ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до бакалаврської роботи

на тему: **“ Метод та засоби встановлення особистих ключів користувачів в хмарному середовищі”**

Виконав: студент 5 курсу, групи
РТЗ-51
спеціальності
172 Телекомунікації і радіотехніка
(шифр і назва спеціальності)

Козачок В.С.
(прізвище та ініціали)

Керівник _____
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконт-
роль_____

Київ – 2021

Р Е Ф Е Р А Т

Текстова частина бакалаврської роботи: 66 стр., 11 рисунків, 1 таблиця, 28 джерел.

Об'єкт дослідження - процеси безпечного управління ключовими даними користувачів хмарних сервісів для надання безпечних транскордонних електронних послуг.

Предмет дослідження - показники якості функціонування мережі майбутнього покоління.

Мета роботи - забезпечення безпеки в хмарних обчисленнях в частині управління ключами для різних моделей розгортання хмари.

Методи дослідження - механізми управління ключами користувачів хмарних сервісів в умовах різних моделей розгортання та надання послуг в хмарі.

У роботі досліджено побудову застосування хмарних обчислень виявив ряд проблемних питань відносно надання користувачам послуг з безпеки інформації. Тобто проблемними є питання забезпечення необхідних рівнів конфіденційності, цілісності, справжності, доступності та неспростовності на усіх етапах її життєвого циклу.

Проведений аналіз дозволив зробити висновок що в суттєвій мірі рівень безпеки інформації, що надається користувачам хмарних сервісів при хмарних обчисленнях визначається якістю управління ключовими даними. При цьому головною проблемою сервісу управління ключовими даними для клієнтів є його розгортання та функціонування в інфраструктурах, які контролюються та управляються в основному постачальниками хмарних послуг. За таких умов користувачі хмарних сервісів в явному виді потребують додаткових гарантій зі сторони постачальника хмарних послуг відносно управління ключовими даними та в ряді випадків в цілому ключовою інформацією.

Особливо проблемними питаннями при використанні хмарних сервісів є управління особистими ключами при виконання асиметричних криптографічних перетворень та таємними ключами при використанні симетричних криптографічних перетворень, а також забезпечення довіри до третьої довіреної сторони у вигляді інфраструктури відкритого ключа.

Галузь використання - сучасні системи хмарних сервісів.

ХМАРНІ ОБЧИСЛЕННЯ, КЛЮЧІ КОРИСТУВАЧІВ, ПОКАЗНИКИ ЯКОСТІ, ОБСЛУГОВУВАННЯ , БАЗА ДАНИХ, IAAS, PAAS, SAAS, УПРАВЛІННЯ КЛЮЧАМИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЦСК	-	Акредитований центр сертифікації ключів
АС	-	Автоматизована система
БД	-	База даних
ЕК	-	Еліптична крива
ЕОМ	-	Електронно-обчислювальна машина
ЕЦП	-	Електронно-цифровий підпис
ІВК	-	Інфраструктура відкритих ключів
ІТС	-	Інформаційно-телекомунікаційна система
КЗІ	-	Криптографічний захист інформації
КСЗІ	-	Комплексні системи захисту інформації
КРА	-	Криптографічний аналітик
НДР	-	Науково-дослідна робота
НСД		Несанкціонований доступ
НШ	-	Направлене шифрування
ОС	-	Операційна система
ПЗ	-	Програмне забезпечення
ПК	-	Персональний комп’ютер
СМО	-	Система масового обслуговування
ТЗІ		Технічний захист інформації
ЦОД	-	Центр обробки даних

ВСТУП

Дослідження кінця двадцятого століття дозволили визначити один із основних напрямків вирішення вказаних проблем на основі створення та застосування систем хмарних обчислень. Нині до таких технологій проявляє велику зацікавленість як великий так і малий бізнес, який намагається за рахунок використання хмарних сервісів оптимізувати свої витрати в процесі різних видів діяльності. Також значну увагу хмарним обчисленням приділяють науковці та технологи, для яких застосування хмарних обчислень дозволяє суттєво скоротити час виконання досліджень та впровадження їх результатів на практиці.

Кабінетом міністрів України в 2013 році було прийнято розпорядження «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [1], якою було передбачено створення та застосування суперкомп'ютерних систем, зокрема на основі та «хмарних» технологій. Також до Верховної Ради України було 24 березня 2016 року було внесено проект «Закону про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» [2].

Актуальність теми. Досвід застосування хмарних обчислень виявив ряд проблемних питань відносно надання користувачам послуг. Тобто проблемними є питання забезпечення необхідних рівнів конфіденційності, цілісності, справжності, доступності та неспростовності на усіх етапах її життєвого циклу.

Проведений аналіз дозволив зробити висновок що в суттєвій мірі рівень безпеки інформації, що надається користувачам хмарних сервісів при хмарних обчисленнях визначається якістю управління ключовими даними. При цьому головною проблемою сервісу управління ключовими даними для клієнтів є його розгортання та функціонування в інфраструктурах, які контролюються та управляються в основному постачальниками хмарних послуг. За таких умов користувачі хмарних сервісів в явному виді потребують додаткових гарантій зі сторони поста-

чальника хмарних послуг відносно управління ключовими даними та в ряді випадків в цілому ключовою інформацією.

Особливо проблемними питаннями при використанні хмарних сервісів є управління особистими ключами при виконання асиметричних криптографічних перетворень та таємними ключами при використанні симетричних криптографічних перетворень, а також забезпечення довіри до третьої довіреної сторони у вигляді інфраструктури відкритого ключа.

На їх вирішення направлена інтенсивна та достатньо охоплююча система стандартизації Національного інституту стандартів та технологій (NIST), та розпочата міжнародна стандартизація, яка находиться в більшості випадків на етапі проектів.

Мета роботи. Метою бакалаврської роботи є забезпечення безпеки в хмарних обчисленнях в частині управління ключами для різних моделей розгортання хмари (приватна, публічна, громадська та гібридна) та різних рівнях надання послуг (IaaS, PaaS, SaaS).

Управління ключами користувача в хмарі складається з процедур, що забезпечують:

– реєстрацію користувача в системі;
– генерацію, розподіл та введення ключів до засобів захисту;
– контроль над використанням ключів;
– зміна та знищення ключів;
– сертифікація ключів;
– архівування, зберігання та відновлення ключів.

Для досягнення мети необхідно вирішити низку таких наукових задач:

– побудова та аналіз моделі загроз для різних варіантів розгортання хмари та управління ключами;

– побудова та аналіз складених механізмів управління ключами для кінцевих користувачів в середовищі хмари;

– обґрунтування вимог до засобів КЗІ для встановлення ключів при хмарних обчисленнях;

– розроблення та обґрунтування практичних рекомендацій зі створення комплексної системи захисту інформації (КСЗІ) хмарних обчислень.

Об’єкт досліджень – процеси безпечного управління ключовими даними користувачів хмарних сервісів.

Предмет дослідження – механізми управління ключами користувачів хмарних сервісів

1 АНАЛІЗ ПРОБЛЕМНИХ ПИТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ

1.1 Обґрунтування захисту інформації в хмарних середовищах

Нині до хмарних технологій все більше проявляє зацікавленість великий та малий бізнес, який намагається за рахунок їх використання оптимізувати свої витрати на підтримку та розгортання IT інфраструктури, а саме знизити капітальні витрати на побудову центрів обробки даних, закупівлю серверного та мережевого обладнання, апаратних і програмних рішень, забезпечення безперервності і працездатності, а також час побудови та введення в експлуатацію нових потужностей.

На тлі оптимізації витрат до хмарних технологій проявляють зацікавленість не тільки великі компанії, які намагаються оптимізувати свої витрати на IT інфраструктуру підприємства, але й малі компанії, які не мають можливості відразу розгорнути свою власну інфраструктуру, а також звичайні користувачі для яких пропонуються такі послуги як зберігання даних та їх обробка, використання програм та сервісів, що надаються он-лайн.

Але, незважаючи на явні переваги при використанні хмарних обчислень необхідно вирішувати і ряд проблемних питань захисту інформації – основними з них є довіра до постачальника сервісу, забезпечення конфіденційності, цілісності, доступності, справжності та неспростовності інформації на усіх етапах її існування, безперебійність в роботі, захист від несанкціонованого доступу (НСД) та збереження важливих даних користувачів, які передаються та обробляється в хмарі.

Необхідність в забезпеченні захисту даних клієнта від порушення конфіденційності та цілісності, несанкціонованого доступу до даних та ресурсів хмари, що надаються клієнту, контролі та управлінні доступом клієнтів до ресурсів хмари, наданні криптографічних послуг з захисту інформації для клієнтів в середовищі хмари, а також управління хмарною інфраструктурою провайдером хмарних послуг, вимагає створення сервісу з управління ключами. Головною проблемою сервісу управління ключами для клієнтів є його розгортання в інфраструктурі, що

контролюється постачальником хмарних послуг. Тобто користувач хмарного сервісу потребує додаткових гарантій постачальника хмарних послуг, що розташовані в хмарі особисті чи таємні ключі не будуть скомпрометовані.

Актуальність розглянутих задач, в першу чергу зумовлена тим, що їх вирішення дозволить суттєво підвищити рівень довіри користувачів до хмарних обчислень та сприятиме їх поширенню та впровадженню.

1.2 Стан створення та застосування хмарних середовищ

В подальшому при дослідженнях безпечності обробки інформації під хмарними обчисленнями будемо розуміти модель забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню, та які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера. Також будемо вважати, що надання хмарних послуг може реалізовуватися з використанням наступних видів інфраструктури побудови хмари: приватна хмара (англ. private cloud), громадська хмара (англ. community cloud), публічна хмара (англ. public cloud), гібридна хмара (англ. hybrid cloud). При цьому основною ознакою за якою відрізняються інфраструктури хмарних обчислень будемо вважати категорії користувачів, що мають доступ до даних і ресурсів хмари.

За рівнем доступу до ресурсів постачальника послуг прийнято розрізняти наступні моделі надання послуг в хмарі [10]: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS), інфраструктура як послуга (IaaS).

Основними перевагами використання технологій хмарних обчислень є гнучкость налаштування параметрів, можливостіь доступу до ресурсів в хмарі, використовуючи Інтернет з’єднання, швидке розгортання сервісів та збільшенні робочого навантаження, підтримка резервування, самовідновлення та масштабування, управління робочими навантаженнями в реальному часі, а також моніторинг в реальному часі завантаження та баланс системи і виділенні ресурсів.

Використання хмари з точки зору захисту інформації надає такі переваги як централізоване керування, конфігураціє системи безпеки та її аудит, можливість динамічного масштабування ресурсів системи, резервування та аварійного відновлення, а також централізоване зберігання даних, що дозволяє підвищити їх захист. Важливим фактором є наявність спеціалізованого персоналу з безпеки.

До ***основних недоліків*** використання хмарних обчислень відносяться такі як: неможливість роботи з сервісами хмари без постійного підключення до Інтернет, складний або неможливий процес переходу від одного постачальника хмарних послуг до іншого, відсутність єдиного міжнародного правового регулювання в сфері хмарних обчислень та обробки інформації в хмарі, а також довіра користувачів до постачальника послуг та питання безпеки даних користувача.

До недоліків використання хмарних обчислень з точки зору безпеки інформації необхідно віднести:

– складність системи для проведення аналізу загроз;

– багатокористувацьке середовищі, що може спричинити виток інформації;

– порушення доступності, при відсутності Інтернет з’єднання;

– привілегійовані користувачі та адміністратори хмари, що можуть мати доступ до даних користувачів;

– відсутність стандартизованих інтерфейсів, для забезпечення резервного копіювання, архівування та відновлення інформації після збоїв або зміни провайдера послуг;

– втрата контролю над інфраструктурою системи тощо.

1.3 Аналіз основних джерел інформації відносно хмарних обчислень

На сьогодні провідними організаціями, що займаються створенням рекомендацій, нормативних документів та стандартів в сфері захисту інформації в хмарних обчисленнях є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, дві державні організації Європи та США: Європейське агентство мережевої та інформаційної безпеки (ENISA) і На-

ціональний інститут стандартів і технологій (NIST), та комітет міжнародної організації з стандартизації ISO/IEC JTC 1/SC 27.

Підвищений інтерес до впровадження хмарних сервісів та їх активне застосування зумовило появу нових міжнародних та закордонних державних стандартів, роз'яснень та рекомендацій з використання хмарних сервісів та забезпечення безпеки в середовищі хмари. Окрім провідних державних організацій Європи та США: Європейського агентства мережевої та інформаційної безпеки (ENISA) і Національного інституту стандартів і технологій (NIST), питаннями стандартизації займається комітет міжнародної організації з стандартизації ISO/IEC JTC 1/SC 27, та об'єднання представників IT-індустрії в сфері хмарних технологій – Альянс безпеки в хмарі (Cloud Security Alliance, CSA).

Аналізу існуючих загроз, побудові моделей загроз та порушника в хмарі присвячено низку публікацій. Так, в роботі [13], автор розглядає питання безпеки ключів, довіри до провайдера, управління ризиками, безпекою архітектури хмарного середовища, управління доступом, захисту даних та ізоляції програм. Подальший розвиток його робота знайшла в якості рекомендацій NIST SP 800-144.

В наукових дослідженнях проводиться детальний аналіз існуючих загроз хмарних обчислень з урахуванням стандартів та рекомендації, що розробляються NIST, ISO\IEC, CSA.

В роботі [6] аналізуються доступні механізми захисту віртуального середовища в хмарі при використанні моделі розгортання IaaS. До розглянутих методів захисту відносяться: захист образів віртуальних машин від порушення цілісності, конфіденційності та доступності, налаштування захисту образів віртуальних машин від вірусів та шпигунського програмного забезпечення (ПЗ), захист внутрішніх мереж. Аналіз питань безпеки управління ключами в хмарі проводиться в роботі [8].

Авторами в роботі [9] робиться аналіз сучасного стану стандартизації в області забезпечення безпеки хмарних обчислень та пропонується підхід з аналізу ризиків, що дозволяє оцінити відповідність хмарного рішення заявленим рівням безпеки.

Аналіз джерел показав, що найбільша увага приділяється аналізу, класифікації та побудові моделей загроз та порушника для хмари при цьому питання моделі загроз управління ключами та ключовими даним недостатньо розроблені. В той же час нині застосування хмарних технологій користувачами, як показав аналіз, в суттєвій мірі залежить від довіри до управління ключовими даними в плані захисту від виявлених загроз.

Також запропоновані моделі управління ключовими даними користувачів не в повній мірі відповідають вимогам хмарного середовища та вимогам захисту ключів.

Окремо слід відзначити відсутність публікацій в області оцінки ефективності та порівняння різних моделей управління ключами.

1.3.1 Стандарти та проекти стандартів NIST

Національний інституту стандартів і технологій в якості пріоритетних виділив такі три області як інформаційна безпеки, інтероперабельність (сумісність) та вимоги до переносимості хмарних послуг. Ним було прийнято низку стандартів, що стосуються питань захисту інформації в середовищі хмарних обчислень. До них відносяться стандарти NIST SP 800-145 та NIST SP 800-146 [10, 11], які визначають поняття хмарних обчислень та надають загальні рекомендації з їх використання та стандарти NIST SP 500-292 і NIST SP 500-293, що визначають хмарну архітектуру, основні її компоненти та механізми взаємодії між ними. Також було прийнято стандарт NIST SP 800-144 [14], який описує питання забезпечення безпеки та конфіденційності в середовищі відкритих хмарних обчислень, та опубліковано проект стандарту NIST SP 500-299 [12], який визначає архітектуру безпеки та модель загроз хмари. Важливим є прийняття стандарту NIST SP 800-125, який описує безпеку технологій повної віртуалізації.

Крім того, загальні стандарти з безпеки, що розроблені NIST, застосовуються до хмарних обчислень, а саме стандарт з керування ризиками, визначення механізмів управління безпекою та конфіденційністю, а також рекомендації з управ-

ління безпекою для федеральних інформаційних систем та організацій NIST SP 800-53 [14], безперервний моніторинг безпеки в федеральних інформаційних системах та організаціях NIST SP 800-137, запис до журналу подій безпеки (NIST SP 800-92) та інші.

В липні 2013 року публікацією NIST SP 500-291 було визначено загальні стандарти, що розробляються та прийняті в сфері захисту хмарних обчислень.

1.3.2 Стандарти та проекти стандартів ISO/IEC

На сьогодні завершено роботу над стандартом ISO / IEC 27018: 2014 «Інформаційні технології. Методи забезпечення безпеки. Практика захисту персональних даних в публічних хмарах, що виступають у ролі обробників персональних даних».

Цей документ містить рекомендації для постачальників хмарних послуг, що обробляють персональні дані і пропонує ряд заходів контролю та управління, які постачальникам слід реалізувати для зменшення ризиків в середовищі публічних хмарних обчислень. Стандарт в першу чергу має на меті сприяти підвищенню довіри до постачальників послуг публічних хмар, а також надати рекомендації щодо того, що необхідно виконувати в рамках договірних зобов'язань і законодавчо-нормативних вимог постачальникам хмарних послуг.

Окрім цього він включає в себе стандарти прозорості, у тому числі повідомлення клієнтів про запити правоохоронних органів на доступ до їх даних і розкриття перед клієнтами відомостей про використання послуг субпідрядників.

Також цей стандарт розглядається як основа для відповідності вимогам національного та наднаціонального законодавства, містить елементи з європейської Директиви 95/46 ЕС про захист персональних даних, такі, як принципи якості обробки. Він також включає в себе принцип підзвітності. Стандарт ISO / IEC 27018: 2014 служить доповненням до стандарту ISO / IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», який встановлює загальні вимоги до систем менеджменту інформацій-

ної безпеки. Він встановлює загальноприйняті цілі та механізми контролю, а також надає керівництво щодо їх реалізації з метою захисту персональних даних відповідно до принципів забезпечення приватності, сформульованими у міжнародному стандарті ISO / IEC 29100 «Інформаційні технології. Методи забезпечення безпеки. Схема конфіденційності» для публічних хмарних середовищ.

Керівні принципи даного стандарту базуються на ISO / IEC 27002 «Інформаційні технології. Методи забезпечення безпеки. Звід правил по управлінню захистом інформації». В свою чергу в розробці комітету також знаходиться стандарт ISO/DIS 27017 «Інформаційні технології - Методи забезпечення безпеки - Система менеджменту хмарної безпеки і захисту персональних даних - Заходи безпеки», що базується на ISO / IEC 27002. Даний Міжнародний стандарт пропонує заходи контролю та управління, а також рекомендації щодо їх впровадження як постачальникам хмарних послуг, так і їх клієнтам.

Крім стандартів з безпеки ISO / IEC в 2014 році було опубліковано стандарти ISO / IEC 17788 «Інформаційні технології - Розподілені прикладні платформи і сервіси - Хмарні обчислення - Загальні положення та словник»; ISO / IEC 17789 «Інформаційні технології - Хмарні обчислення - Еталонна архітектура». Стандарт ISO / IEC 17788 описує концепцію хмарних обчислень і містить ряд термінів і визначень. Він стане термінологічної основою для подальшої роботи зі стандартизації у сфері хмарних обчислень [12-13].

Стандарт ISO / IEC 17789 містить огляд загальних понять і характеристик хмарних обчислень, типів хмар, компонент хмарних обчислень сторін-учасниць, а також взаємовідносин між цими елементами. У ньому зроблено наголос на вимоги до того, що повинні забезпечувати хмарні сервіси, а не на питання проектування та впровадження відповідних рішень.

1.3.3 Стандарти та проекти стандартів, що визначають управління даними в хмарі

В вересні 2013 року NIST було опубліковано внутрішній звіт NIST IR 7956, що на основі набору функцій в трьох базових моделях надання послуг в хмарі, визначає функції безпеки, криптографічні функції, а також вимоги та задачі з управління ключами в середовищі хмарних обчислень. Криптографічні алгоритми з управління ключами, що містяться в документі NIST IR 7956, детально розглянуті в таких документах, як NIST SP 800-57-1, NIST SP 800-57-2 та NIST SP 800-57-3 [14-17].

Станом на початок 2016 року міжнародною організацією ISO/IEC не розробляється стандарт з управління ключовими даними в хмарі, але існуючі стандарти управління ключами з сімейства ISO / IEC 11770, які прийняті в Україні можуть бути використані в хмарній інфраструктурі.

1.4 Модель хмари

Першочерговою задачею при аналізі будь-якої системи є побудова моделі цієї системи з завданим рівнем деталізації. Модель хмари, запропонована NIST SP 500-292 [5] включає в себе 5 основних ролей: користувач хмари, провайдер хмарних послуг, провайдер доступу до хмарних послуг, аудитор хмари, хмарний брокер (рис. 1.1).

Рис. 1.1. Модель хмари

Розглянемо окремо кожну з ролей та функції, що вона виконує.

1. Користувач хмари – особа або організація, яка підтримує ділові відносини з постачальниками хмарних послуг і використовує їх сервіси.

Взаємодія користувача з постачальником хмарних послуг відбувається через брокера, використовуючи постачальника доступу до хмарних послуг. В залежності від потреб користувач використовує різні рівні сервісів, що пропонуються постачальником, у зв’язку з чим має доступ до програмних додатків в хмарі (SaaS), операційної системи та розробки програмних додатків (PaaS), віртуальних комп’ютерів та компонентів мережі (IaaS). Споживі користувачем ресурси можуть бути виміряні як час роботи додатків чи операційної системи, використана загальна процесорна потужність тощо.

2. Провайдер хмарних послуг – особа або організація відповідальна за створення та управляння хмарою та її службами. Провайдер також займається підтримкою інфраструктури та програмного забезпечення, яке забезпечує роботу хмари.

В залежності від рівня надання послуг провайдер може займатися розгортанням хмарних послуг, конфігурувати, підтримувати і оновлювати роботу про-

грамних додатків хмарної інфраструктури (SaaS), управляти обчислювальною інфраструктурою для платформи та контролювати програмне забезпечення компонентів хмари: стеку програмного забезпечення, баз даних та іншого службове забезпечення (PaaS), контролювати програмне забезпечення, яке необхідне для доступу користувачів до хмарних послуг: хостові операційні системи (ОС) і гіпервізор віртуалізації, а також фізичні сервери, мережеве обладнання, пристрої зберігання даних (IaaS).

Провайдер, що надає послуги на рівні SaaS виконує більшість обов'язків з управління та контролю додатків та інфраструктури, в той час як споживачі мають обмежений адміністративний контроль додатків. На рівні PaaS користувачу надається доступ до середовища розробки додатків для хмарних сервісів (IDE) та набору компонентів програмного забезпечення для розробки (SDK), при цьому користувач має доступ до налаштувань програмного забезпечення та деяких налаштувань хмарного середовища, можливий також доступ до деяких налаштувань нижнього рівня: операційної системи, мережі, файлового сховища. Рівень сервісу IaaS представлений віртуалізацією фізичних компонентів до яких має доступ користувач: сервери, комп’ютерні мережі, мережне обладнання та інше підтримуюче обладнання.

3. Аудитор хмари – особа або організація, яка може виконувати незалежну експертизу хмарного сервісу, на основі перевірки відповідності побудованої хмари стандартам, оцінці послуг, що надаються провайдером хмари з точки зору контролю безпеки, недоторканності приватного життя, продуктивності і т.д.

Аудит безпеки також включає перевірку дотримання політики безпеки, регулюючих документів та відповідності до чинних законів про конфіденційність, цілісність та доступність інформації на всіх етапах розробки та експлуатації хмари.

4. Хмарний брокер – особа або організація, яка керує використанням, продуктивністю і доставкою хмарних послуг, а також веде переговори між провайдерами хмари і споживачами.

Основною задачею брокера – є полегшення взаємодії користувачів з про-

вайдерими хмарних послуг, за рахунок поліпшення управління доступом до хмарних сервісів, ідентифікацією користувачів, отримання результатів звітності, підвищення рівня безпеки. Також брокер може виконувати функції агрегації послуг: поєднувати в собі та інтегрувати кілька служб в одну або кілька нових послуг, забезпечувати інтеграцію даних та їх безпечне переміщення між споживачем хмари і провайдером хмарних послуг. Функція арбітражу брокера схожа на функцію агрегації послуг, однак послуги, що агрегуються не є фіксованими та є можливість обирати та об'єднувати послуги від декількох провайдерів.

5. Провайдер доступу до хмарних послуг – посередник, який забезпечує підключення і транспортування хмарних послуг від хмари до споживачів.

На основі моделі хмари (рис. 1.1), в NIST SP 500-293 було запропоновано формальну модель безпеки хмари (рис. 1.2), яка визначає компоненти безпеки для кожної з ролей в хмарі. Компоненти безпеки було розмішено відповідно функції та областей діяльності ролі в хмарі. У випадку коли ролі (або компоненти формальної моделі хмари) виконують ідентичні функції безпеки або виконують їх разом, компонент безпеки охоплює декілька ролей (компонентів формальної моделі хмари).

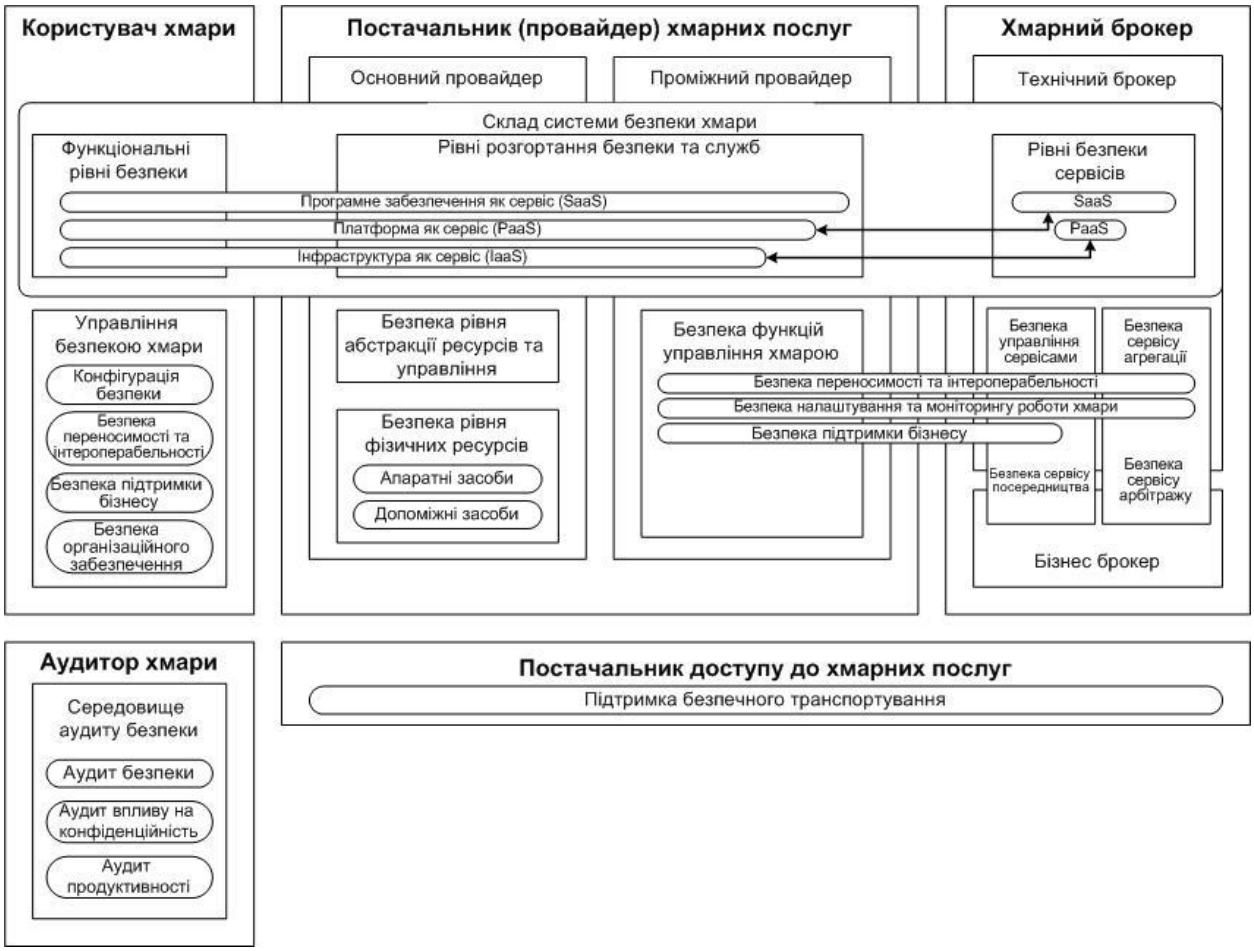

Рис. 1.2. Формальна модель безпеки хмари

Розглянемо більш детально компоненти архітектури безпеки та їх основні функції. До складу ролі «Користувач хмари» входять наступні компоненти безпеки:

Управління безпекою хмари – компонент безпеки, що включає в себе всі функції, які необхідні для управління та роботи сервісу, який використовує користувач хмарних послуг. Він поділяється на наступні субкомпоненти:

– безпека переносимості та інтероперабельності гарантує переміщення та розгортання між різними провайдерами хмарних послуг або брокерами даних, додатків, сервісів користувача з дотриманням конфіденційності, цілісності та надійності;

– безпека підтримки бізнесу включає питання безпеки з ведення ділових відносин з іншими ролями в хмарі, наприклад: управління контрактами (підпи-

сання, розірвання, виконання), закупівля послуг, керування обліковими записами користувачів та інше;

– безпека організаційного забезпечення, що охоплює політику, процедури і процеси, що надаються організацією для підтримки безпечного управління споживанням хмарних послуг;

– конфігурація безпеки, що включає інструменти та політики, використання яких забезпечує налаштування безпеки хмарних ресурсів з дотриманням стандартів безпеки, технічних умов та правил, в тому числі угод з надання відповідного рівня сервісу. В рамках цього компонента повинні бути розглянуті питання безпеки оперативного розгортання хмарних систем, зміни та оновлення в конфігурації розгорнутої системи, моніторингу, звітності, вимірювання та обліку спожитих ресурсів, забезпечення рівня обслуговування;

До складу системи безпеки хмари входить сукупність елементів системи, які підтримують надання хмарних послуг в організації, координацію і управління обчислювальними ресурсами хмарних сервісів з метою надання безпечних послуг користувачам. Субкомпоненти, що входять до складу компонентів системи безпеки для користувача хмари є функціональні рівні безпеки, що реалізуються користувачем для забезпечення необхідної функціональності, та нерозривно корелює з наборами компонентів безпеки, що реалізовані іншими хмарними суб'єктами. В якості верхнього шару використовується інтерфейс наданий провайдером послуг чи брокером.

Компоненти безпеки ролі «Провайдер хмарних послуг» розміщенні на всіх рівнях хмари, що контролюються провайдером та визначаються в залежності від сервісів, що їм реалізуються та надаються, а саме сервіс впровадження, сервіс оркестровки, сервіс управління хмарою, сервіс безпеки та конфіденційності. Існує два типи провайдерів: основний та провайдер-посередник. Основний провайдер надає послуги клієнтам за допомогою технічного брокеру або провайдера-посередника. Аналогічно свої послуги клієнтам надає провайдер-посередник, крім цього він може співпрацювати з декількома основними провайдерами. В зв’язку з чим провайдер-посередник не тільки включає всі компоненти безпеки основного

провайдера, але додатково включає компонент безпеки для роботи з декількома провайдерами.

Зазвичай, постачальниками доступу до хмарних послуг виступають провайдери телекомунікаційних мереж, що фізично з’єднують та забезпечують передачу інформації між провайдерами хмарних послуг та їх користувачами. Головними вимогами, що висуваються до провайдерів є надання безперервного, надійного та безпечного каналу доступу до провайдера хмарних послуг.

1.4.1 Управління ключами в хмарі

Управління ресурсами, що надають хмарні сервіси, та пов’язаною з нею інфраструктурою хмари є невід’ємною складовою частиною хмарних обчислень. Для взаємодії з різними службами в хмарі, обробка, передавання та зберігання даних сервісами хмари, необхідно реалізовувати функції безпеки. Засновуючись на базовому наборі функцій сервісів для трьох основних типів надання послуг: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) і програмне забезпечення як послуга (SaaS), можна визначити набір функцій безпеки, необхідних для реалізації функцій сервісу і криптографічних операції.

2 ДОСЛІДЖЕННЯ МОДЕЛІ ЗАГРОЗ ДАНИМ ІТС ХМАРНИХ ОБЧИСЛЕНЬ

2.1 Класифікація ключових даних та ключової інформації за власником

Аналіз показує, що незалежно від моделі розгортання та обслуговування хмари, всі ключі, що використовуються в середовищі хмарних обчислень можна поділити за призначенням та власником на такі два класи:

– ключі, що використовуються провайдером хмарних послуг та є його власністю;

– ключі, що використовуються клієнтами провайдера хмарних послуг та є їх власністю.

Наприклад, якщо хмара розгорнута як публічна та надає послуги PaaS, то користувач хмари на основі сервісу, що надається провайдером, реалізує свої рішення, послугами якого користуються клієнти користувача. За цих умов користувач для своїх клієнтів буде виступати в якості провайдера хмарних послуг, а отже в цьому випадку будуть існувати також два класи ключів:

– клас ключів провайдера хмарних послуг, до якого відносяться ключі провайдера хмарних послуг публічної хмари, що надає послуги PaaS та ключі користувача хмари, по відношенню до клієнтів користувача;

– клас ключів користувача хмарних послуг, до якого відносяться по відношенню до провайдера хмарних послуг, ключі користувача хмарних послуг та ключі клієнтів користувача хмарних послуг.

Аналогічним чином можна виділити та показати існування лише двох класів ключів для інших моделей розгортання та надання послуг в хмарі. Така модель хмари, у якій існує тільки дві ролі – користувач та провайдер, на відміну від моделі NIST, дозволяє зменшити складність аналізу безпеки управління ключами, включаючи крипто живучість.

Роль аудитора хмари, може бути виключена, за рахунок того, що вона виступає в якості пасивного елементу хмари, та має доступ до хмари лише під час проведення аудиту з використанням строгого переліку доступних можливостей.

Вказане є справедливим і до посередника (брокера) хмарних послуг, який для провайдера хмарних послуг розглядається з точки зору клієнта, а для клієнта брокер є провайдером хмарних послуг. Теж саме можна прийняти і до транспортувальника хмарних послуг – його головна задача, це забезпечення доступності сервісів. За забезпечення конфіденційності та цілісності даних, що передаються, відповідають користувач та провайдер хмарних послуг.

Ґрунтуючись на наведеному, розглянемо модель порушника хмарних обчислень, на основі якої побудуємо модель загроз відносно управління ключовими даними.

2.2 Класифікація ключових даних та ключової інформації за призначенням

Стандарт NIST SP 800-57, що є основним нормативним документом в сфері управління ключовими даними США, визначає два основні типи ключової інформації, що потребує забезпечення безпеки:

– ключі (підпису, перевірки підпису, автентифікації, шифрування даних, шифрування ключів, генерації псевдовипадкових послідовностей, генерації ключів, транспортування ключів, встановлення ключів, авторизації);

– загальна та службова інформація (загальносистемні параметри, вектори ініціалізації, спільні секрети, дані заповнення генераторів випадкових чисел (seed), відкрита інформація протоколів (nonce), дані передобчислень або виконання криптографічних операцій, інформація для управління ключами (ідентифікатор ключа), випадкові числа, що застосовуються для генерації ключів, паролі, інформація журналу аудиту).

За типом криптографічної системи, в якій застосовуються ключі, вони поділяються на симетричні та несиметричні ключі. В свою чергу несиметричні

ключі поділяються на особисті та відкриті. За рівнем доступу ключі можуть бути секретними (зазвичай симетричні, та особисті) або загальнодоступними (несиметричні відкриті).

Наведена класифікація ключових даних за призначенням та застосуванням дозволяє виявити та визначити ряд проблемних питань, а також сформулювати вимоги до ключових даних за умови їх застосування для хмарних сервісів. Причому, основні проблемні питання пов'язані з управлінням ключовими даними. В першу чергу до них необхідно віднести такі.

1. Встановлення таємних чи особистих ключів користувачів на об'єктах хмари з забезпеченням їх конфіденційності, цілісності, справжності, доступності, неспростовності та надійності.

2. Розповсюдження та встановлення чи отримання доступу до відкритих ключів користувачів з забезпеченням їх цілісності, справжності, доступності, неспростовності та надійності.

3. Оперативне виявлення фактів компрометації таємних та особистих ключів користувачів та виведення їх з дії з подальшим захищеним відновлення.

4. Дистанційне блокування чи знищення таємних та особистих ключів користувачами чи уповноваженими особами.

5. Захист таємних та особистих ключів користувачів від несанкціонованого доступу від внутрішніх та зовнішніх порушників, включаючи спеціалісті служб безпеки.

6. Створення, впровадження та застосування інфраструктур відкритого ключа (ІВК) в частині виготовлення та обслуговування сертифікатів відкритих ключів для надання електронних довірчих транскордонних послуг.

7. Забезпечення відносно особистих та відкритих ключів ІВК різних періодів чинності, наприклад чинність відкритих ключів повинна бути не менше періоду зберігання захищеної інформації архівів тощо.

Аналіз джерел [23] показав, що наведені вище проблемні питання відносяться і до захисту ключових даних безпосередньо хмарних обчислень та службових ключових даних посадових осіб.

2.3 Модель загроз відносно ключів та ключової інформації

На основі розроблених моделей хмарних обчислень, порушника та загроз ІТС хмарних обчислень(сервісів) з суттєвим урахуванням визначено, що найбільш проблемними з точки зору перекриття є загрози відносно ключів та ключової інформації.

На рис. 2.1 наведено визначений в процесі досліджень перелік загроз ключовим даним (ключам), які необхідно застосовувати для криптографічного захисту інформації в процесі хмарних обчислень.

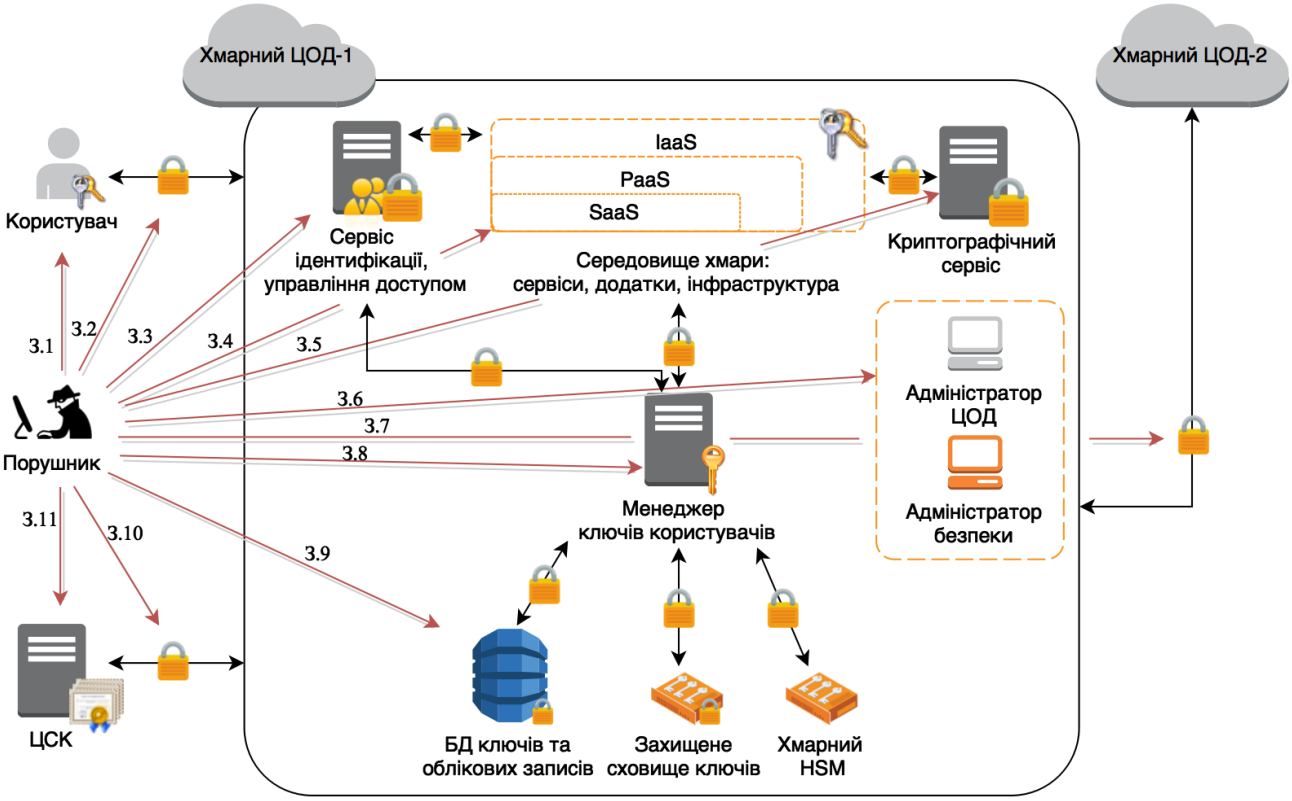

Рис. 2.1. Загрози ключам в середовищі хмари

Враховуючи в аналізі наведенні дані стандарту ISO \ IEC 11770-1, приймемо що в середовищі хмари відносно ключових даних можуть існувати та реалізовуватись зі сторони порушника такі загрози:

– компрометація ключів та ключової інформації;

– несанкціоноване знищення ключів та ключової інформації;

– перехоплення та запам’ятовування ключів та ключової інформації;

– нав’язування помилкових або хибних ключів та ключової інформації;

– нав’язування слабких ключів або напівслабких ключів;

– підміна ключів або ключової інформації;

– отримання несанкціонованого доступу до ключів чи ключової інформації;

– отримання можливості несанкціонованого використання ключів тощо.

Зважаючи на пропозиції та визнані критерії, що наведені в, приймемо в якості основного критерію ймовірність реалізації загрози. Також приймемо, що вона може оцінюватись як: низька, середня та висока.

На основі аналізу переліку загроз та моделі загроз ключовим даним можна зробити висновки про те, що порушник може з високою ймовірністю здійснювати:

– компрометацію, знищення, отримання несанкціонованого доступу чи несанкціоноване використання ключів відносно користувача;

– перехоплення, нав’язування та підміну ключів через канали зв’язку між користувачем та хмарою;

– отримання несанкціонованого доступу до ключів через сервіси ідентифікації, автентифікації, авторизації та керування правами доступу;

– отримання несанкціонованого доступу чи несанкціоноване використання ключів через хмарне середовище – сервісів додатків та, інфраструктуру;

– найбільшу небезпеку в середовищі хмарних обчислень для ключових даних користувача представляють адміністратори хмарних сервісів, які мають доступ до середовища в якому розгорнуто хмарні додатки користувача.

Для захисту від вказаних загроз на рівні користувача необхідно використовувати захищені з необхідним рівнем носії ключів.

На рівні каналів зв’язку між користувачем та хмарою необхідно застосовувати захищені канали зв’язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються.

На рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом необхідно реалізовувати та застосовувати надійні протоколи автентифікації з стійкими криптографічними алгоритмами, також методи багатофакторної автентифікації.

На рівні хмарного середовища, тобто сервісів додатків та інфраструктури, для здійснення криптографічних операцій необхідно використовувати захищені відповідним чином криптографічні модулі – HSM.

2.4 Вимоги до ключів та управління ключами

Безумовною вимогою для гарантування належного рівня безпеки в хмарі є застосування загальноприйнятих та міжнародних практик з використання та управління ключами. Відсутність контролю над хмарним середовищем, одночасна обробка декількох потоків інформації з різним рівнем безпеки, неоднорідність системи, а також її розгалуженість висуває нові вимоги до ключів та їх управління. Аналогічно, як і до існуючих ІТС , в середовищі хмарних обчислень висуваються вимоги з забезпечення конфіденційності, цілісності, доступності, спостережливості, неспростовності, крипто живучості та надійності ключів. Виконання цих вимог може бути досягнуто за рахунок технічних, організаційних та криптографічних методів захисту.

В середовищі хмарних обчислень існують значні проблеми в забезпеченні виконання цих вимог. Аналіз еталонної моделі хмари NIST [6] показав, що в процесі використання хмарних сервісів користувачам можуть надаватись три типи послуг - IaaS, PaaS та SaaS [10], а також необхідні засоби забезпечення безпеки та архітектурні рішення, що забезпечують реалізацію цих послуг.

Управління ресурсами, що пов'язані з хмарними сервісами є найважливішим аспектом хмарних обчислень та потребують забезпечення безпеки. При чо-

му, на рівні з організаційними та технічними механізмами та методами забезпечення безпеки, криптографічні механізми та методи є обов'язковими для забезпечення безпечного управління ресурсами хмари. Окрім необхідності забезпечення безпеки управління хмарою та ресурсами, розглядаючи згідно з моделлю NIST роль користувача в хмарі , необхідно відзначити, що криптографічні перетворення необхідні також для безпечної взаємодії користувача хмари з різними сервісами хмари, а також для зберігання даних, що були генеровані та/або оброблені цими сервісами.

Таким чином система управління ключами, що необхідна для підтримки криптографічних перетворень для зазначених вище функцій, може бути складною, зважаючи на відмінності відносно контролю над рівнями інфраструктури хмари, в яких знаходяться KMS та ресурси, що захищаються.

Наприклад, хоча споживач і має право власності на дані, що знаходяться та обробляються в хмарі, дані фізично зберігаються на ресурсах, що контролюються провайдером хмарних послуг, і в багатьох випадках KMS, яка необхідна для управління ключами для захисту даних також буде розгорнута на ресурсах постачальника хмарних послуг. Це породжує проблему безпеки і довіри хмарних користувачів до криптографічних операцій, що виконуються в хмарі.

Хоча є деякі розбіжності в послугах, що надаються хмарними провайдерами, але можна визначити набір функцій для основних моделей надання послуг (IaaS, PaaS та SaaS). Ґрунтуючись на цьому наборі функції визначається можливості, щодо реалізації функцій захисту та архітектурних рішень для досягнення цих можливостей безпеки. Слід зазначити, що не залежно від реалізованих функцій безпеки та архітектурного рішення, у випадках, коли криптографічні ключі зберігаються в хмарі є обмеження на ступінь забезпечення безпеки, на яку може розраховувати споживач хмари при будь-якій моделі надання послуг, в зв'язку з тим, що логічні і фізичні ресурси повністю під контролем хмарного провайдера.

Проведений аналіз показав, що наведені вище проблемні питання можуть бути вирішеними, якщо ключові дані та взагалі системи управління ключовими даними хмарних ІТС задовольняють наступним вимогам.

1. Сторони, які здійснюють основні функції з управління ключами повинні бути належним чином автентифіковані, а також повинен бути належним чином перевірений їх дозвіл на виконання функцій управління ключами для заданого ключа чи ключових даних.

2. Всі основні команди управління ключами і пов'язані з ними дані повинні бути надійно захищені від підміни: автентифікація джерела повинна здійснюватися до виконання команди.

3. Всі основні команди управління ключами і пов'язані з ними дані повинні бути захищені від неявних та несанкціонованих модифікацій: необхідно забезпечувати захист цілісності.

4. Секретні та особисті ключі повинні бути захищені від несанкціонованого доступу.

5. Всі ключі та метадані повинні бути захищені від підміни: автентифікація джерела повинна здійснюватися перед доступом до ключів та метаданих.

6. Всі ключі та метадані повинні бути захищені від неявних та несанкціонованих модифікацій: необхідно забезпечувати захист цілісності.

7. Криптографічні перетворення, що використовуються для захисту ключів, повинні мати стійкість не меншу ніж стійкість ключів, що захищаються.

Розглянемо детально управління ключами в різних модулях розгортання хмари згідно документу NIST IR 7956.

2.4.1 Управління ключами в моделі IaaS

Модель надання послуг IaaS передбачає, що користувачу надається доступ до хмарної інфраструктури, на базі якої він розгортає власну автоматизовану систему з обробки інформації. Інфраструктура користувача може бути розгорнута як безпосередньо на фізичних ресурсах хмари так і з використанням технології віртуалізації. При використанні технології віртуалізації образи віртуальних машин (ВМ), які надаються користувачу провайдером хмарних послуг повинні бути отримані з довірених джерел та захищені від модифікації. Після конфігурації та

завантаження образу ВМ, доступ до операцій з управління роботою образу ВМ (запуск, зупинка, перезавантаження, видалення) повинні виконуватися тільки авторизованими користувачами. Крім того взаємодія користувача з окремим образом ВМ повинна відбуватися використовуючи захищений канал зв'язку. Ці операції повинні виконуватися з використанням адміністративного інтерфейсу управління доступного користувачу. Для забезпечення безпеки виконання цих функцій повинні бути реалізовані наступні функції безпеки [16]:

– IaaS-SC1 – функції безпеки, що забезпечують автентичність образів ВМ, що надаються провайдером хмарних послуг користувачам;

– IaaS-SC2 – функції безпеки, що забезпечують доступ до інтерфейсу управління хмарою, автентифікованим користувачам;

– IaaS-SC3 – функції безпеки, що забезпечують захищений зв'язок для виконання адміністративних операцій з ВМ;

– IaaS-SC4 – функції безпеки, що забезпечують захищений зв'язок з додатками для користувачів, що запущені на ВМ;

– IaaS-SC5 – функції безпеки, що забезпечують зберігання конфігураційних даних додатку;

– IaaS-SC6 – функції безпеки, що забезпечують зберігання даних додатку в структурованій формі, з використанням системи управляння базою даних;

– IaaS-SC7 – функції безпеки, що забезпечують зберігання даних додатку в неструктурованій формі.

2.4.2 Управління ключами в моделі PaaS

Модель надання послуг PaaS, передбачає що користувачу надається обчислювальна платформа та необхідний набір інструментів для розробки та розгортання своїх власних додатків (зазвичай ОС з додатками). Користувач не має контролю над конфігурацією середовища ОС та додатків, але має можливість взаємодії з ними в процесі розробки та розгортання власних додатків. Використання

хмари користувачем передбачає необхідність забезпечення захищеного каналу передачі даних між користувачем та хмарою, захищеного зберігання даних користувача в середовищі хмари, захист розміщених додатків в хмарі. Дана конфігурація передбачає наявність в PaaS функцій безпеки хмарних сервісів (SC), які дозволяють виконувати ці операції є [14]:

– PaaS-SC1 – функції безпеки, що забезпечують встановлення безпечного каналу передачі з розгорнутими додатками та/або інструментами розробки;

– PaaS-SC2 – функції безпеки, що забезпечують безпечне зберігання службових даних додатків;

– PaaS-SC3 – функції безпеки, що забезпечують безпечне зберігання даних в структурованому вигляді використовуючи систему управління базами даних;

– PaaS-SC4 – функції безпеки, що забезпечують безпечне зберігання даних додатку в неструктурованому вигляді.

Реалізація функцій безпеки та управління ключами PaaS-SC1 - PaaS-SC4 є аналогічною до функцій IaaS-SC1 - IaaS-SC4.

2.4.3 Управління ключами в моделі SaaS

Модель надання послуг SaaS, передбачає що користувачу необхідні механізми для забезпечення конфіденційного зв’язку з додатками з використанням автентифікації, розмежування доступу, зберігання та обробка даних в зашифрованому вигляді. Таким чином типовий набір функцій безпеки SaaS [18]:

– SaaS-SC1 – функції безпеки, що забезпечують встановлення безпечного каналу;

– SaaS-SC2 – функції безпеки, що забезпечують зберігання даних додатку (структурованих та неструктурованих) в зашифрованому вигляді.

3 КЛАСИФІКАЦІЯ ТА АНАЛІЗ СИСТЕМ УПРАВЛІННЯ КЛЮЧАМИ ІТС ХМАРНИХ ОБЧИСЛЕНЬ

3.1 Аналіз моделей механізмів управління ключами

Забезпечення захисту від загроз для ключових даних вирішується за рахунок застосування механізмів управління ключами в хмарі.

Під криптографічним механізмом захисту інформації будемо розуміти – конкретний процес, метод, криптографічний протокол або криптографічний алгоритм, що використовується для реалізації певних послуг та/або функцій криптографічного захисту інформації та інформаційних ресурсів [17].

Управління ключами користувача в хмарі складається з процедур, що забезпечують:

– реєстрацію користувача в системі;

– генерацію, розподіл та введення ключів до засобів захисту;

– контроль над використанням ключів;

– зміна та знищення ключів;

– сертифікація ключів;

– архівування, зберігання та відновлення ключів.

Аналіз закордонних публікацій [9-13] та патентів в області хмарних обчислень, а також проведені дослідження показали, що для управління ключами зі сторони користувача можна застосовувати 7 основних механізмів (Keys management mechanism, КММ - ключовий механізм управління):

– механізм управління ключами з використанням сертифікатів відкритих ключів (КММ-1);

– механізм управління ключами на основі паролів (КММ-2);

– механізм управління ключами з використанням апаратного модулю захисту (Hardware secure module, HSM) хмарного ЦОД (КММ-3);

– механізм управління ключами з використанням HSM користувача (КММ-4);

– механізм управління ключами з використанням криптографічного сервісу та захищеного сховища ключів (КММ-5);

– механізм управління ключами з використанням хмарного HSM та криптографічного сервісу (КММ-6);

– механізм управління ключами з використанням розподілених апаратних засобів захисту ключів (КММ-7).

Проведемо їх аналіз та порівняння з метою обґрунтування та вибору найбільш перспективних для застосування користувачем хмарних сервісів.

В механізмах, що розглядаються, захищений канал між користувачем та хмарним ЦОД реалізується з використанням асиметричної пари ключів провайдера та, за наявності, користувача. Будемо також вважати, що він реалізується у відповідності до криптографічних протоколів згідно стандарту ISO/IEC 11770-3.

3.1.1 Механізм управління ключами з використанням сертифікатів відкритих ключів

Механізм управління ключами з використанням сертифікатів відкритих ключів передбачає взаємодію між трьома об’єктами – користувачем, хмарним ЦОД та ЦСК (рис. 3.1).

Застосування механізму потребує:

– узгодження загальносистемних параметрів: алгоритми ЕЦП, розподілу ключів, гешування, симетричного зашифрування та їх відкриті параметри;

– генерацію користувачем асиметричної пари ключів підпису та узгодження ключів – (d_{Ksign}, Q_{Ksign}), (d_{Kkep}, Q_{Kkep}) та отримання відповідних сертифікатів відкритих ключів $Certifiacate_{Ksign}$, $Certifiacate_{Kkep}$ в центрі сертифікації ключів (ЦСК);

– генерацію хмарним ЦОД асиметричної пари ключів підпису та узгодження ключів – $(d_{\Pi sign}, Q_{\Pi sign})$, $(d_{\Pi кер}, Q_{\Pi кер})$ та отримання відповідних сертифікатів відкритих ключів $Certifiacate_{\Pi sign}$, $Certifiacate_{\Pi кер}$ ЦСК.

Основні процедури з управління ключами здійснюється безпосередньо користувачем, окрім процедур пов'язаних з реєстрацією користувача в системі хмарного ЦОД. За ідентифікацію, автентифікацію та визначення прав доступу до ресурсів хмари відповідає окремий сервіс, що працює в середовищі хмарного провайдера.

При доступі до ресурсів хмари програмне забезпечення (ПЗ), що встановлене у користувача, звертається до носія ключової інформації (1, 2) з використанням паролю доступу користувача до ключа. Якщо результатом виконання операції є успішним, то ПЗ користувача ініціює захищену сесію для доступу до ресурсів хмари (3) з використанням захищеного каналу. Далі ПЗ хмари автентифікує користувача на основі сертифікату (4) та надає доступ до ресурсів хмари (5). Шифрування даних в БД та файловому сховищі в цьому механізмі не передбачене. Шифрування даних, що передаються до хмари, повинно бути організовано на стороні клієнта.

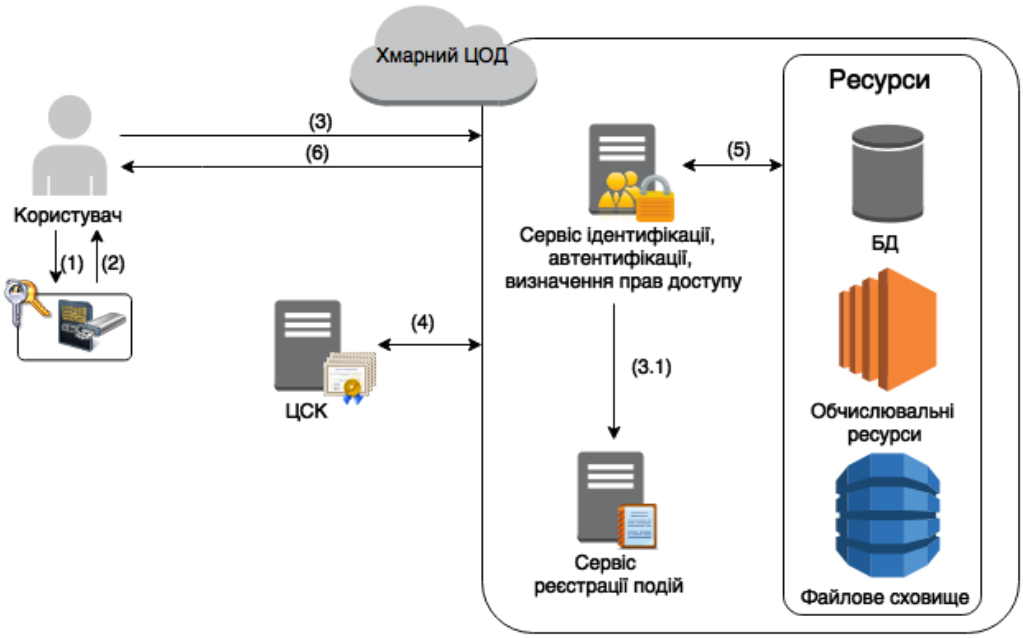

Рис. 3.1. Механізм управління ключами КММ-1

Основні переваги механізму КММ-1:

– механізм може бути реалізований з використанням існуючих програмно-апаратних рішень;

– ключ користувача зберігається на захищеному носії у користувача та не передається до хмари;

– провайдер хмарних послуг не потребує проходження сертифікації з захисту даних користувачів, в частині забезпечення конфіденційності та цілісності;

– автентифікація користувача здійснюється після встановлення захищеного каналу доступу до хмари.

Недоліки та особливості механізму КММ-1:

– відсутність можливості забезпечення конфіденційності даних на стороні провайдера хмарних послуг;

– як наслідок першого недоліку відсутність можливості спільного доступу користувачів до сервісів зберігання даних;

– необхідність отримання сертифікату відкритого ключа;

– необхідність розгортання у користувачів ПЗ з управління ключами.

3.1.2 Механізм управління ключами на основі паролів

Механізм управління ключами на основі паролів передбачає взаємодію між двома об’єктами – користувачем та хмарним ЦОД (рис. 3.2).

Застосування механізму потребує:

– генерацію хмарним ЦОД асиметричної пари узгодження ключів – $(d_{Пкер}, Q_{Пкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{Пкер}$ ЦСК для створення захищеного каналу для користувача;

Основні процедури з управління ключами здійснюється в середовищі хмари через відповідні інтерфейси, що надаються хмарним ЦОД.

В механізмі КММ-2 користувачу надається доступ до захищеної БД для зберігання ключових даних. Захищений канал до хмари реалізується з використанням тільки сертифіката відкритого ключа хмари.

При доступі до ресурсів хмари ПЗ, що встановлене у користувача, звертається до хмари (1) з використанням паролю доступу, використовуючи захищений канал. Сервіс ідентифікації та автентифікації, у випадку успішної автентифікації користувача, надає доступ до ключа користувача, що зберігається в БД, та повертає особистий ключ та/або секретний ключ користувача (3) отриманий з БД ключів.

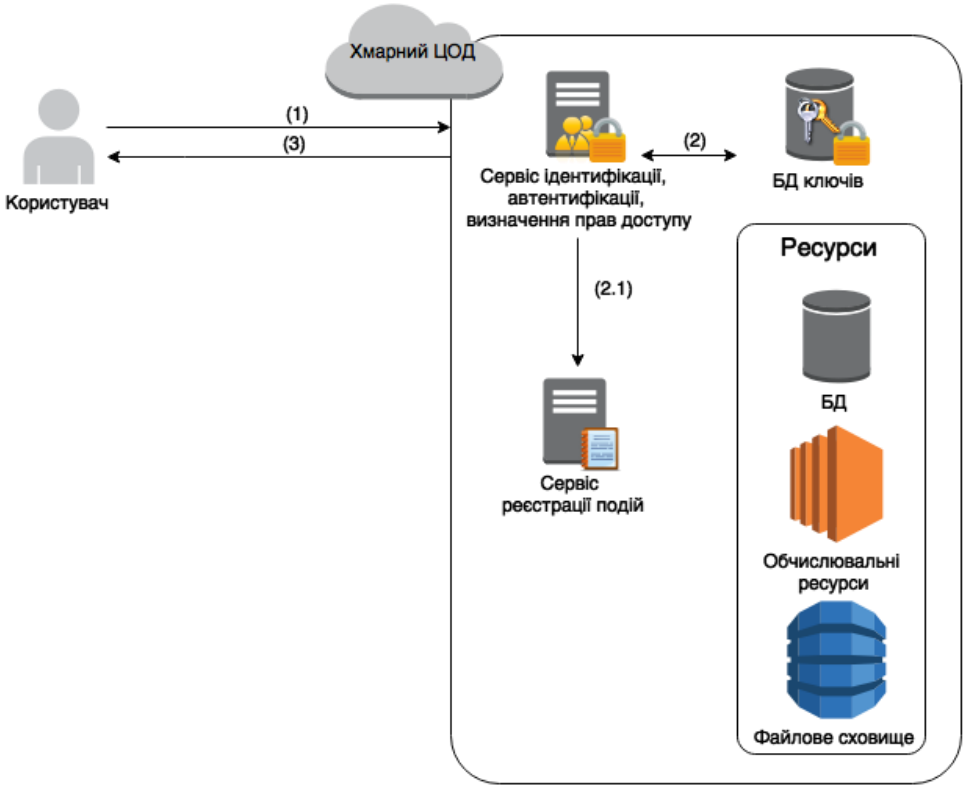

Рис. 3.2. Механізм управління ключами КММ-2

Основні переваги механізму КММ-2:

– реалізація механізму не потребує придбання додаткового обладнання та є одним з найбільш дешевих;

– широкі можливості щодо розширення та резервування;

– управління ключами відбувається безпосередньо в хмарі, що дозволяє реалізовувати спільний доступ до ресурсів за рахунок тільки хмарного забезпечення.

Недоліки та особливості механізму КММ-2:

– низький рівень забезпечення безпеки ключів та висока ймовірність їх компрометації;

– фактична відсутність контролю над ключовими даними зі сторони користувача;

– низька стійкість механізму автентифікації користувача в хмарі.

3.1.3 Механізм управління ключами з застосуванням апаратного модуля захисту хмарного провайдера

Механізм управління ключами з використанням модуля криптографічного захисту інформації (HSM) хмарного ЦОД передбачає взаємодію між двома об’єктами – користувачем та хмарним ЦОД (рис. 3.3).

Застосування механізму потребує:

– генерацію хмарним ЦОД асиметричної пари ключів узгодження ключів – $(d_{Пкер}, Q_{Пкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{Пкер}$ ЦСК для створення захищеного каналу для користувача;

– встановлення обладнання HSM хмарним ЦОД в окремому приміщенні;

– генерація виробником для HSM асиметричної пари узгодження ключів – $(d_{HSMкер}, Q_{HSMкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{HSMкер}$ ЦСК для створення захищеного каналу для користувача;

Основні процедури з управління ключами здійснюється в середовищі HSM через відповідні інтерфейси, що надаються хмарним ЦОД. Реєстрація користувача та доступ до інтерфейсів управління HSM надається хмарним ЦОД. Захищений канал до хмари реалізується з використанням тільки сертифіката відкритого ключа хмари.

При доступі до ресурсів хмари ПЗ, що встановлене у користувача, звертається до хмари (1) з використанням паролю доступу до хмарного HSM, використовуючи захищену сесію. При цьому ПЗ хмари передає запит до хмарного HSM, який у випадку успішної автентифікації користувача повертає ключові дані користувача до хмари (3). Далі ПЗ хмари, використовуючи отримані ключі, за попередньо захищеною сесією повертає користувачеві дані, що запитувались (4).

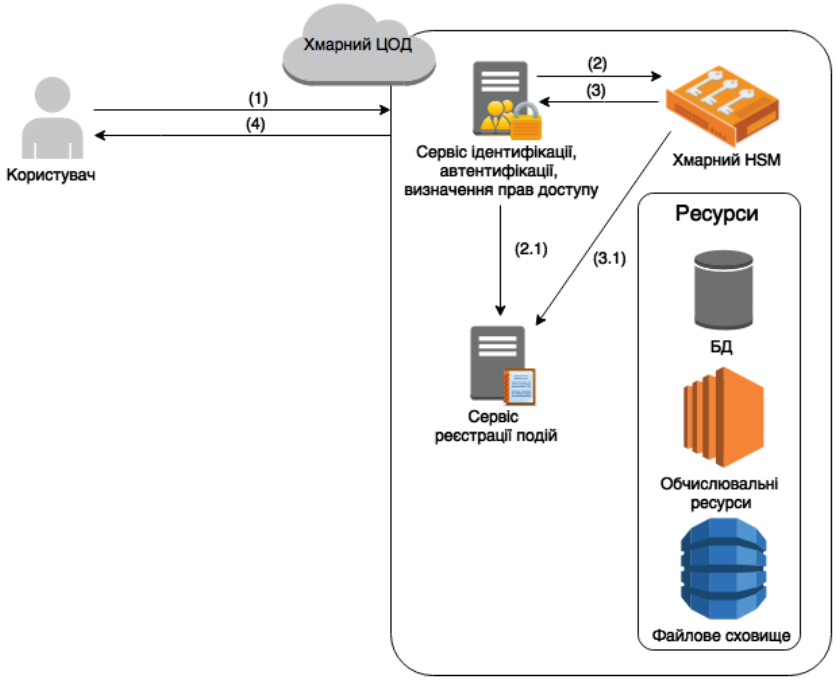

Рис. 3.3. Механізм управління ключами КММ-3

Основні переваги механізму КММ-3:

– механізм забезпечує конфіденційність зберігання та контроль доступу до ключових даних користувача за рахунок використання спеціалізованого обладнання HSM;

– високий рівень безпеки зберігання ключів, та низький рівень їх компрометації;

– можливість реалізації механізмів спільного доступу;

– гнучкі можливості, щодо масштабування кількості ключів – користувач платить лише за оренду HSM, що використовує.

Недоліки та особливості механізму КММ-3:

– необхідність закупки провайдером спеціалізованого обладнання, проходження процедури сертифікації, і, як наслідок, подорожчання рішення з управління ключами;

– відсутність контролю над HSM зі сторони користувача;

– обмеження на кількість ключових даних, що зберігаються в HSM, а також складність архівування ключів;

– відсутність механізму перевірки справжності встановленого ключа в HSM.

3.1.4 Механізм управління ключами з використанням апаратного модуля захисту користувача

Механізм управління ключами з використанням HSM, що знаходиться у користувача передбачає взаємодію між двома об’єктами – користувачем та хмарним ЦОД (рис. 3.4).

Застосування механізму потребує:

– генерацію хмарним ЦОД асиметричної пари ключів узгодження ключів – $(d_{Пкер}, Q_{Пкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{Пкер}$ ЦСК для створення захищеного каналу для користувача;

– встановлення обладнання HSM користувачем;

– генерація користувачем\виробником для HSM асиметричної пари узгодження ключів – $(d_{HSMкер}, Q_{HSMкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{HSMкер}$ ЦСК для створення захищеного каналу для користувача.

Основні процедури з управління ключами здійснюється безпосередньо користувачем через відповідні інтерфейси, що надаються хмарним HSM. Хмарний ЦОД виконує реєстрацію користувача. Захищений канал до хмари реалізується з використанням тільки сертифіката відкритого ключа хмари.

В механізмі КММ-4 користувачу надається в використання один з хмарних HSM, на якому користувач самостійно генерує ключові дані. Захищений канал до хмари реалізується з використанням тільки сертифіката відкритого ключа хмари. Захищений канал до HSM реалізується з використанням сертифіката відкритого ключа HSM модуля.

При доступі до ресурсів хмари ПЗ, що встановлене у користувача, звертається до HSM (1) з використанням паролю доступу до хмарного HSM, використовуючи захищену сесію. У разі успішної автентифікації, користувачу надається доступ до його ключових даних. ПЗ користувача звертається до сервісу ідентифікації та автентифікації (3) та у разі успіху отримує доступ до ресурсів хмари (4, 5). За наявності функцій з реєстрації подій в хмарному HSM, можлива реєстрація подій з управління ключами на віддаленому сервісу реєстрації подій хмари (1.1) або безпосередньо на стороні користувача.

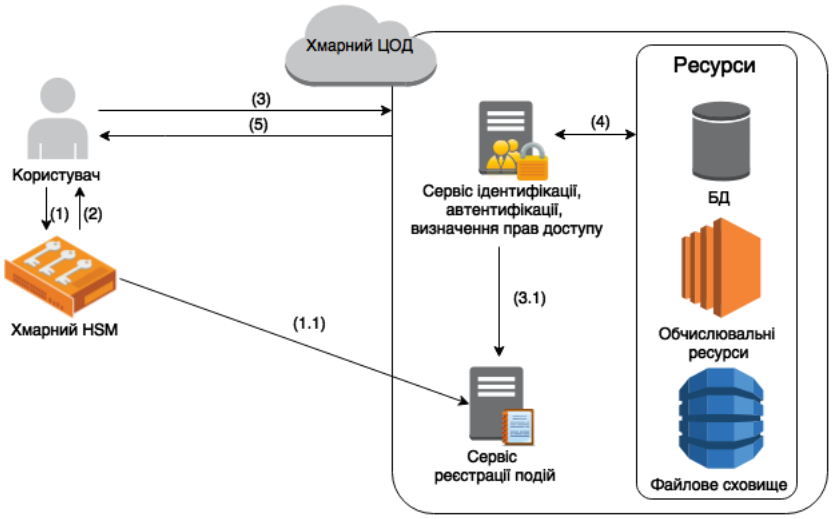

Рис. 3.4. Механізм управління ключами КММ-4

Основні переваги механізму КММ-4:

– на основі використання спеціалізованого обладнання HSM забезпечується конфіденційність зберігання та контроль доступу до ключових даних користувача;

– високий рівень безпеки зберігання ключів, та низький рівень їх компрометації;

– можливість повного контролю над HSM зі сторони користувача.

Недоліки та особливості механізму КММ-4:

– необхідність закупки користувачем спеціалізованого обладнання HSM, як наслідок здорожчання рішення з управління ключами;

– обмеження до створення спільного доступу до ресурсів HSM;

– низькі можливості щодо масштабування системи з управління ключами.

3.1.5 Механізм управління ключами з використанням криптографічного сервісу та захищеного сховища ключів

Механізм управління ключами з використанням криптографічного сервісу та сховища ключів, передбачає взаємодію між двома об'єктами – користувачем та хмарним ЦОД (рис. 3.5).

Застосування механізму потребує:

– генерацію хмарним ЦОД асиметричної пари ключів узгодження ключів – $(d_{Пкер}, Q_{Пкер})$ та отримання сертифікату відкритого ключа $Certifiacate_{Пкер}$ ЦСК для створення захищеного каналу для користувача;

– встановлення обладнання для захищеного зберігання ключів в хмарному ЦОД.

В цьому механізмі користувачеві для збереження ключової інформації в захищеному вигляді надається апаратний пристрій. Захищений канал до хмари реалізується з використанням тільки сертифіката відкритого ключа хмари. При чому, захищений пристрій зберігання ключів знаходиться у спеціалізованому приміщенні провайдера хмарних послуг, та забезпечує лише автентифікацію користувача при доступі до ключових даних.

При доступі до ресурсів хмари ПЗ, що встановлене у користувача, для отримання доступу до ресурсів звертається до хмари (1) з використанням паролю доступу до ключа. Запит до ресурсів користувача перенаправляється до менедже-

ру ключів користувачів (2), який отримує доступ до ключових даних користувача на захищеному пристрої (3). У разі успіху (4), ключові дані повертаються користувачу за захищеним каналом зв'язку (5, 6). Доступ до ресурсів хмари виконується за допомогою криптографічного сервісу та з використання ключових даних користувача. До складу механізму, також входить сервіс реєстрації подій, що забезпечує реєстрацію подій в середовищі хмари.

Управління ключами в розглянутому механізмі надається як сервіс хмари. До складу сервісів входять:

– ідентифікація (за попередньо встановленими факторами ідентифікації);
– автентифікація;
– керування правами доступу;
– управління ключами користувачів;
– захищене сховище ключів;
– реєстрація подій, що виникають під час роботи сервісу.

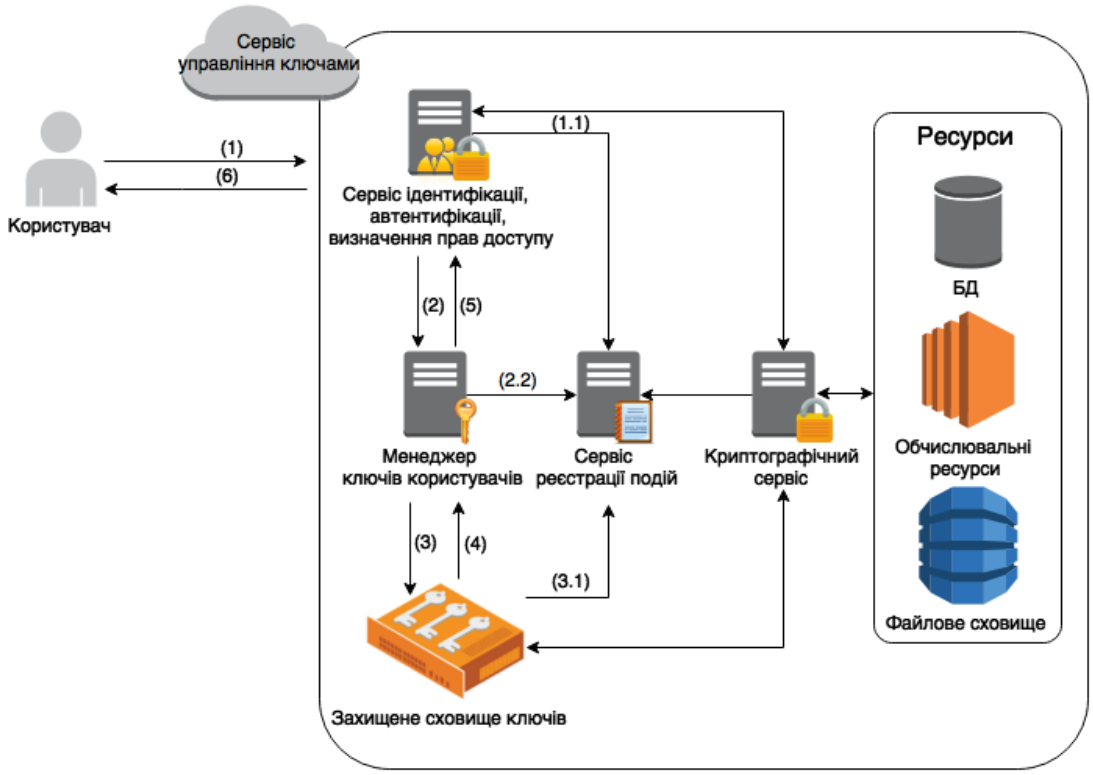

Рис. 3.5. Механізм управління ключами КММ-5

Основні переваги механізму КММ-5:

– за рахунок використання спеціалізованого обладнання для зберігання ключів забезпечується конфіденційність зберігання та контроль доступу до ключових даних користувача;

– високий рівень безпеки зберігання ключів, та низький рівень їх компрометації;

– можливість реалізації механізмів спільного доступу;

– можливість обробки даних в середовищі хмари;

– значні можливості з масштабування системи, зберігання ключів.

Недоліки та особливості механізму КММ-5:

– необхідність закупки провайдером хмарних послуг спеціалізованого обладнання для зберігання ключів, внаслідок чого зростає ціна рішення з управління ключами;

– відсутність контролю над обладнанням зі сторони користувача;

– обмеження на кількість ключових даних, що зберігаються.

3.1.6 Механізм управління ключами з використанням ІВК

Для усунення недоліків механізму КММ-1, запропоновано наступні зміни до механізму (рис. 3.6):

– сервіс ідентифікації, автентифікації та визначення прав доступу, що знаходиться в хмарі та працює на основі сертифікатів відкритих ключів користувача;

– хмарний HSM, що використовується для зберігання та управління ключами користувача, які необхідні для роботи додатків та інфраструктури користувача, що розгорнута в хмарі;

– сервіс реєстрації події – пасивний елемент захисту в механізмі управління ключами, що призначений для реалізації послуги спостережливості.

Механізм передбачає взаємодію між трьома об’єктами в системі – користувачем, хмарним ЦОД та ЦСК.

Застосування механізму потребує:

– узгодження загальносистемних параметрів: алгоритми ЕЦП, розподілу ключів, гешування, симетричного зашифрування та їх відкриті параметри;

– генерацію користувачем асиметричної пари ключів підпису та узгодження ключів – (d_{Ksign}, Q_{Ksign}), (d_{Kkep}, Q_{Kkep}), а також отримання відповідних сертифікатів відкритих ключів $Certifiacate_{Ksign}$, $Certifiacate_{Kkep}$ в центрі сертифікації ключів (ЦСК);

– генерацію хмарним ЦОД асиметричної пари ключів підпису та узгодження ключів – $(d_{Пsign}, Q_{Пsign})$, $(d_{Пkep}, Q_{Пkep})$ та отримання відповідних сертифікатів відкритих ключів $Certifiacate_{Пsign}$, $Certifiacate_{Пkep}$ ЦСК;

– встановлення спеціалізованого обладнання (HSM) хмарним ЦОД в окремому приміщенні;

– генерація виробником HSM асиметричної пари ключів підпису та узгодження ключів – $(d_{HSMsign}, Q_{HSMsign})$, (d_{HSMkep}, Q_{HSMkep}), а також отримання сертифікатів відкритих ключів $Certifiacate_{HSMsign}$, $Certifiacate_{HSMkep}$ від ЦСК;

Основні процедури з управління ключами здійснюється в середовищі HSM через відповідні інтерфейси, що надаються хмарним ЦОД. Реєстрація користувача та доступ до інтерфейсів управління HSM надається хмарним ЦОД. Захищений канал до хмари та автентифікація сторін реалізується з використанням сертифікатів $Certifiacate_{Ksign}$, $Certifiacate_{Kkep}$та $Certifiacate_{Пsign}$, $Certifiacate_{Пkep}$. Захищений канал до HSM реалізується з використанням сертифікатів $Certifiacate_{Ksign}$, $Certifiacate_{Kkep}$ та $Certifiacate_{HSMsign}$, $Certifiacate_{HSMkep}$.

При доступі до управління ключами в хмарі програмне забезпечення (ПЗ), встановлене у користувача, звертається до носія ключової інформації (1, 2) з використанням паролю доступу користувача до ключа. Якщо результатом виконання операції є успішним, то ПЗ користувача ініціює захищену сесію для проходження ідентифікації та автентифікації в хмарі (3). Далі ПЗ хмари автентифікує користувача на основі сертифікату (4) та надає доступ до хмарного HSM (5, 6, 7). Використання ключових даних, що знаходяться в хмарному HSM здійснюється

користувачем за рахунок звернень до криптографічного сервісу. Функції сервісів управління ключами та криптографічний сервіс, зазвичай, реалізуються в HSM.

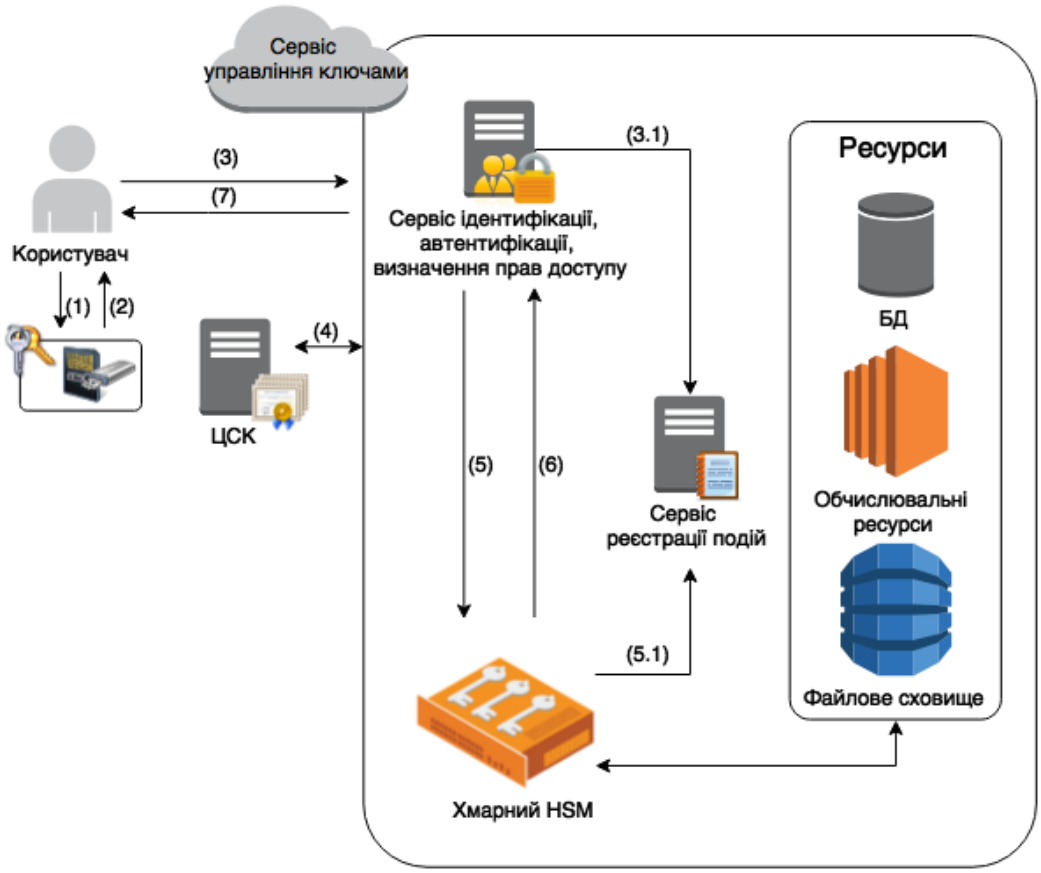

Рис. 3.6. Механізм управління ключами KMM-6

Основні переваги механізму KMM-6:

– механізм забезпечує конфіденційність зберігання та контроль доступу до ключових даних користувача за рахунок використання спеціалізованого обладнання HSM;

– забезпечення високого рівня безпеки сервісів ідентифікації, автентифікації та розмежування доступу до ключів та криптографічних сервісів за рахунок використання сертифікатів відкритих ключів;

– високий рівень безпеки зберігання ключів, та низький рівень загрози їх компрометації;

– можливість реалізації механізмів спільного доступу;

– гнучкі можливості, щодо масштабування кількості ключів – користувач платить лише за аренду HSM, що використовує.

Недоліки та особливості механізму КММ-6:

– необхідність закупки провайдером спеціалізованого обладнання, проходження процедури сертифікації, і як наслідок, здороження рішення з управління ключами;

– відсутність контролю над HSM зі сторони користувача;

– обмеження на кількість ключових даних, що зберігаються в HSM, а також складність архівування ключів.

3.1.7 Механізм управління ключами з використанням розподілених апаратних засобів захисту ключів

Розподілена архітектура хмари, що фізично складається з декількох ЦОД потребує створення можливості одночасного зберігання та використання ключів на всіх ЦОД. Основним недоліком попередньо розглянутих механізмів є відсутність розподілення ключових даних. Таким чином механізм КММ-7 (рис. 3.7) призначено для усунення цього недоліку. Це досягається шляхом нового елементу управління ключами – віртуальним хмарним HSM, який представляє собою сукупність об’єднаних в єдину мережу хмарних HSM з використанням захищеного каналу передачі та загального інтерфейсу доступу до них в середовищі хмари.

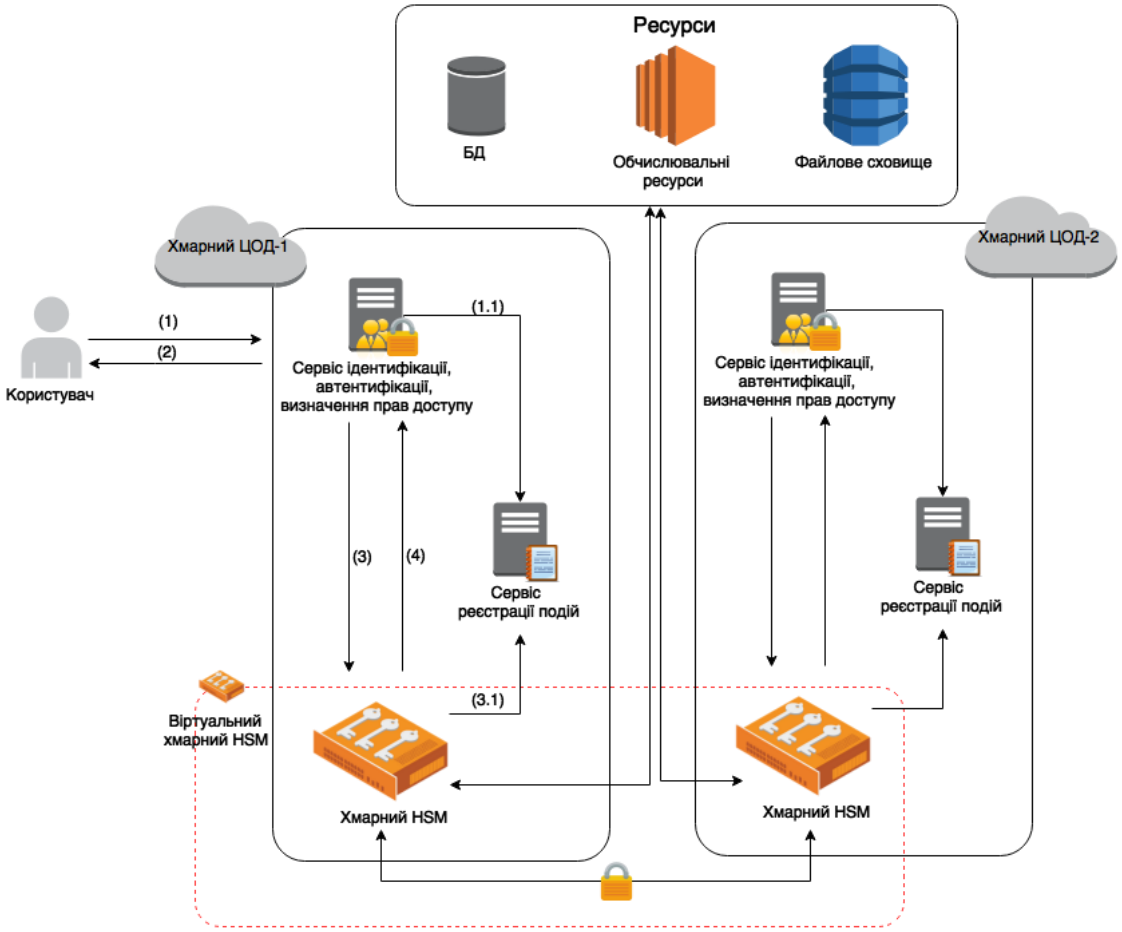

Рис. 3.7. Механізм управління ключами КММ-7

У випадках, коли необхідно забезпечити більш високий рівень надійності, до складу віртуального HSM може бути включено апаратний HSM, що розташовано у користувача.

Основні переваги механізму КММ-7 аналогічні до КММ-6, крім того:

– механізм забезпечує розподілення ключових даних між декількома відокремленими HSM;

– підвищення надійності та масштабованості за рахунок використання декількох HSM.

Окрім недоліків КММ-6, використання в механізмі КММ-7 декількох HSM збільшує загальну вартість рішення, а також існує загроза компрометації ключів користувача за рахунок реалізації атак на протокол архівування та передачі ключів між апаратними модулями.

3.1.8 Узагальнена модель механізму управління ключами користувача в хмарному середовищі

З урахуванням розглянутих механізмів та вимог стандартів до управління ключовими даними, пропонується узагальнена модель управління ключами (рис. 3.8), що включає наступні основні структурні елементи: сервіс ідентифікації, автентифікації та визначення прав доступу, менеджер ключів користувачів, захищене сховище ключів або хмарний HSM, криптографічний сервіс, а також допоміжні: адміністратор ЦОД, сервіс реєстрації подій, адміністратор безпеки, ЦСК.

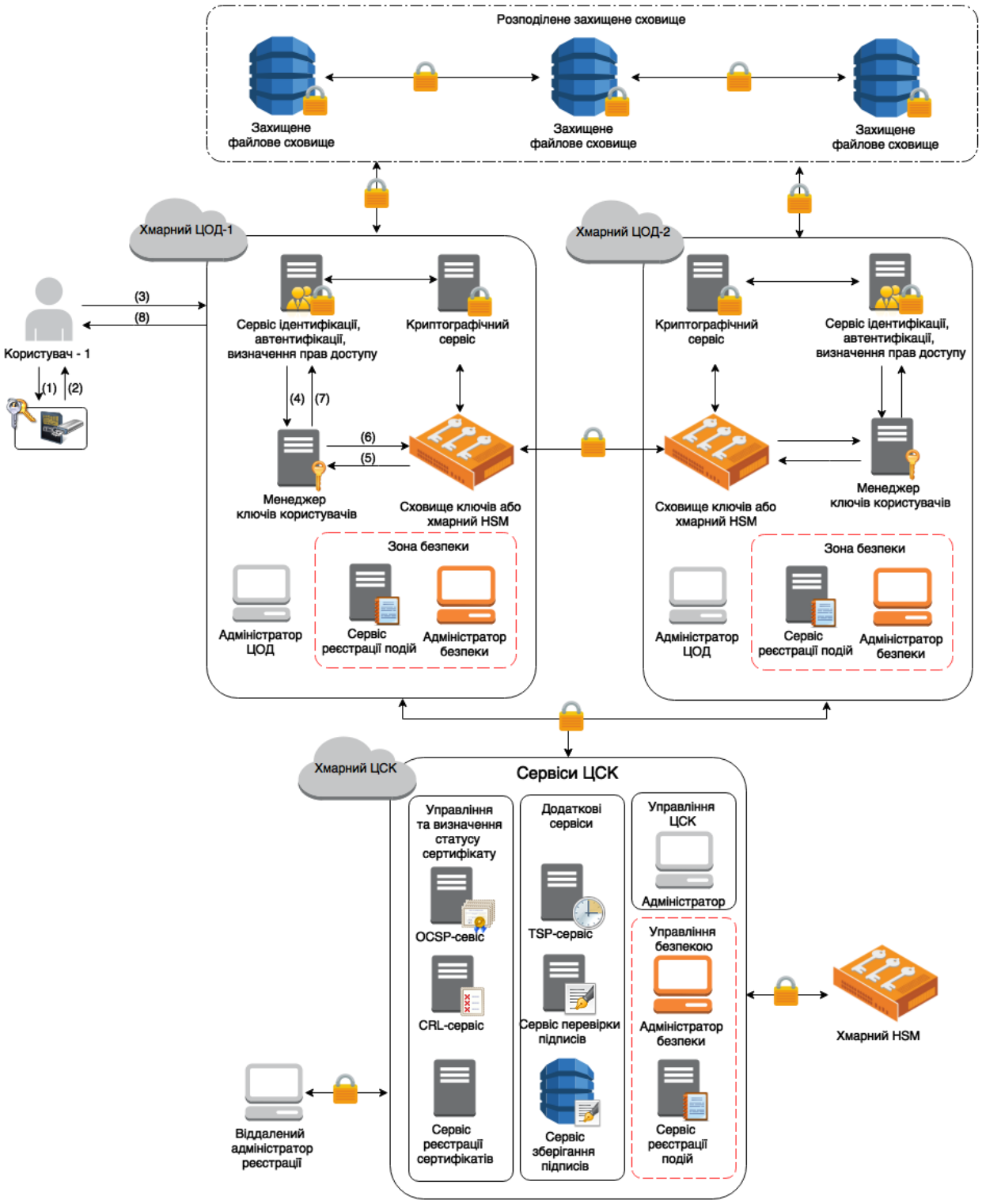

Рис. 3.8. Узагальнена модель механізму управління ключами

Елементи моделі механізму управління ключами, забезпечують:

– конфіденційність ключових даних користувача, за рахунок використання захищеного сховища ключів або хмарного HSM;

– ідентифікацію, автентифікацію та розмежування доступу до ключів та криптографічних сервісів за рахунок використання сертифікатів відкритих ключів та ЦСК;

– реалізацію спільного доступу до ключових даних користувача;

– гнучкі можливості, щодо масштабування кількості ключів – користувач платить лише за оренду захищеного сховища ключів чи HSM, що використовує.

3.2 Порівняння механізмів управління ключами

Для кожного з розглянутих механізмів можна виділити такі основні характеристики, як попередні налаштування, взаємодіючі сторони, елементи системи, сервіси, функції управління ключами, моделі розгортання хмари, моделі надання послуг та вразливі елементи.

За цими характеристиками, було виконано аналіз та порівняння розглянутих механізмів управління ключами. Результати порівняння наводиться табл.3.1.

Порівняння механізмів управління ключами Таблиця 3.1

Характеристики механізму	Механізм						
	1	2	3	4	5	6	7
1. Попередні налаштування							
$(d_{Ksign}, Q_{Ksign,} Certifiacate_{Ksign})$,	+	-	-	-	-	+	-
$(d_{Kkep}, Q_{Kkep}, Certifiacate_{Kkep})$	+	-	-	-	-	+	-
$(d_{Пsign}, Q_{Пsign,} Certifiacate_{Пsign})$,	+	-	-	-	-	+	-
$(d_{Пkep}, Q_{Пkep}, Certifiacate_{Пkep})$	+	+	+	+	+	+	+
$(d_{HSMkep}, Q_{HSMkep}, Certifiacate_{HSMkep})$	-	-	+	+	-	+	+
2. Взаємодіючі сторони							
Хмарний ЦОД	+	+	+	+	+	+	+
Користувач	+	+	+	+	+	+	+
ЦСК	+	-	-	-	-	+	-
3. Елементи системи							

Продовження таблиці 3.1

Характеристики механізму	Механізм						
	1	2	3	4	5	6	7
HSM	-	-	+	+	-	+	+
Захищене сховище ключів	-	-	-	-	+	-	-
4. Сервіси							
Реєстрації події	+\-	+\-	+\-	+\-	+	+	+
Криптографічний сервіс	-	-	-	-	+	+	+
Сервіс ідентифікації та автентифікації	+	+	+	+	+	+	+
Сервіс управління ключами	-	-	-	-	+	+	+
5. Функції управління ключами в хмарі							
реєстрація користувача в системі	+	+	+	+	+	+	+
генерація, розподіл та введення ключів	-	+	+	-	+	+	+
контроль над використанням ключів	+	-	-	+	-	+\-	+\-
зміна та знищення ключів	+	-	-	+	-	+\-	+\-
архівування, зберігання та відновлення кл.	+	-	-	+	-	+\-	+\-
6. Модель розгортання хмари							
Приватна	+	+	+	+	+	+	+
Публічна	+	-	+	+	+\-	+	+
Гібридна	+	-	+	+	+\-	+	+
7. Модель надання послуг хмари							
IaaS	+\-	+	+	+\-	+	+	+
PaaS	+\-	+	+	+\-	+	+	+
SaaS	+	+	+	+	+	+	+
8. Вразливі елементи							
Носій особистого ключа	+	-	-	-	-	+	+
БД з ключами	-	+	-	-	-	-	-
HSM	-	-	+	+	-	+	+
Захищене сховище	-	-	-	-	+	+	+
Криптографічний сервіс	-	-	-	-	+	+	+

Продовження таблиці 3.1

Характеристики механізму	Механізм						
	1	2	3	4	5	6	7
Сервіс управління	-	-	-	-	+	+	+
Сервіс ідентифікації та автентифікації	+	+	+	-	+	+	+

Аналіз таблиці 3.1 дозволив визначити перелік вимог та обмежень до механізмів з управління ключами. Головними вимогами при синтезі механізму управління ключами в хмарі є реалізація функції з управління ключами безпосередньо в хмарі для забезпечення інтероперабельності з високим рівнем захисту. Високий ступінь захисту в хмарі може бути реалізований за рахунок використання спеціалізованого обладнання для зберігання або управління ключами. У випадках коли відсутня необхідність безпосередньо в хмарі реалізовувати обробку даних, найбільш оптимальною є механізм КММ-1.

На основі запропонованої моделі механізму управління ключами, а також результатів порівняння можна вирішити задачу вибору механізму управління ключами на основі висунутих вимог в процесі розробки до системи управління ключами користувача в хмарі.

3.3 Механізм генерації та встановлення єдиної ключової пари між захищеними апаратними носіями без передачі особистого ключа

3.3.1 Вихідні дані, постановка задачі досліджень та критерії оцінки

Нехай в хмарі встановлено N апаратних модулів захисту (HSM) з'єднаних між собою. Кожний з модулів повинен володіти ключовою парою для підпису (k_{sign}, Q_{sign}) та ключовою парою для направленого шифрування (k_{env}, Q_{env}). Відкритим ключам повинні відповідати сертифікати – $Cert_{sign}, Cert_{env}$. Ключі підпису призначені для автентифікації модулів захисту, забезпечення цілісності даних, а також підпису відкритих ключів користувача для відправки в ЦСК. Ключі шифру-

вання призначені для забезпечення захищеного каналу передачі інформації між модулями.

Таким чином необхідно забезпечити генерацію та встановлення ключової пари в системі з N –вузлами при використанні якої забезпечується встановлення ключів по відкритому каналу зв'язку.

На основі аналізу та використання [13, 16] з урахуванням постановки досліджень запропоновано механізм та на його основі криптографічний протокол. Сутність кроків захищеного криптографічного протоколу у наступному.

Механізм реалізується засобом виконання захищеного криптографічного протоколу та складається з наступних кроків:

1. Налаштування засобом обрання та встановлення загальносистемних параметрів у всіх N –модуля захисту.

2. Вироблення спільної системної ключової пари (k_{HSM}, Q_{HSM}).

3. Підпис отриманого відкритого ключа Q_{HSM}, ключем підпису модуля захисту та відправлення на сертифікацію до ЦСК.

Для різних криптографічних примітивів протокол вироблення спільної ключової пари відрізняється.

Протокол може бути реалізований при застосування криптографічних перетворень в групі точок еліптичних кривих, а також за необхідності в скінченному полі.

Для оцінки криптографічних протоколів проведемо з застосування критеріїв, що запропоновані в [17]:

– наявність (реалізація) послуги автентифікації об'єкта (процесу), суб'єкта;
– наявність (реалізація) послуги автентифікації ключа (ключів);
– вид автентифікації об'єктів (процесів) і суб'єктів;
– вид автентифікації ключів;
– наявність послуги встановлення ключа (ключів);
– наявність послуги підтвердження ключа (ключів);
– перелік послуг з управління ключами;

– захищеність від загроз типу «маскарад»;

– захищеність від загроз типу «модифікація»;

– криптографічна живучість у встановлених ключів;

– гарантії забезпечення послуг, конфіденційність, цілісність, доступність, справжність (автентичність) і неспростовність щодо інформації автентифікації та ключів;

– число обмінів при здійсненні криптографічного протоколу;

– складність виконання криптоаналізу відносно ключів та інформації, що захищається;

– складність обчислень при здійсненні криптографічного протоколу;

– наявність та вимоги до третьої довірчої сторони тощо.

3.3.2 Побудування та аналіз протоколу встановлення ключа в групі точок еліптичної кривої

Налаштування та генерація ключа

Загальносистемні параметри: еліптична крива - E, базова точка еліптичної кривої - G, порядок базової точки - n, розмір поля, який визначає базове кінцеве поле $-F(p)$. Алгоритм передбачає встановлення спільної пари ключів між двома вузлами за один прохід. Якщо $N > 2$ спочатку спільна пара генерується для двох вузлів, після чого спільна пара генерується між вузлами де вже встановлено ключ та новим вузлом.

Протокол встановлення ключа

1. Кожний з вузлів системи генерує особистий ключ - випадкове число $d_i\,(1 \le d_i < n)$, та обчислює відкритий ключ Q_i:

$$Q_i = d_i G (\mathrm{mod}\, p) \qquad (3.1)$$

2. Відкритий ключ кожного з вузлів Q_i підписується за допомогою особистого ключа HSM та передається іншим вузлам.

3. Два вузли обчислюють загальний секрет S за протоколом Діффі-Гелмана:

$$S_1 = d_1 Q_2 (\mathrm{mod}\, p) \quad (3.2)$$

$$S_2 = d_2 Q_1 (\mathrm{mod}\, p) \quad (3.3)$$

$$S = d_1 d_2 G (\mathrm{mod}\, p) \quad (3.4)$$

4. Отриманий спільний секрет S перетворюється за допомогою функції вироблення ключа H, в псевдовипадкове число $d\,(1 \le d < n)$. Відкритий ключ Q, обчислюється згідно виразу 3.1.

5. Якщо в системі $N > 2$ відкритий ключ Q підписується особистим ключем HSM та передається наступному вузлу для формування спільної пари.

6. Отримане значення ключової пари (d, Q) на останньому кроці – є спільною ключовою парою для всіх вузлів. Відкритий ключ Q відправляється на сертифікацію.

3.3.3 Протокол вироблення спільної пари в полях Галуа

У випадках, коли застосування математики ЕК або спарювання точок ЕК не можливе, а вимоги стійкості до атак типу «повне розкриття» дозволяють використовувати криптографічні алгоритми з субекспоненційною стійкістю протокол може бути побудовано з використанням математичних примітивів в полях Галуа наступним чином.

Налаштування та генерація ключа

Загальносистемні параметри: просте поле Галуа $F(p)$, просте сильне число - P, первісний елемент поля – Θ. Алгоритм передбачає встановлення спільної пари ключів між двома вузлами за один прохід. Якщо $N > 2$ спочатку спільна пара генерується для двох вузлів, після чого спільна пара генерується між вузлами де вже встановлено ключ та новим вузлом.

Протокол встановлення ключа

1. Кожний з вузлів системи генерує випадкове число $x_i\,(1 < x_i < p-1)$, та обчислює Y_i:

$$Y_i = \Theta^{x_i} (\mathrm{mod}\, p) \quad (3.5)$$

2. Відкритий ключ кожного з вузлів Y_i підписується за допомогою особистого ключа HSM та передається іншим вузлам.

3. Два вузли обчислюють загальний секрет S за протоколом Діффі-Гелмана:

$$S_1 = Y_2^{x_1} (\mathrm{mod}\, p) \tag{3.6}$$

$$S_2 = Y_1^{x_2} (\mathrm{mod}\, p) \tag{3.7}$$

$$S = \Theta^{x_1 x_2} (\mathrm{mod}\, p) \tag{3.8}$$

4. Отриманий спільний секрет S перетворюється за допомогою функції вироблення ключа H, в псевдовипадкове число $k\,(1 < k < p-1)$. Відкритий ключ Q, обчислюється згідно виразу 3.5.

5. Якщо в системі $N > 2$ відкритий ключ Q підписується особистим ключем HSM та передається наступному вузлу для формування спільної пари.

6. Отримане значення ключової пари (k, Q) на останньому кроці – є спільною ключовою парою для всіх вузлів. Відкритий ключ Q відправляється на сертифікацію.

3.3.4 Аналіз властивостей на основі прийнятих критеріїв

1. Забезпечується взаємна автентифікація суб'єктів, оскільки вони володіють тимчасовими особистими та відкритими ключами, справжність яких підтверджена підписом захищеного модуля.

2. Автентифікація ключів не передбачена протоколом, але може бути виконана за рахунок взаємодії сторін після встановлення спільної ключової пари – для ключів підпису шляхом підпису деякої інформації кожним з вузлів та перевірки її іншими вузлами, для ключів шифрування шляхом направленого шифрування випадкового значення на кожний з вузлів з подальшим розшифруванням іншими вузлами.

3. Новизна ключів забезпечується за рахунок використання генератора випадкових чисел на етапі формування допоміжних ключів, що використовуються при встановленні спільного ключа.

4. Захист від атак типу «маскарад» та «модифікація» для відкритих ключів допоміжних ключів забезпечується за рахунок використання ЕЦП, з використанням особистого ключа модуля безпеки та посиленого сертифіката відкритого ключа модуля безпеки.

5. При виробленні розділюваного спільного ключа передачі особистого ключа не відбувається. Але протокол, що розглядається, не забезпечує криптоживучості у випадках компрометація одного із тимчасових ключів, однозначно приводить до компрометації розділюваного секретного ключа і виробленого з його використанням спільного ключа.

6. Гарантії з забезпечення послуг, конфіденційність, цілісність, доступність, справжність (автентичність) і неспростовність щодо інформації автентифікації та ключів забезпечуються захищеним модулем та третьою довіреною стороною, що управляє сертифікатами відкритих ключів.

7. Число обмінів при виконанні протоколу залежить від кількості вузлів та використаного математичного апарату. Для протоколів, що використовують математику в полі та математику в групі точок еліптичної кривої:

$$\sum_{n=1}^{N} n = \frac{k(\mathrm{k}+1)}{2} \tag{3.9}$$

8. Складність криптоаналізу полягає в складності вирішення відповідної криптографічної задачі на якій базується математичний апарат асиметричного перетворення, що застосовується в протоколі Діффі-Гелмана, а також підбору особистого ключа, що засновано на недосконалості функції перетворення спільного секрету в особистий ключ.

9. Виконання передобчислень не можлива.

10. Всі суб’єкти впливають на розділюваний таємний ключ за рахунок використання відкритих ключів.

11. При виробленні розділюваного спільного ключа передачі особистого ключа не відбувається.

12. При використанні протоколу необхідно звертатися до третьої довірчої сторони для виготовлення та підтримання життєвого циклу сертифікатів HSM, а також сертифікатів відкритих ключів сформованих в результаті застосування протоколу. При застосуванні протоколу на спарюванні точок ЕК необхідною умовою є уповноважений на генерацію особистих ключів.

13. При компрометації спільного особистого ключа в одному з модулів HSM, особистий ключ в інших модулях також є скомпрометований.

14. При додаванні або зміні вузлів в системі потребує повторної генерації спільного ключа.

ВИСНОВКИ

Теоретичні та практичні дослідження кінця 20-го та початку 21-го століть дозволили визначити один із основних напрямків удосконалення та розвитку ІТС, що пов'язаний з хмарними обчисленнями. До технологій хмарних обчислень проявляє велику зацікавленість як великий так і малий бізнес, який намагається за рахунок використання хмарних сервісів оптимізувати свої витрати в процесі різних видів діяльності. Особливу зацікавленість до хмарним обчислень проявляють науковці та технологи, які дозволяють суттєво скоротити час виконання досліджень та впровадження їх результатів на практиці. Але досвід застосування хмарних обчислень виявив ряд проблемних питань відносно надання користувачам послуг з безпеки. При чому, дуже важливою проблемою в забезпеченні управління ключовими даними для клієнтів, в першу чергу в частині її розгортання та функціонування в інфраструктурах які контролюються та управляються в основному постачальниками хмарних послуг. За таких умов користувачі хмарних сервісів в явному виді потребують додаткових гарантій зі сторони постачальника хмарних послуг відносно управління ключовими, надання їм електронних довірчих послуг конфіденційності, цілісності, справжності, доступності, криптографічної живучості, неспростовності тощо в управління ключами.

В цьому напрямі за результатами проведених досліджень наступні теоретичні результати:

– проаналізована модель загроз ключовим даним користувачів хмарних сервісів, що дозволяє класифікувати загрози за їх метою та об’єктами, на які вони направлені, оцінити можливості порушника, з метою вибору найбільш ефективних методів, механізмів та засобів захисту.

– представлено модель загроз хмарних обчислень, яка дозволяє оцінити ефективність засобів захисту та мінімізувати втрати за рахунок оцінки ризиків та використання методів оцінки ефективності.