УДК 004.49

Добришин Ю.Є., к.т.н, доцент
Національна академія Служби безпеки України

ЗАГРОЗИ ТА РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ХМАРНИХ ОБЧИСЛЕННЯХ

На теперішній час політики безпеки становяться головним елементом кібербезпеки, тому що вони формалізують підходи до захисту інформаційних ресурсів, визначають правила взаємодії користувачів, програмних сервісів та модулів інформаційних систем. У традиційних інформаційних системах політики безпеки переважно орієнтувалися на захист мережевого периметра, контроль фізичного доступу та розмежування прав користувачів у межах локальної інфраструктури. Однак із розвитком хмарних обчислень такі підходи виявилися недостатніми.

На відміну від традиційних локальних систем, хмарні платформи передбачають спільне використання ресурсів, віддалений доступ і динамічну зміну конфігурацій, що істотно ускладнює ідентифікацію та управління ризиками. У таких умовах зростає значення системного підходу до аналізу загроз і формування політик безпеки.

Однією з найбільш поширених загроз у хмарних середовищах є неправильна конфігурація ресурсів. Відкриті сховища даних, надмірні права доступу та помилки в налаштуваннях мережевих політик залишаються основними причинами витоку інформації. Дослідження підтверджують, що більшість таких інцидентів пов'язані з відсутністю чітко визначених політик безпеки та недостатнім контролем відповідності конфігурацій установленим вимогам. Це свідчить про необхідність автоматизації процесів контролю та перевірки налаштувань безпеки.

Суттєвим ризиком є компрометація облікових даних користувачів і сервісних акаунтів. Хмарні середовища активно використовують механізми віддаленої автентифікації, що робить їх вразливими до фішингових атак і викрадення облікових даних. У разі отримання зловмисником доступу до облікового запису з надмірними повноваженнями можливе масштабне порушення безпеки всієї інфраструктури. Цей ризик безпосередньо пов'язаний із недотриманням принципу мінімально необхідних повноважень.

Окрему групу загроз формують внутрішні ризики, пов'язані з діями легітимних користувачів. Використання несанкціонованих хмарних сервісів і програмного забезпечення, відоме як Shadow IT, призводить

до втрати централізованого контролю над інформаційними ресурсами та ускладнює виконання вимог політик безпеки. Такі дії можуть бути як свідомими, так і ненавмисними, проте в обох випадках вони підвищують імовірність витоку або компрометації даних.

Загрози доступності інформації також мають важливе значення для хмарних середовищ. Відмови в обслуговуванні, збої в роботі сервісів або помилки масштабування можуть призвести до тимчасової чи повної недоступності критично важливих ресурсів. Хоча провайдери хмарних сервісів забезпечують високий рівень відмовостійкості, відповідальність за управління такими ризиками значною мірою покладається на користувача, який повинен враховувати їх під час формування політик безпеки.

Додатковим фактором ризику є недостатній рівень моніторингу та фіксації подій за допомогою логічних журналів. Відсутність централізованого збору та аналізу логів ускладнює своєчасне виявлення інцидентів і реагування на них. Наукові дослідження наголошують, що затримка у виявленні атак у хмарних середовищах істотно збільшує масштаби завданої шкоди та ускладнює подальше розслідування інцидентів.

Таким чином, загрози та ризики інформаційної безпеки у хмарних обчисленнях мають багатовимірний характер і тісно пов’язані з організаційними та технічними аспектами використання хмарних сервісів. Це зумовлює необхідність формування комплексних політик безпеки, які враховують специфіку хмарних середовищ, сучасні підходи до управління ризиками та результати наукових досліджень.

Список використаних джерел

1. Вахула О., Опірський І. Дослідження проблематики безпеки в хмарних середовищах та вирішення з застосуванням підходу “безпека як код”. *Ukrainian information security research journal*. 2023. Т. 25, № 3. С. 113–122. URL: https://doi.org/10.18372/2410-7840.25.17936 (дата звернення: 17.03.2026).

2. Король М., Опірський І. Дослідження та аналіз проблем та викликів, що виникають у забезпеченні кібербезпеки в хмарних обчисленнях. *Ukrainian information security research journal*. 2024. Т. 26, № 1. С. 63–71. URL: https://doi.org/10.18372/2410-7840.26.18829 (дата звернення: 16.03.2026).

3. Ojha P. Enhanced cloud computing security based on single to multi cloud systems. *Journal of research in science and engineering*. 2024. Т. 6, № 8. С. 52–56. URL: https://doi.org/10.53469/jrse.2024.06(08).12 (дата звернення: 10.03.2026).