

УДК 004.588

Михайлюк О.В., здобувач

Національний університет «Київський авіаційний інститут»

МЕТОДИ ЗБОРУ ТА ОБРОБКИ ДАНИХ ПРО СТАН СЕРВІСІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

У роботі досліджено методи збору та обробки даних про стан системних сервісів у операційній системі *Windows*. Розглянуто сучасні підходи до моніторингу, включаючи використання *WMI* та *PowerShell*, а також принципи аналізу даних у системах забезпечення надійності. Обґрунтовано необхідність комплексного підходу до моніторингу.

Ключові слова: моніторинг, *Windows*, сервіси, *WMI*, *PowerShell*, обробка даних, *SRE*, *observability*

У сучасних інформаційних системах стабільність роботи програмного забезпечення значною мірою залежить від коректного функціонування системних сервісів. В операційній системі *Microsoft Windows* сервіси забезпечують виконання ключових фонових процесів, що впливають на продуктивність, безпеку та надійність системи.

Згідно з дослідженнями у сфері *Site Reliability Engineering (SRE)*, ефективний моніторинг дозволяє зменшити час простою систем і підвищити їх надійність [1]. Концепція *observability* передбачає аналіз системи на основі метрик, логів і трасувань [2].

Таким чином, проблема ефективного збору та обробки даних про стан сервісів є актуальною.

Метою роботи є аналіз та систематизація методів збору й обробки даних про стан сервісів у середовищі *Windows* з урахуванням сучасних підходів [1].

Завдання дослідження

1. Дослідити особливості функціонування сервісів у *Windows*.
2. Проаналізувати методи збору інформації про їх стан [3].
3. Розглянути підходи до обробки та аналізу даних [4].
4. Визначити ефективність сучасних підходів до моніторингу [2].
5. Сформулювати вимоги до систем моніторингу [5].

Об'єкт дослідження: процеси функціонування системних сервісів у операційній системі *Microsoft Windows*.

Предмет дослідження: методи збору та обробки даних про стан сервісів та підходи до їх аналізу [4].

Системні сервіси в *Microsoft Windows* є важливими компонентами, які забезпечують виконання фонових процесів і підтримку функціонування прикладного програмного забезпечення.

Моніторинг сервісів передбачає збір, аналіз і інтерпретацію даних про їх стан. Сучасні підходи базуються на концепції *observability*, яка включає метрики, логи та трасування [2].

Основними методами збору інформації є: використання вбудованих засобів Windows; застосування технологій *Windows Management Instrumentation* та *PowerShell*; аналіз системних журналів подій.

Згідно з документацією *Microsoft*, використання *WMI* та *PowerShell* забезпечує ефективний доступ до системної інформації та дозволяє автоматизувати процес моніторингу [3].

Після збору даних виконується їх обробка. Вона включає фільтрацію, агрегацію та аналіз тенденцій, що дозволяє виявляти аномалії [4].

Сучасні дослідження показують, що системи моніторингу повинні підтримувати прогнозування збоїв та автоматичне реагування [5].

Таким чином, ефективний моніторинг сервісів повинен базуватися на комплексному підході.

Висновки: У результаті дослідження встановлено, що ефективний моніторинг сервісів у середовищі *Windows* потребує комплексного підходу, який включає сучасні методи збору та обробки даних.

Використання *WMI* та *PowerShell* дозволяє отримувати детальну інформацію про стан системи, а впровадження підходів *observability* підвищує ефективність аналізу [2].

Список використаних джерел:

1. Beyer B., Jones C., Petoff J., Murphy N. Site Reliability Engineering: How Google Runs Production Systems. – Sebastopol: O’Reilly Media, 2016. – 552 p. – URL: <https://sre.google/sre-book/table-of-contents/>
2. Mukhi N. From Monitoring to Observability. – Zenodo, 2024. – URL: <https://zenodo.org/records/17410892>
3. Microsoft Docs. Windows Management Instrumentation (WMI) and PowerShell Documentation. – URL: <https://learn.microsoft.com>
4. Cleland-Huang J. et al. Monitoring in Software Engineering // Information and Software Technology. – 2016. – Vol. 80. – P. 1–20. – URL: <https://doi.org/10.1016/j.infsof.2016.07.002>
5. Sosnowski J., Król M. Dependability Evaluation Based on System Monitoring // InTech. – 2010. – URL: <https://www.intechopen.com>