УДК 004
Ганський Д.А.[1], Степаненко О.О.[2]
[1] студ. гр. КНТ-124м НУ «Запорізька політехніка»
[2] доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ НА ПРОГРАМНА РЕАЛІЗАЦІЯ МОНІТОРИНГУ В LINUX НА ОСНОВІ EBPF У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Об'єкт дослідження – процес моніторингу роботи, розроблення та тестування програмного забезпечення операційних системах, побудованих на ядрі Linux.

Предмет дослідження – методи і засоби збору моніторингових даних про роботу систем на ядрі Linux та додатків у режимі реального часу.

Мета роботи – створити програмне рішення, яке забезпечує збір моніторингових даних в ОС Linux з використанням технології eBPF, для

збільшення їх обсягу та спрощення процесу моніторингу в контейнеризованих середовищах порівняно зі стандартними підходами.

Матеріали, методи та технічні засоби: документація eBPF, приклади застосування з відкритих джерел, тестові сценарії навантаження, операційна система Linux (Ubuntu/Debian/інші), компілятор clang/LLVM, бібліотеки libbpf, мови програмування C та Go, інструменти bcc/bpftrace, апаратні ресурси ПК/серверу.

В ході роботи було проаналізовано та досліджено предметну область, програмні засоби, інструменти та технології для моніторингу систем на основі Linux.

Досліджено та проаналізовано найпоширеніші програмні рішення, технології та підходи для моніторингу систем на основі Linux. На основі проведеного аналізу визначено ключові функціональні вимоги до розроблюваного програмного забезпечення для моніторингу Linux-систем.

Проведено дослідження існуючих мов програмування, технологій для розробки моніторингового програмного забезпечення та підходів для збору моніторингових даних. Обрано наступні технології: eBPF – як інструмент для безпечного та ефективного перехоплення даних на рівні ядра; Go – для реалізації користувацької частини; C – для написання коду, що виконується в ядрі Linux; OpenTelemetry (OTel) – для експорту метрик, логів та даних трасування в єдиному форматі незалежно від програмного продукту для відображення та візуалізації моніторингових даних.

Було розроблено програмний додаток, який надає користувачам зручні та ефективні інструменти для збору моніторингових даних, зокрема метрик, журналів подій та даних трасування. Система забезпечує можливість отримання цих даних із будь-яких середовищ, що функціонують на основі ядра Linux, що робить її універсальним рішенням для різних типів інфраструктур. Завдяки оптимізованій архітектурі та раціональному використанню системних ресурсів, додаток не створює суттєвих накладних витрат на продуктивність, не впливає на стабільність роботи операційної системи чи інших програмних компонентів, встановлених у середовищі виконання.

Наукова новизна роботи полягає у розробці програмного рішення для моніторингу систем на основі Linux з використанням технології eBPF, що дозволяє збирати детальні метрики, журнали та трасування як з ядра Linux, так і з користувацьких додатків, забезпечуючи глибший та точніший аналіз стану системи порівняно з традиційними методами моніторингу. Використання eBPF розширює можливості збору даних, дозволяючи отримувати інформацію, яка раніше була недоступною, що відкриває нові можливості оптимізації роботи систем на основі Linux, а використання OpenTelemetry дозволяє експортувати

зібрані дані в уніфікованому форматі, що робить додаток незалежним від системи, де обробляються моніторингові дані.

У процесі перевірки роботи програмного продукту не було виявлено жодних системних помилок, збоїв чи порушень у функціонуванні окремих компонентів. Також не зафіксовано потенційних загроз безпеці, зокрема щодо несанкціонованого доступу до користувацьких даних, а також проблем з швидкістю обробки даних та загальною продуктивністю додатку. Завдяки використанню технології eBPF та верифікатору, який є невід'ємною частиною процесу завантаження eBPF програм і має суворі правила щодо завантажуваного коду, забезпечується високий рівень контролю за виконанням програм у ядрі операційної системи, досягається підвищена надійність роботи, унеможливлюється аварійне завершення системи або програм, що виконуються в програмному середовищі. Таким чином, можна зробити висновок, що розроблений програмний продукт функціонує стабільно, повністю відповідає визначеним технічним та функціональним вимогам і є готовим до подальшого практичного використання.

Інтеграція розробленого програмного продукту в середовище користувачів дозволить DevOps інженерам та SRE спеціалістам своєчасно виявляти потенційні проблемні місця, такі як затримки в обробці запитів, надмірне навантаження на CPU чи інші компоненти системи в застосунках, що працюють у цьому середовищі. У разі виникнення несправності інженер зможе швидко визначити її джерело, яке спричинило простій системи або некоректну роботу. Крім того, якщо користувач виявить повторювану проблему (наприклад, підвищене навантаження на диск), він може переглянути поточну архітектуру своєї системи, щоб оптимізувати її роботу або зменшити витрати на інфраструктуру.

Галузь використання – інформаційна безпека, адміністрування та експлуатація серверів і хмарних середовищ.