Добровольський Д. В., здобувач,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАХИСТ ІТ-ІНФРАСТРУКТУРИ В УМОВАХ ХМАРНИХ ТЕХНОЛОГІЙ

Зростання популярності хмарних технологій в останні роки викликає необхідність вдосконалення захисту ІТ-інфраструктури. З погляду бізнесу та суспільства, забезпечення конфіденційності, цілісності та доступності даних стає критичною задачею. Із зростанням кількості кіберзагроз та інцидентів, пов'язаних із кібербезпекою, виникає необхідність розробки та вдосконалення процесів побудови захищеної ІТ-інфраструктури в умовах хмарних технологій [1].

Таким чином, завдання розроблення нових дієвих та ефективних методів протидії кібернетичним атакам та несанкціонованому доступу, а також удосконалення існуючих методів і технологій є актуальним. Метою дослідження є застосування методики захисту ІТ-інфраструктури в умовах хмарних технологій для вирішення завдань своєчасного виявлення та протидії кібератак та несанкціонованого доступу до конфіденційної інформації.

Забезпечення надійного та дієвого захисту інформації, важливих компонентів ІТ-інфраструктури є комплексним завданням, яке включає в себе сукупність взаємопов'язаних між собою задач. Саме тому, для досягнення мети дослі дження запропоновано методику, яка складається з таких етапів:

- аналіз загроз та ризиків;
- фізична та мережева безпека;
- управління ризиками;
- захист даних;
- адаптація заходів до хмарних платформ;
- відповідь на регуляторні та внутрішні вимоги.

Детальний розгляд методики і демонстрація прикладу буде подано в доповіді, тому представимо коротку характеристику кожного етапу.

Першим етапом у побудові захищеної ІТ-інфраструктури є аналіз потенційних загроз та ризиків, які випливають із використання хмарних сервісів. Традиційні атаки на програмне забезпечення, функціональні атаки на елементи інфраструктури та інші типи загроз вимагають їх детального вивчення та класифікації.

Безпека ІТ-інфраструктури включає суворий контроль фізичного доступу до центрів обробки даних (ЦОД) та використання міжмережевого екрану для ефективної фільтрації та розмежування внутрішніх мереж. Захист від вторгнень є ключовим елементом в цьому контексті.

Застосування моделі управління ризиками для хмарної інфраструктури дозволяє ефективно виявляти, оцінювати та мінімізувати потенційні ризики. Це включає в себе розробку індивідуальних систем захисту для вирішення високорівневих завдань, пов'язаних із керуванням хмарним середовищем.

Основою безпеки в хмарному середовищі є шифрування даних, які зберігаються та передаються. Забезпечення захисту інформації при передачі даних, автентифікація користувачів та їх ізоляція один від одного, стають невід'ємною частиною ефективної архітектури безпеки.

З урахуванням віртуалізації, як ключового фактору у хмарних технологіях, виникає потреба в адаптації існуючих заходів безпеки до хмарних платформ. Це включає в себе контроль та управління хмарними сервісами, а також розробку спеціалізованих заходів для вирішення нових викликів.

З урахуванням росту вимог з боку зовнішніх регуляторів та внутрішніх питань політики захисту, необхідно встановити ефективну систему відповіді на ці вимоги. Це включає в себе вдосконалення технічних аспектів та розробку політики безпеки ЦОД.

Таким чином, проблема забезпечення безпеки в хмарному середовищі є достатньо складним завданням, яке вимагає системного підходу та постійного вдосконалення. Захист ІТ-інфраструктури в умовах хмарних технологій вимагає врахування специфічних загроз та впровадження сучасних методів захисту даних. Тільки так можна забезпечити надійність та безпеку використання хмарних обчислень в сучасних умовах.

Список використаних джерел

1. S. Singh. A survey on cloud computing security : Issues, threats, and solutions. – 2016. – URL: https://www.sciencedirect.com/science/article/abs/pii/S1084804516301990.