УДК 004.056.5

**Д. Р. Годованнік**

# МОНІТОРИНГ ВРАЗЛИВОСТЕЙ БЕЗСЕРВЕРНИХ ФУНКЦІЙ ІЗ ВИКОРИСТАННЯМ АДАПТИВНОГО СИГНАТУРНОГО АНАЛІЗУ ТА СТАНДАРТІВ OWASP

Вінницький національний технічний університет

***Анотація***

*У роботі розглянуто проблему забезпечення кібербезпеки безсерверних функцій у хмарних середовищах. Встановлено, що традиційні методи виявлення вразливостей, зокрема SAST, DAST, IAST, SCA та CSPM, мають суттєві обмеження в умовах Function as a Service через ефемерність середовища виконання, подієво-орієнтовану архітектуру та відсутність доступу до операційної системи. Запропоновано підхід до побудови автоматизованої системи моніторингу вразливостей, яка поєднує легковагове проміжне програмне забезпечення, модуль збору подій, аналітичне ядро та базу адаптивних сигнатур. Система орієнтована на виявлення атак відповідно до актуальних категорій OWASP, зокрема порушення контролю доступу, ін'єкцій подій, небезпечної конфігурації та атак типу Denial of Wallet.*

***Ключові слова:*** *безсерверні обчислення, FaaS, кібербезпека, OWASP, адаптивний сигнатурний аналіз, моніторинг вразливостей, IAM, Denial of Wallet.*

***Abstract***

*The paper considers the problem of ensuring cybersecurity of serverless functions in cloud environments. It is established that traditional vulnerability detection methods, including SAST, DAST, IAST, SCA, and CSPM, have significant limitations in Function as a Service environments due to the ephemeral nature of execution environments, event-driven architecture, and lack of access to the operating system. An approach to the development of an automated vulnerability monitoring system is proposed, combining lightweight middleware, an event collection module, an analytical core, and an adaptive signature database. The system is focused on detecting attacks according to relevant OWASP categories, including broken access control, event injection, security misconfiguration, and Denial of Wallet attacks.*

***Keywords:*** *serverless computing, FaaS, cybersecurity, OWASP, adaptive signature analysis, vulnerability monitoring, IAM, Denial of Wallet.*

## Вступ

Безсерверні обчислення є одним із найбільш динамічних напрямів розвитку хмарних технологій. Модель Function as a Service дозволяє розробникам створювати масштабовані застосунки без необхідності адміністрування серверної інфраструктури. У таких середовищах керування ресурсами, балансування навантаження та масштабування виконуються хмарним провайдером, тоді як розробник зосереджується переважно на реалізації прикладної логіки [1].

Однак перехід до безсерверної архітектури суттєво змінює підхід до забезпечення кібербезпеки. Традиційний мережевий периметр фактично зникає, а кожна функція, що викликається через HTTP-запит, повідомлення з черги, зміну стану бази даних або завантаження файлу в хмарне сховище, стає потенційною точкою входу для зловмисника [2].

Крім того, короткий життєвий цикл безсерверних функцій ускладнює журналювання, моніторинг та подальший аналіз інцидентів. Саме тому класичні засоби захисту, орієнтовані на постійно доступні сервери, операційні системи та мережевий периметр, не забезпечують достатнього рівня ефективності у FaaS-середовищах [3].

Особливої актуальності набуває проблема несанкціонованого доступу в умовах хмарних середовищ. Якщо у традиційних системах НСД часто пов'язувався зі зламом операційної системи або мережевого сервісу, то у FaaS-середовищах він здебільшого реалізується через помилки прикладного коду, відкриті API, ін'єкції подій або надмірні права IAM-ролей [4].

Метою даної роботи є розробка підходу до побудови автоматизованої системи моніторингу вразливостей безсерверних функцій із використанням адаптивного сигнатурного аналізу та стандартів OWASP.

## Результати дослідження

У ході дослідження було проаналізовано особливості безсерверних обчислень та встановлено, що класичні засоби захисту не забезпечують достатнього рівня безпеки для FaaS-середовищ. Зокрема, статичний аналіз коду не враховує реальний хмарний контекст виконання та IAM-права функцій. Динамічний аналіз орієнтований переважно на HTTP-інтерфейси та не здатний повноцінно імітувати асинхронні події. Інтерактивні засоби захисту потребують встановлення агентів у середовище виконання, що є проблематичним у керованих безсерверних платформах.

Для подолання цих обмежень запропоновано архітектуру автоматизованої системи моніторингу вразливостей, яка складається з чотирьох основних компонентів:

1. **Middleware-рівень** – легковагове проміжне програмне забезпечення, яке розміщується у просторі пам'яті безсерверної функції та перехоплює вхідні JSON-події до їх передавання в основну бізнес-логіку.
2. **Модуль збору подій** – компонент, що відповідає за асинхронну агрегацію логів, метрик, трасувань та подій хмарної інфраструктури.
3. **Аналітичне ядро** – модуль, який виконує профілювання нормальної поведінки функцій, аналіз аномалій та формування нових адаптивних сигнатур.
4. **База адаптивних сигнатур** – сховище захисних правил, що забезпечує швидке використання згенерованих сигнатур під час перевірки нових подій.

Основою запропонованої системи є адаптивний сигнатурний аналіз. На відміну від класичних сигнатурних систем, які працюють лише з наперед заданими шаблонами, адаптивний підхід передбачає динамічне формування нових правил на основі виявлених відхилень від нормальної поведінки функції. Для цього аналізуються час виконання, обсяг спожитої пам'яті, граф API-викликів, структура JSON-подій та характер взаємодії функції з іншими хмарними сервісами.

У межах дослідження запропоновано використовувати статистичне профілювання поведінки функцій. Час виконання може моделюватися з урахуванням особливостей хмарного середовища, зокрема мережевих затримок, планування ресурсів та ефекту холодного старту [5]. Для аналізу аномалій доцільно застосовувати методи поведінкового виявлення, які дозволяють фіксувати відхилення від типової роботи системи [6].

Для підвищення точності виявлення нетипових подій у системі можуть використовуватися методи машинного навчання та поведінкового аналізу. Такий підхід є доцільним для аналізу багатовимірних ознак, оскільки дозволяє виявляти об'єкти, які суттєво відрізняються від типової поведінки системи, без необхідності попереднього опису всіх можливих атак [6].

Запропонована система орієнтована на виявлення загроз, що відповідають категоріям OWASP Serverless Top 10 [4]. Найбільш важливими для безсерверних функцій у межах даного дослідження є такі напрями:

1. Порушення контролю доступу. Для протидії цій загрозі запропоновано аналізувати IAM-активність функцій та порівнювати її з еталонним графом дозволених дій. Якщо функція виконує нетиповий API-виклик або намагається отримати доступ до ресурсу, який не відповідає її нормальній поведінці, система може сформувати блокувальне правило або ініціювати тимчасове обмеження прав скомпрометованої функції.
2. Ін'єкції подій. Для виявлення цього типу атак Middleware виконує перевірку структури вхідних JSON-повідомлень. Аналізується абстрактне синтаксичне дерево документа та відповідність типів даних очікуваній структурі. Якщо замість скалярного значення передається вкладений об'єкт із потенційно шкідливим вмістом, система класифікує таку подію як аномальну.
3. Атаки типу Denial of Wallet. Для протидії таким атакам система аналізує повторювані виклики функцій, ідентифікатори трасування та поступове зростання навантаження. У разі виявлення рекурсивної петлі або аномального збільшення кількості викликів система ініціює блокування запиту або обмеження інтенсивності викликів на рівні API Gateway.
4. Небезпечна конфігурація та надмірні привілеї. Окрему увагу приділено виявленню ситуацій, коли безсерверна функція має ширші права доступу, ніж потрібно для виконання її бізнес-логіки. Такі помилки конфігурації можуть бути використані зловмисником для розвитку атаки після компрометації однієї функції.

Важливою особливістю запропонованого підходу є ретроспективна перевірка нових сигнатур на історичних логах. Це дозволяє зменшити кількість хибних спрацювань і не допустити блокування легітимних користувацьких запитів. Лише після успішної перевірки сигнатура переводиться в активний стан і використовується для подальшого моніторингу.

Таким чином, запропонована система поєднує переваги сигнатурного аналізу, поведінкового профілювання та хмарної телеметрії. Вона не потребує доступу до операційної системи, не порушує модель відповідальності хмарного провайдера та може бути інтегрована у безсерверні застосунки з мінімальним впливом на продуктивність.

## Висновок

У результаті дослідження встановлено, що безсерверні обчислення формують нову модель кіберризиків, у якій традиційні засоби захисту не забезпечують достатньої ефективності. Основними проблемами є ефемерність середовища виконання, подієво-орієнтована модель запуску функцій, складність контролю IAM-прав та неможливість використання класичних агентів рівня операційної системи.

Запропонована автоматизована система моніторингу вразливостей дозволяє підвищити рівень захищеності FaaS-середовищ за рахунок використання адаптивного сигнатурного аналізу. Її архітектура передбачає поєднання Middleware-рівня, модуля збору подій, аналітичного ядра та бази адаптивних сигнатур. Такий підхід забезпечує виявлення аномалій у реальному часі, формування нових сигнатур для невідомих атак та зменшення кількості хибних спрацювань завдяки ретроспективній перевірці правил.

Практичне значення роботи полягає у можливості застосування запропонованого підходу для захисту хмарних застосунків, що використовують FaaS-платформи. Подальші дослідження можуть бути спрямовані на програмну реалізацію прототипу системи, експериментальне вимірювання затримок, оцінювання точності виявлення атак та оптимізацію механізмів генерації адаптивних сигнатур.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Serverless Computing: Current Trends and Open Problems. arXiv.org. URL: https://arxiv.org/abs/1706.03178 (date of access: 13.05.2026).
2. Cloud Programming Simplified: A Berkeley View on Serverless Computing. arXiv.org. URL: https://arxiv.org/abs/1902.03383 (date of access: 13.05.2026).
3. Serverless Computing: A Survey of Opportunities, Challenges, and Applications. ACM Digital Library. URL: https://doi.org/10.1145/3510611 (date of access: 13.05.2026).
4. OWASP Serverless Top 10. OWASP Foundation. URL: https://owasp.org/www-project-serverless-top-10/ (date of access: 13.05.2026).
5. Peeking Behind the Curtains of Serverless Platforms. USENIX. URL: https://www.usenix.org/conference/atc18/presentation/wang-liang (date of access: 13.05.2026).
6. Anomaly Detection: A Survey. ACM Digital Library. URL: https://doi.org/10.1145/1541880.1541882 (date of access: 13.05.2026).



***Годованнік Денис Русланович*** – студент групи 2КІТС-22Б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: dengodovannnnnnnik@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** - кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: karpinets@vntu.edu.ua

**Hodovannik Denys R.** – student of group 2KITS-22B, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dengodovannnnnnnik@gmail.com

**Supervisor: Karpinets Vasyl V.** – Candidate of Technical Sciences, Associate Professor, Head of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: karpinets@vntu.edu.ua