UDC 004.056:005.1 DOI: https://doi.org/10.64076/iedc250821.07

Information security management of the company's cloud environment using the Cisco Cloudlock cloud service

Pavlo Chipko
National University "Lviv Polytechnic", Lviv
Oksana Svatyuk
National University "Lviv Polytechnic", Lviv

Abstract. *The theses consider the features of information security management of cloud environments using the Cisco Cloudlock cloud service. The relevance of the issue of information security management of cloud environments is considered. The importance of an integrated approach in the management of cloud environment security is substantiated. The problems of cloud environment security and measures for information security management of cloud environments are considered.*
Keywords: *information security, management, cloud environment, Cisco Cloudlock, data protection.*

Менеджмент інформаційної безпеки хмарного середовища компанії з використанням хмарного сервісу Cisco Cloudlock

Павло Чіпко
Національний університет
"Львівська Політехніка", м. Львів
Оксана Сватюк
Національний університет
"Львівська Політехніка", м. Львів

Анотація. *У тезах розглядається особливості менеджменту інформаційної безпеки хмарних середовища з використанням хмарного сервісу Cisco Cloudlock. Розглянута актуальність питання менеджменту інформаційної безпеки хмарних середовищ. Обгрунтовано значення комплексного підходу в менеджменті безпки хмарних середовищ. Розглянуто проблеми безпеки хмарних середовищ та заходи менеджменту інформаційної безпеки хмарних середовищ.*
Ключові слова: *інформаційна безпека, менеджмент, хмарне середовище, Cisco Cloudlock, захист даних.*

В сучасному світі коли хмарні технології широко використовуються компаніями в їхній діяльності. З впровадженням в компаніях хмарних середовищ зростає і потреба захисту даних які в них обробляються. Забезпечення безпеки хмарних середовищ вимагає поєднання ефективного менеджменту та технічних, організаційних та аналітичних заходів.

Одними з основних проблем, які повстають при забезпеченні безпеки хмарного середовища є:

- Неналежний контроль доступу.
- Загрози витоку даних через вразливості в конфігурації хмарних сервісів.

- Зловживання працівниками хмарними ресурсами (тіньові IT).
- Недотримання стандартів і нормативних вимог.
- Забезпечення конфіденційності та захищеності даних.
- Безпека API.
- Сумісність та інтегрованість з наявною інфраструктурою [1].

Менеджмент безпеки хмарних середовищ вимагає системного підходу до інформаційної безпеки в хмарних середовищах. Системний підхід включає технічні засоби контролю та моніторингу, формування політик та навчання працівників в сфері інформаційної безпеки.

Одним з засобів, які забезпечує системний підхід до менеджменту інформаційної безпеки хмарних середовищ є Cisco Cloudlock. Cisco Cloudlock це хмарний сервіс, який базується на технології Cloud Access Security Broker (CASB), яка дозволяє забезпечувати ефективний захист для хмарних середовищ.

Cisco Cloudlock – це сервіс, який забезпечує управління доступу, моніторинг та контроль за діями користувачів в хмарних середовищах. Для забезпечення безпеки хмарний сервіс використовує безагентну архітектуру, яка взаємодіє з іншими хмарними сервісами задопомогою API. Cisco Cloudlock швидко впроваджується в існуючу інфраструктуру та має можливість інтеграції з іншими сервісами, що забезпечує широкий спектр функціональних можливостей.

Основними функціональними можливостями Cisco Cloudlock для менеджменту безпеки в хмарних середовищ є:

- Data Loss Prevention (DPL).
- Захист від загроз в режимі реального часу.
- Менеджмент інцидентів.
- Виявлення та контроль додатків.
- Забезпечення відповідності вимогам.
- Users Events and Behavior Analysis (UEBA).
- Інтеграція та розширюваність.
- Управління політиками [2].

Cisco Cloudlock дозволяє створити ефективну систему менеджменту інформаційної безпеки, яка буде орієнтована на превентивний захист та мінімізацію ризиків. Ефективність використання Cisco Cloudlock залежить від впроваджених політик та організації менеджменту політиками. Основні заходи менеджменту включають:

- Формування політик безпеки.
- Навчання персоналу.
- Створення програм менеджменту інцидентами.
- Проведення регулярного аудиту та тестування систем безпеки.
- Інтеграція Cisco Cloudlock з іншими інструментами кіберзахисту (SIEM-системи, багатофакторна автентифікація, VPN) [3].

Використання функціоналу Cisco Cloudlock з організаційними заходами дозволяє створити ефективну систему безпеки менеджменту безпеки хмарного середовища.

Отже менеджмент інформаційної безпеки в хмарних середовищах є одним із найважливіших напрямів корпоративного управління безпекою. Використання хмарного сервісу Cisco Cloudlock для менеджменту інформаційної безпеки забезпечує компаніям ефективний захист від загроз, контроль та управління інцидентами, контроль доступу до ресурсів та даних і відповідність стандартам і вимогам. Таким чином використання даного сервісу в системах менеджменту інформаційно безпеки дозволяє компаніям знизити ризики, підвищити довіру клієнтів та забезпечити стабільність бізнес процесів у хмарних середовищах.

Список використаних джерел

1. Назаренко Д.М. Огляд проблем захисту даних у хмарних технологіях Сучасні інформаційні системи та технології : матеріали 3-ї науково-практичної конференції. 4 – 16 Листопада 2019, Харків, Україна С. 170–172.

2. Cisco Cloudlock Documentation [Електронний ресурс] – URL: https://docs.umbrella.com/cloudlock-documentation/docs/building-different-types-of-event-policies (дата звернення: 10.08.2025).

3. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock [Електронний ресурс] – URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2663/2557 (дата звернення: 10.08.2025).

UDC 004.94:81’32

Machine learning in R&D of linguistic projects with artificial intelligence in crisis times

Svitlana Krasnyuk
Kyiv National University of Technologies and Design, Kyiv
https://orcid.org/0000-0002-5987-8681

Abstract. *Machine learning (ML) is a core element of artificial intelligence (AI) and a key tool for linguistic research during crises. Classical ML ensures interpretability and efficiency for structured data, while neural network approaches are effective for large-scale and unstructured information. In unstable contexts, ML enables automation, adaptability, and rapid analysis of texts. Its applications include natural language processing, machine translation, and corpus-based forecasting of linguistic trends. Despite challenges such as data quality, bias, and resource limitations, hybrid integration of classical and neural methods provides both accuracy and resilience. Thus, ML strengthens the stability and continuity of linguistic R&D projects in times of crisis.*

Keywords: *computational linguistics, machine learning, artificial intelligence.*