Володимир ФЛЬОНЦ;
проф., д.т.н. Дмитро ЛАНДЕ.

АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ХМАРНИХ ТА ГІБРІДНИХ СЕРЕДОВИЩАХ ДЛЯ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНО-ПОШУКОВИХ СЕРВІСІВ

Анотація. Проведений порівняльний аналіз підходів до побудови інформаційної безпеки в хмарних та гібридних середовищах для реалізації інформаційно-пошукових сервісів в малих та середніх об'єднаних територіальних громадах із застосуванням 14 принципів хмарної безпеки Національного центру кібербезпеки Великобританії (NCSC).

Summary. A comparative analysis of approaches to building information security in cloud and hybrid environments for the implementation of information and search services in small and medium-sized united territorial communities using the 14 principles of cloud security of the National Cyber Security Center of Great Britain (NCSC).

Ключові слова: інформаційна безпека, хмарні середовища, хмарні послуги.

Прийняття в лютому 2022 року Закону України «Про хмарні послуги» визначило основні правові відносини, що виникають при наданні хмарних послуг, та встановило особливості використання хмарних послуг органами державної влади та органами місцевого самоврядування. Швидке поширення хмарних технологій та їх використання для хостингу публічних і службових сервісів органами державної влади та органами місцевого самоврядування створюють необхідність пошуку ефективних рішень для забезпечення належного рівня інформаційної безпеки і відповідей на кіберзагрози національного кіберпростіру.

Наразі національні вимоги до хмарних сервісів в тому числі до забезпечення інформаційної безпеки під час використання хмарних послуг розробляються і впроваджуються прямо зараз. Проте їх відсутність не зупиняє практичне розгортання та експлуатацію інформаційних сервісів в хмарному середовищі. Тому доцільним може буде використання міжнародного досвіду і підходів до побудови інформаційної безпеки, зокрема 14 принципів хмарної безпеки Національного центру кібербезпеки Великобританії (NCSC).

З точки зору інформаційної безпеки, однією з найбільших груп ризику серед публічних користувачів хмарних послуг є органи

місцевого самоврядування малих територіальних громад з населенням до 100 тисяч громадян. Для дослідження потреб публічних користувачів хмарних послуг було опитано 10 територіальних громад різних розмірів, від об'єднаної територіальної громади села до райцентру. За результатами опитування виявилось, що кожна територіальна громада експлуатує та підтримує роботу від 3 до 8 інформаційних сервісів, зокрема офіційних веб-сайтів з публічним доступом. В Таблиці 1 наведено п'ять найпоширеніших сервісів, що використовують малі територіальні громади:

Таблиця 1. Найпоширеніші сервіси територіальних громад.

Назва інформаційної системи або сервісу	**Кількість ОТГ (з 10)**
Офіційний веб-сайт територіальної громади	10
Звернення громадян, доступ до публічної інформації	10
Веб-сайт центру надання адміністративних послуг	8
Сервіс електронних петицій	7
Веб-сайт міської (селищної) ТВК	6

Порівняння підходів до побудови інформаційної безпеки у надавачів хмарних послуг відбувалось у двох категоріях:

1) національні надавачі хмарних послуг, що мають атестат відповідності за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог і норм інформаційної безпеки, та/або впровадили систему управління інформаційною безпекою відповідно до європейських стандартів ISO/IEC 27001: DeNovo, Gigacloud;

2) міжнародні надавачі хмарних послуг, що впровадили СУІБ відповідно до ISO/IEC 27001 і пропонують рішення для урядів європейських країн: Amazon Web Services, Microsoft Azure та Google Cloud.

Порівняння проводилось з урахуванням інформаційного ризику, що визначається як функція трьох змінних:

$$R = \sum_i P(t)_i \cdot P(v)_i \cdot S_i$$

де $P(t)$ - ймовірність реалізації загрози; $P(v)$ - ймовірність наявності вразливості; S – потенційний вплив; $i = 1..n$ – кількість загроз.

Висновки. В результаті вивчення потреб публічних користувачів хмарних послуг і порівняльного аналізу надавачів хмарних послуг, можна зробити наступні висновки:

- підходи до побудови інформаційної безпеки і реалізації послуг з кіберзахисту у національних та міжнародних надавачів відрізняються

в першу чергу згідно до основної послуги яку вони пропонують: у національних надавачів це інфраструктура як послуга (IaaS), у міжнародних надавачів це платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS), відповідно використання національних надавачів потребує глибшого розуміння ризиків інформаційної безпеки і часто власноручної реалізації безпекових послуг;

- суттєвим викликом залишається відсутність необхідних підзаконних нормативно-правових актів, які мають визначити національні вимоги до надавачів хмарних послуг, що в свою чергу стримує використання хмарних послуг публічними користувачами хмарних послуг, такими як малі територіальні громади;
- використання малими територіальними громадами хмарних послуг із застосуванням 14 принципів хмарної безпеки, для розміщення офіційних інформаційно-пошукових сервісів, дозволяє забезпечити виконання вимог інформаційної безпеки із використанням меншого бюджету порівняно з реалізацією на фізичних (bare-meal) серверах.