИНГУ КОМПАНІЇ

Ірина Данилюк; Людмила Будник

Західноукраїнський національний університет, Тернопіль, Україна

Резюме. Присвячено розкриттю процесу здійснення комплексного ІТ-моніторингу компанії. Моніторинг ІТ-інфраструктури важливий процес, допомагає компанії відстежити зміни в інфраструктурі. Метою моніторингу є збирання та аналіз даних щодо ІТ-сервісів, компонентів інформаційної інфраструктури та використання отриманих даних для контролю всіх елементів, запобігання збоїв, помилок, з рештою, безпека компанії. Для здійснення моніторингу використовують спеціалізовані системи моніторингу ІТ-інфраструктури, вони збирають усі необхідні дані, об'єднують в єдину базу даних, де відбувається структуризація та аналіз. Шляхом постійного моніторингу різних параметрів та метрик, таких, як завантаженість системи, доступність ресурсів процесора, швидкодія мережі, використання ресурсів процесора, пам'яті, дискового простору, завчасно можна виявити певні проблеми та вжити необхідні заходи щодо їх усунення. ІТ-моніторинг включає в себе використання великої кількості різноманітних інструментів та технологій, зокрема: монітори ресурсів, системи сповіщень, журнали подій, аналітичні звіти, панелі управління, що допомагають отримувати, аналізувати, візуалізувати дані про стан ІТ-інфраструктури та сервісів. Відповідність системи моніторингу встановленим метрикам та показникам дозволяє забезпечити ефективну роботу ІТ-систем, швидко реагувати на виникаючі проблеми (виявляти операційні проблеми, несправність устаткування), визначати можливі порушення безпеки (зловмисні атаки) та планувати майбутні ресурси. Моніторинг є необхідним елементом управління ІТ-середовища, оскільки він дозволяє виявляти, контролювати, вирішувати проблеми, що виникають у інфраструктурі та впливають на якість і продуктивність ІТ-сервісів. Ефективний моніторинг сприяє покращенню доступності, продуктивності та якості ІТ-сервісів, що, у свою чергу, сприяє досягненню бізнес-цілей, задоволенню потреб користувачів. Особливу увагу в статті приділено елементам ІТ-інфраструктури, що підлягають моніторингу (сервери, мережеві пристрої, бази даних, програмне забезпечення), оскільки моніторинг зазначених елементів дозволяє оперативно виявляти проблеми, контролювати ресурси, вживати вчасно заходи для їх вирішення.

Ключові слова: моніторинг, ІТ-інфраструктура, ІТ-сервіси, інструменти, база даних, сервери, мережеве обладнання, безпека, аномалії, апаратне забезпечення.

https://doi.org/10.33108/galicianvisnyk_tntu2024.02.040

Отримано 25.01.2024

UDC 621.491

TECHNOLOGY OF CARRYING OUT A COMPREHENSIVE IT MONITORING OF THE COMPANY

Iryna Danylyuk; Liudmyla Budnyk

West Ukrainian National University, Ternopil, Ukraine

Summary. The article is devoted to the disclosure of the process of carrying out comprehensive IT monitoring of the company. IT infrastructure monitoring, an important process, helps a company track changes in the infrastructure. Monitoring purpose is the collection and analysis of IT services data, components of the information infrastructure and use received data to control all elements, prevent failures, errors, and finally, for the company's security. For monitoring, specialized IT infrastructure monitoring systems are used, they collect all the necessary data, combine them into a single database, where structuring and analysis takes place. By constantly

monitoring various parameters and metrics, such as system load, availability of processor resources, network speed, usage of processor resources, memory, and disk space, certain problems can be identified in advance and take the necessary measures to eliminate them. IT monitoring includes the use of various tools and technologies, in particular: resource monitors, notification systems, event logs, analytical reports, control panels that help to obtain, analyze, visualize data on the state of IT infrastructure and services. The compliance of the monitoring system with established metrics and indicators allows to ensure IT system efficiency, quickly respond to emerging problems (identify operational problems, equipment malfunction), identify possible security breaches (malicious attacks) and plan future resources. Monitoring is a necessary element of IT environment management, as it allows to identify, control, and solve problems that arise in the infrastructure and affect the IT services quality and performance. Effective monitoring helps to improve the availability, productivity, and quality of IT services, which, in turn, helps to achieve business goals and meet user needs. Particular attention in the article was paid to the elements of the IT infrastructure that are subject to monitoring (servers, network devices, databases, software), since the monitoring of these elements allows quickly identify problems, control resources, and take timely measures to solve them.

Key words: monitoring, IT infrastructure, IT services, tools, database, servers, network equipment, security, anomalies, hardware.

https://doi.org/10.33108/galicianvisnyk_tntu2024.02.040

Received 25.01.2024

Постановка проблеми. Сьогодні важко уявити сучасний об'єкт господарювання, бізнес-середовище без належної функціональності та ефективності інформаційно-технологічної інфраструктури (ІТ). ІТ-системи та сервіси стали невід'ємною складовою життєдіяльності кожної компанії, незалежно від розміру, роду діяльності, галузі. У зазначеному контексті забезпечення надійності, захищеності, продуктивності, безперебійної роботи ІТ-інфраструктури стає пріоритетним завданням як структурної одиниці, так і самої компанії, що прагне досягти успіху у всепоглинаючому цифровому світі.

Складність, розмаїття ІТ-систем та сервісів створюють виклики у відстеженні, контролі їх роботи. Саме тут виникає необхідність впровадження комплексного ІТ-моніторингу, процесу систематичного спостереження, збирання, аналізу, інтерпретації та оцінювання різних аспектів ІТ-інфраструктури, сервісів з метою забезпечення їх оптимальної продуктивності, надійності, доступності, якості.

Аналіз останніх досліджень і публікацій. Вагомий вклад у дослідження питань, що стосуються технології управління ІТ-інфраструктурою внесли такі науковці: Ю. В. Бойко [9], О. І. Ролік [12], С. Ф. Теленик [11].

Мета статті. Дослідити технологію проведення комплексного ІТ-моніторингу компанії з метою визначення стану ІТ-середовища, включаючи продуктивність, пропускну здатність, безпеку.

Постановка завдання. Для досягнення поставленої мети визначено такі наукові завдання: дослідити та проаналізувати процес здійснення комплексного ІТ-моніторингу компанії, включаючи моніторинг роботи ІТ-інфраструктури та ІТ-сервісів; розкрити основні поняття, принципи, технології, пов'язані з ІТ-моніторингом, окреслити основні вимоги щодо ефективності впровадження зазначеної системи задля виявлення й вирішення проблем з оперативністю, надійністю, доступністю, продуктивністю, безпекою, задоволенням користувачів, що є ключовими факторами успіху в епоху цифрової трансформації.

Для вирішення зазначених завдань використано такі методи дослідження: аналітичний, графічний, табличний, метод класифікації, узагальнення результатів, моделювання процесів.

Виклад основного матеріалу. ІТ-моніторинг є процесом систематичного спостереження, збирання, аналізу та оцінювання різних аспектів ІТ-інфраструктури, ІТ-сервісів з метою забезпечення їх оптимальної продуктивності, доступності, якості, що включає постійний нагляд за різними складовими, зокрема: серверами, мережевими

пристроями, базами даних, програмним забезпеченням, а також здійснює контроль за роботою різноманітних серверів компанії. Метою ІТ-моніторингу є своєчасне виявлення проблем, аномалій, різного виду збоїв у ІТ-інфраструктурі, її компонентах задля запобігання можливим витратам часу, грошей, репутаційним ризикам. Для цього використовують спеціалізовані системи моніторингу ІТ-інфраструктури, які здійснюють збирання даних, їх об'єднання в єдину базу даних, де пізніше відбувається структуризація та аналіз останніх.

Про ефективність ІТ-моніторингу можна казати, якщо він буде здійснюватися на всіх рівнях ІТ-інфраструктури та охоплювати всі її складові (рис. 1).



Рисунок 1. Складові ефективного ІТ-моніторингу

Дамо коротку характеристику складових ІТ-інфраструктури (рис. 2).

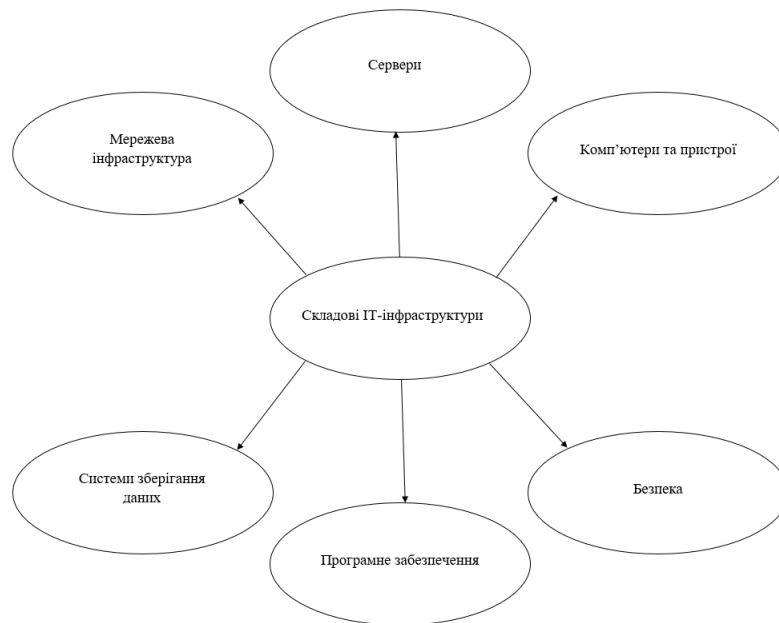


Рисунок 2. Основні складові ІТ-інфраструктури

Мережеве й серверне обладнання мають постійно контролюватися на предмет їх працездатності, оскільки будь-яка кінцева точка/додаток, під'єднаний до вашої компанії, може вважатися потенційним об'єктом для атак сторонніх осіб (зловмисників), які прагнуть отримати конфіденційну інформацію [1].

Моніторинг апаратного забезпечення дає можливість переконатися в бездоганній роботі обладнання, оскільки системи моніторингу відстежують інформацію про завантаженість процесора, обсяг вільної пам'яті, встановлюють трафік мережі й стан мережевих портів, навантаження, продуктивність, визначають заряд батареї, напругу струму.

Що стосується моніторингу мережі, системи контролюють дані відносно справності останньої, її продуктивності, досліджують конфігураційні зміни. Моніторинг цієї складової дає можливість відстежувати не лише швидкість передавання даних та пропускну спроможність мережі, а й отримувати сповіщення щодо доданих мережевих пристроїв [1].

Системи моніторингу додатків відображають дані про програмне забезпечення, розташованих на комп'ютері/сервері й дають можливість вносити зміни в роботі додатків і контролювати їх продуктивність.

ІТ-сервіси відіграють важливу роль у забезпеченні бізнес-процесів. Це набір послуг, що надаються через ІТ-інфраструктуру з метою підтримання роботи користувачів, оптимізації бізнес-процесів та досягненні кінцевої стратегічної цілі компанії. На рис. 3 відображені складові ІТ-сервіса.



Рисунок 3. Складові ІТ-сервіса

Їх основні функції – підтримання функціонування систем, забезпечення доступу до важливих даних та задоволення потреб користувачів.

Системи моніторингу можуть бути різні, водночас така різноманітність все ж має вузьку спрямованість, яка у статті представлена трьома групами, зокрема (рис. 4).

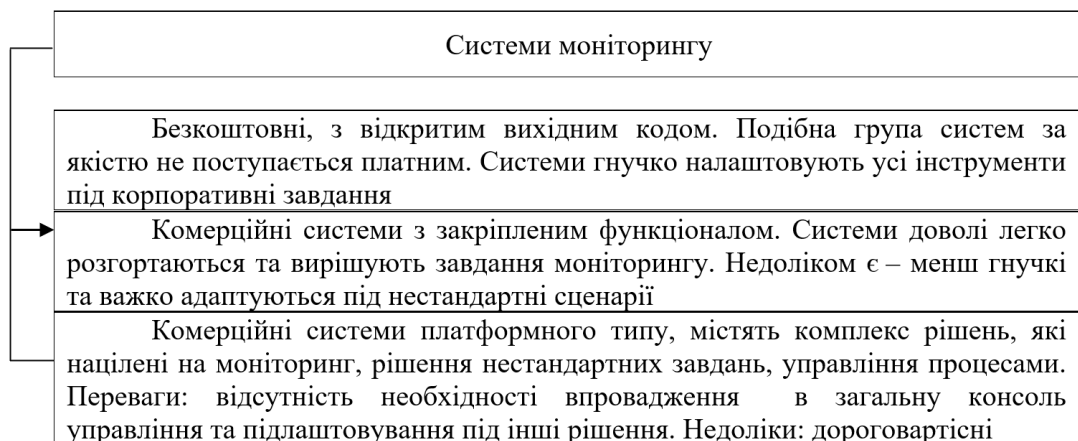


Рисунок 4. Види моніторингу та їх характеристики [2]

Процес моніторингу ІТ-інфраструктури компаніям необхідний, однак він може бути доволі клопітким, викликати певні труднощі, якщо налаштований неякісно.

Розглянемо детальніше інструменти й технології, що використовують для моніторингу ІТ-інфраструктури та сервісів (рис. 5).

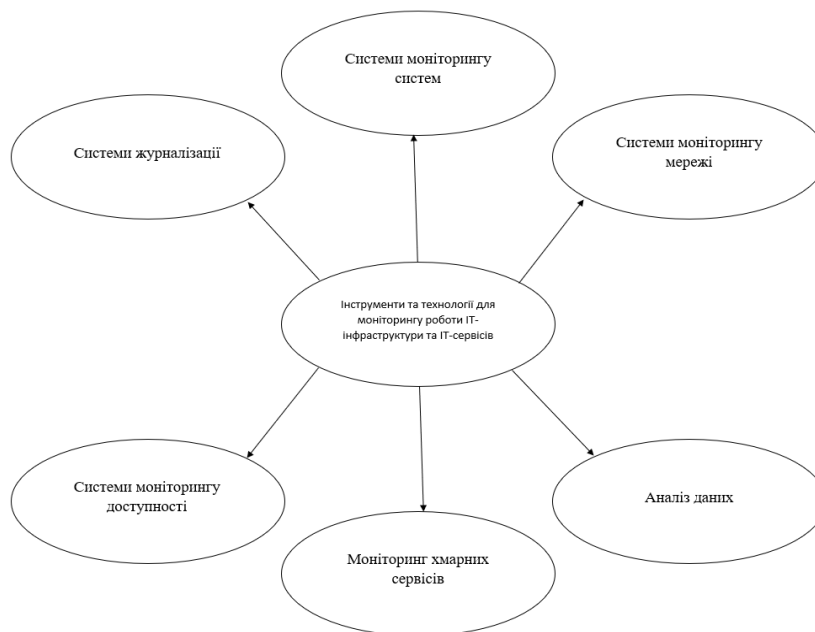


Рисунок 5. Інструменти й технології моніторингу ІТ-інфраструктури та ІТ-сервісів

В табл. 1 наведено ТОП 20 систем моніторингу ІТ-інфраструктури, включаючи системи моніторингу систем, мереж, систем журналізації, моніторинг доступності, моніторинг хмарних сервісів, аналізу даних.

Таблиця 1. ТОП 20 систем моніторингу ІТ-інфраструктури [3]

№ з/п	Назва системи	Характеристика
1	2	3
1	AppDynamics	- це комплексне рішення, охоплює компоненти сервера, сховища, мережі в хмарних та гібридних середовищах (можете розглянути локально/використовувати як службу SaaS). Особливість системи-співвідношення проблеми продуктивності з вузькими місцями інфраструктури низького рівня
2	Checkmk	- за основу взята система Nagios зі суттєвими доповненнями. Система проста, зручна, функціональна, має гарний вебінтерфейс, поріг входу – низький. Моніторинг здійснюється за допомогою агентів snmp. Якщо додає зміни, необхідно підтвердити
3	Icinga	- самостійний, якісний, безкоштовний продукт. Дані збирає за допомогою агентів та й без них. Бекенд написано на C++, вебінтерфейс на php, як базу даних підтримує MySQL, Oracle Database, PostgreSQL
4	LibreNMS	- форк Observium, але має ширший функціонал, можна запускати в Docker, має інтеграцію з Grafana, можна зберігати інформацію в InfluxDB. Система заточена на моніторинг мереж з SNMP. Унікальна тим, що має підтримку майже всіх популярних мережевих пристроїв, вміє моніторити Windows, Linux, FreeBSD (тому використовує агенти). Працює на базі PHP+MySQL
5	Monika	- це утиліта, виконує різні сценарії вебперевірок, сповіщає також різними способами (підтримують у всі напрямки-SMTP, Slack, Telegram, WhatsApp, Discord тощо), гарне рішення для автоматизації: збирає, тестує, надсилає результат. Налаштування зберігаються в одному JSON файлі
6	Monit	- легкий у користуванні, акцент на моніторинг певного сервера, може виконувати зашифровані дії, дані зберігає в SQLife.
7	PRTG Network Monitor	- комерційний інструмент моніторингу, дозволяє відстежувати стан мережевого обладнання, а також серверів, додатків, інших компонентів інфраструктури
8	Tableau та Power BI	- комерційні платформи бізнес-аналітики, надають розширені можливості візуалізації та аналізу даних
9	Munin	- простий, швидкий моніторинг окремого сервера/невеликої групи, написаний на Perl, в RRDtool зберігаються дані

Закінчення таблиці 1

1	2	3
10	Nagios	- один з найпопулярніших відкритих інструментів моніторингу, дозволяє відстежувати статус різних системних параметрів (CPU), пам'ять, дисковий простір, навантаження на мережу тощо
11	Datadog	- комерційний інструмент моніторингу, підтримує відстеження різних показників інфраструктури, включаючи хмарні сервіси.
12	Wireshark	- відкрите програмне забезпечення для аналізу мережевого трафіку, дозволяє перехоплювати, аналізувати та відстежувати пакети даних, що проходять через мережу
13	Cisco Prime Infrastructure	- інтегрована система управління, надає можливості моніторингу, конфігурації та управління мережевими обладнаннями Cisco.
14	ELK Stack	- система включає: Elasticsearch (використовується для зберігання та пошуку журнальних даних), Logstash (для збору, обробки і передачі даних), Kibana (для візуалізації та аналізу цих даних)
15	Pingdom	- веб-сервіс, який періодично перевіряє доступність веб-сайтів та сервісів з різних географічно розташованих точок, надсилає сповіщення про будь-які відмови в роботі.
16	Splunk	- платформа аналізу даних, дозволяє знаходити корисну інформацію з великих обсягів журнальних даних, візуалізувати дані та створювати звіти
17	SolarWinds Server & Application Monitor (SAM)	- система забезпечує глибокий моніторинг і локально, і в хмарі, може підтримувати понад 1200 програм/систем та кілька інших шаблонів. Відстеження відбувається за допомогою WMI, SNMP, Powershell, REST API тощо
18	The Dude	- система проста у налаштуванні, невибаглива у плані ресурсів, доступна, не вимагає особливих знань, моніторинг на базі ОС RouterOS, яка використовується у Mikrotik; уміє автоматично сканувати мережу, додавати до моніторингу всі знайдені пристрої
19	WhatsUp Gold	- рішення для моніторингу мережі (можна розширити при застосуванні модулів для моніторингу компонентів інфраструктури), відстежує споживання пропускної спроможності компонентів програми, продуктивність мережі (використання ЦП, пам'яті, диска...)
20	Zabbix	- вільний інструмент моніторингу, надає розширені можливості для відстеження різних метрик системи, крім того, можливість налаштування сповіщення про відхилення від заданих порогових значень (підтримує кілька видів моніторингу)

Оцінювання стану IT-інфраструктури містить ряд основних метрик та показників, що дозволяють проаналізувати продуктивність, ефективність, надійність, безпеку останньої (рис. 6).

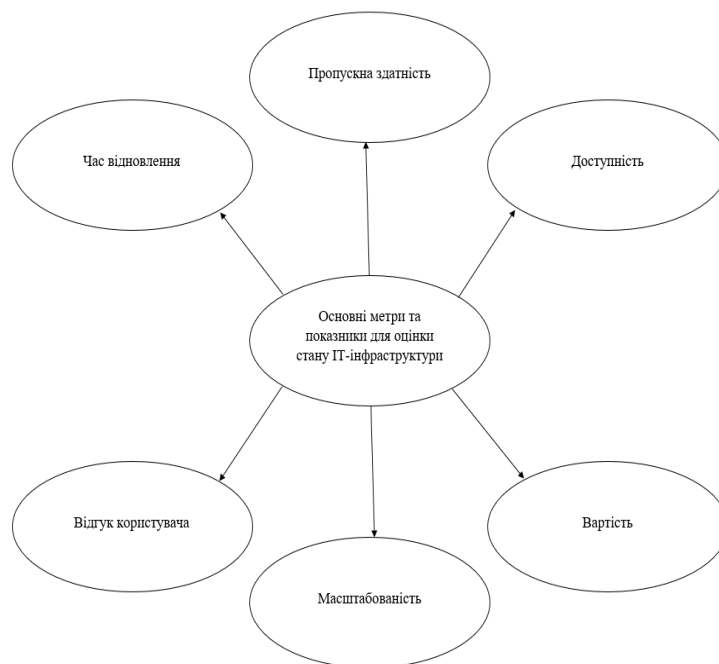


Рисунок 6. Основні метри та показники для оцінювання стану IT-інфраструктури

Врахування зазначених складових дасть можливість зрозуміти стан ІТ-інфраструктури, виявити слабкі місця, попрацювати над удосконаленням системи. Однак конкретні метрики (їх значення) можуть певною мірою відрізнятися від вимог вашого бізнесу, характеру діяльності та контексту використання [4].

Задля досягнення мети моніторингу, підтримання оптимальної продуктивності, а також безперебійної роботи системи існує ряд методів та підходів, які розглянемо, зокрема: агент-базований моніторинг (англ. agent-based monitoring). Зазначений підхід застосовують для моніторингу комп'ютерних систем й мереж та включає в себе встановлення додаткових агентів/програмного забезпечення на цільові пристрої. Перевагою є те, що такий вид моніторингу дає більше можливостей у плані гнучкості й деталізації у збиранні інформації, може виконувати локальний аналіз та опрацювання даних. Однак встановлення й керування агентами на кожному цільовому пристрої може бути ресурсооб'ємним та вимагати регулярного оновлення.

Підхід агент-лесс моніторинг (англ. agentless monitoring) – це процес моніторингу комп'ютерних систем і мереж, який не вимагає встановлення додаткових агентів/програмного забезпечення на цільові пристрої, і в цьому є його перевага (простота та гнучкість, відсутність додаткових витрат). Моніторинг здійснюється за допомогою запитів та отримання відповідей через існуючі мережеві протоколи. Агент-лесс моніторинг дозволяє виявляти проблеми зі збоєм системи, відстежувати метрики продуктивності, виявляти збої безпеки та забезпечувати відповідну реакцію на них.

Крім того існує ще активний і пасивний моніторинг – два підходи до збирання та аналізу інформації. Активний моніторинг – це свідомі дії та участь користувача/системи. Його зміст залежить від вашої мети щодо отримання інформації, зокрема налаштування програмного забезпечення для моніторингу мережі, що відправлятиме запити до певних пристроїв на мережі для перевірки доступності й відстеження шляху сигналу. Що стосується пасивного моніторингу, він здійснюється без активної участі користувача/системи. Отже, збирання інформації відбувається автоматично без потреби у втручанні, зокрема формування даних провайдерами Інтернету без вашої безпосередньої участі про ваш же трафік з метою аналізу та виявлення аномальних партнерів, можливо, загроз безпеці. Даний вид моніторингу здійснюється у фоновому режимі й може бути менш помітним для користувача.

Залежно від мети та обсягу інформації, який необхідно отримати, застосовується активний (специфічний, коли ви контролюєте процес та встановлюєте параметри моніторингу) або пасивний моніторинг (універсальний, але обмежений у можливостях, оскільки користувач не бере активної участі). Архітектура системи моніторингу може бути різноманітною, залежить від потреб та вимог до систем і мереж, які підлягають моніторингу. Але основні складові все ж існують (рис. 7).

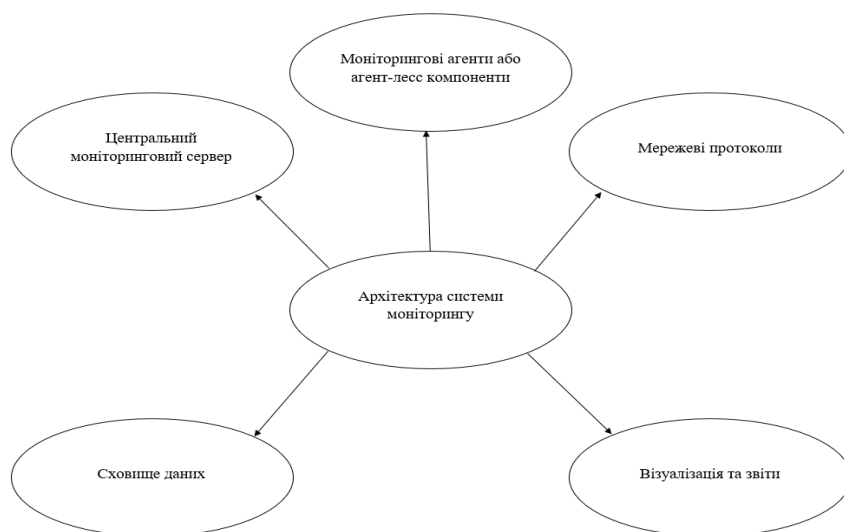


Рисунок 7. Основні елементи архітектури системи моніторингу ІТ-інфраструктури

Залежно від розміру та складності інфраструктури система моніторингу може бути розподіленою та масштабованою, включати розташування компонентів на різних фізичних серверах, використання хмарних сервісів, контейнеризацію для забезпечення гнучкості, доступності, масштабованості системи моніторингу [5].

При виборі інструментів і технологій для проведення комплексного ІТ-моніторингу необхідно врахувати кілька ключових аспектів, зокрема: функціональні можливості, надійність, масштабованість, вартість.

Перше – визначаємося із системою моніторингу мережі. Такі системи моніторингу як Nagios або Zabbix, є традиційними, надають базові функціональні можливості (моніторинг доступності й стану мережевих пристроїв), не можуть працювати за великого обсягу мережевого обладнання, а тому потребують розширення функціональних можливостей за допомогою використання більш масштабованих систем, що працюють з великим обсягом даних. До систем, які надають додаткові інструменти пропускну здатності, завантаження каналів, аналізу мережевого трафіку можна віднести PRTG Network Monitor або SolarWinds Network Performance Monitor [6].

Ключовим аспектом також вважаємо моніторинг серверів комплексного ІТ-моніторингу. Застосування таких інструментів, як Prometheus, Datadog або New Relic, дає можливість відстежувати метрики серверів (завантаженість процесора, використання пам'яті, мережевий трафік тощо), надають можливість встановлення трендів, аналізу подій, сповіщають про виявлені аномалії. Вибір інструментів залежить від вимог, мети, потреб користувача, підтримання певних операційних систем і технологічних стеків.

Використання агентів моніторингу може допомогти відстежувати метрики на рівні ОС/додатків. На серверах можна встановити свій власний агент для збирання даних Prometheus, а для моніторингу різних мов програмування, фреймворків можна скористатися інструментом New Relic, що дозволяє деталізувати інформацію стосовно продуктивності та працездатності додатків.

Хмарні сервіси (Amazon Web Services або Microsoft Azure Monitor) надають свої власні інструменти моніторингу. AWS CloudWatch та Azure Monitor дозволяють відстежувати різні метрики та події з хмарних ресурсів (контейнери, віртуальні машини, бази даних тощо), підтримують інтеграцію з іншими засобами моніторингу та оповіщеннями [7].

Інструменти ELK Stack (Elasticsearch, Logstash, Kibana) або Splunk використовують для аналізу лог-файлів (збирання, зберігання, аналіз логів з різних джерел). Отже, здійснюють пошук, фільтрацію, візуалізацію та аналіз лог-даних, трендів для виявлення проблем, крім того, забезпечують безпеку систем.

До інструментів управління подіями та інцидентами відносять такі, як PagerDuty, VictorOps або ServiceNow, які сповіщають команду про проблеми та координують відновлення сервісу, інтегруються з різними інструментами моніторингу/сповіщення, що є необхідним при відстеженні та вирішенні проблеми.

Процес упровадження системи моніторингу доволі складний, вимагає кропіткої підготовки. Сам процес можна відобразити схемою (рис. 8).



Рисунок 8. Процес упровадження системи моніторингу

Можна зробити висновок, що впровадження системи моніторингу – це безперервний процес, який потребує уваги до деталей, налаштування та постійного підтримання.

Висновки. Моніторинг ІТ-інфраструктури – важливий процес. Він допомагає компанії відстежувати зміни, які в ній відбулися, здійснює збирання та аналіз даних ІТ-сервісів, компонентів інформаційної інфраструктури, контролює всі її елементи, запобігає проблемам, збоям, атакам. Це – необхідний елемент управління ІТ-середовищем, дозволяє виявляти, контролювати та вирішувати проблеми, що виникають в інфраструктурі та впливають на якість і продуктивність ІТ-сервісів, відповідно, ефективний моніторинг сприяє покращенню доступності, продуктивності, якості ІТ-сервісів, а це, у свою чергу, – досягненню бізнес-цілей компанії.

Успішна імплементація моніторингу в компанії вимагає відповідного планування, вибору дієвих інструментів, встановлення належних процесів, але результатом є значна вигода та ефективна робота компанії.

Conclusions. IT infrastructure monitoring is an important process. It helps the company to track the changes that have taken place in it, collects and analyzes data from IT services, information infrastructure components, controls all its elements, prevents problems, failures, and attacks. This is a necessary element of IT environment management, it allows to identify, monitor, and solve problems that arise in the infrastructure and affect the quality and performance of IT services, respectively, effective monitoring helps to improve the availability, productivity, and quality of IT services, and this, in turn, achieves the company's business goals.

Successful implementation of monitoring in the company requires appropriate planning, selection of effective tools, establishment of proper processes, but the result is a significant benefit and efficient operation of the company.

Список використаних джерел

1. Ефективний моніторинг ІТ-інфраструктури – що і як моніторити: веб-сайт. URL: <https://onbiz.biz/monitoring-of-it-infrastructure/>. (дата звернення: 20.01.2024).
2. Моніторинг ІТ-інфраструктури: навіщо він потрібен: веб-сайт. URL <http://tsu.ua/monitoryng-it-infrastruktury> (дата звернення: 20.01.2024).
3. ТОП 20 систем моніторингу ІТ інфраструктури: веб-сайт. URL: https://blog.iteducenter.ua/ratings/monitoring_tools/ (дата звернення: 20.01.2024).
4. Turnbull J. The Art of Monitoring. 2016. 645 p. URL <https://www.oreilly.com/library/view/the-art-of/9780988820241> (Last accessed: 22.01.2024).
5. Davis J., Devers C., Sable T. Modern System Administration: Building and Maintaining Reliable Systems. 2021. 300 p. URL: <https://bigl.ua/ua/p2026141934-modern-system-administration> (Last accessed: 22.01.2024).
6. Liefting N. Zabbix 5 IT Infrastructure Monitoring Cookbook: Explore the new features of Zabbix 5 for designing, building, and maintaining your Zabbix setup. 2021. 464 p. URL: https://www.oreilly.com/library/view/zabbix-5-it/9781800202238/B16104_FM_ePub_RK.xhtml (Last accessed: 23.01.2024).
7. Jackie F. Key Trends to Watch in Gartner Emerging Technologies Hype Cycle. 2012. 255 p. URL: <https://www.gartner.com/en/documents/2100915> (Last accessed: 25.01.2024).
8. Мешков В. Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security: Дніпровська політехніка. Вип. 1. 2023. С. 85–92. DOI: <https://doi.org/10.32782/IT/2023-1-11>
9. Бойко Ю. В., Волохов В. М., Глибовець М. М. Методи та новітні підходи до проектування, управління і застосування високопродуктивних ІТ-інфраструктур : монографія. Київ : ВПЦ «Київський університет», 2016. 447 с.
10. Теленик С. Ф., Ролік О. І., Терещенко П. І., Букасов М. М. Забезпечення процесів діяльності ресурсами з визначеним рівнем надійності в інформаційно-телекомунікаційній системі спеціального призначення : зб. наук. праць. Київ : ВІПІ НТУУ «КПІ», 2006. № 3. С. 134–138.
11. Теленик С. Ф., Ролік О. І., Букасов М. М. Технологія управління ІТ-інфраструктурою на основі ресурсного підходу. Вісник ЖДТУ. 2008. № 4 (47). С. 180–189.
12. Бойко Ю. В., Глибовець М. М., Єршов С. В., Кривий С. Л., Погорілий С. Д., Ролік О. І., Теленик С. Ф., Ясочка М. В. Управління високопродуктивними ІТ-інфраструктурами. Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. 2014. № 61. С. 120–141.

References

1. Efektyvnyj monitoryng IT-infrastruktury-shho i jak monitoryty. Available at: <https://onbiz.biz/monitoring-of-it-infrastructure/> (accessed 20 January 2024).
2. Monitoring IT-infrastruktury: navishho vin potriben. Available at: <http://tsu.ua/monitoryng-it-infrastruktury> (accessed 20 January 2024).
3. TOP 20 system monitoryng IT infrastruktury. Available at: https://blog.iteducer.ua/ratings/monitoring_tools (accessed 20 January 2024).
4. Turnbull J. (2016). *The Art of Monitoring*. 645 p. Available at: <https://www.oreilly.com/library/view/the-art-of/9780988820241> (accessed 22 January 2024).
5. Davis J., Devers C., Sable T. (2021). *Modern System Administration: Building and Maintaining Reliable Systems*. 300 p. Available at: <https://bigl.ua/ua/p2026141934-modern-system-administration> (accessed 23 January 2024).
6. Liefting N. (2021). *Zabbix 5 IT Infrastructure Monitoring Cookbook: Explore the new features of Zabbix 5 for designing, building, and maintaining your Zabbix setup*. 464 p. Available at: https://www.oreilly.com/library/view/zabbix-5-it/9781800202238/B16104_FM_ePub_RK.xhtml (accessed 23 January 2024).
7. Jackie F. (2012). *Key Trends to Watch in Gartner Emerging Technologies Hype Cycle*. 255 p. Available at: <https://www.gartner.com/en/documents/2100915> (accessed 25 January 2024).
8. Meshkov V. (2023). Analiz system intelektualnogho monitorynghu trafiku komp'juternoji merezhi dlja system vyjavlennja atak. [Information Technology: Computer Science, Software Engineering and Cyber Security], vol. 1, pp. 85–92. <https://doi.org/10.32782/IT/2023-1-11>
9. Bojko Ju. V., Volokhov V. M., Ghlybovecj M. M. (2016). *Metody ta novitni pidkhody do proektuvannja, upravlinnja i zastosuvannja vysokoproduktyvnykh IT-infrastruktur [Methods and latest approaches to design, management and application of high-performance IT-infrastructures] : monohrafija*. Kyjiv: VPC “Kyjivsjkyj universytet”. 447 p.
10. Telenyk S. F., Rolik O. I., Tereshhenko P. I., Bukasov M. M. (2006). Zabezpechennja procesiv dijajnosti resursamy z vyznachenym rivnem nadijnosti v informacijno-telekomunikacijnij systemi specialnogho pryznachennja [Provision of activity processes with resources with a certain level of reliability in the special-purpose information and telecommunication system] : zb. nauk. pracj. Kyjiv: VITI NTUU “KPI”, No. 3. Pp. 134–138
11. Telenyk S. F., Rolik O. I., Bukasov M. M. (2008). Tekhnologhija upravlinnja IT-infrastrukturoju na osnovi resursnogho pidkhodu [IT-infrastructure management technology based on resource approach]. *Visnyk ZhDTU*, no. 4 (47). pp. 180–189.
12. Bojko Ju. V., Ghlybovecj M. M., Jershov S. V., Kryvyj S. L., Poghorilyj S. D., Rolik O. I., Telenyk S. F., Jasochka M. V. (2014). *Upravlinnja vysokoproduktyvnymy IT-infrastrukturamy [Managing high-performance IT-infrastructures]*. *Visnyk NTUU “KPI”. Informatyka, upravlinnja ta obchysljuvaljna tekhnika*, no. 61, pp. 120–141.