Василь ОЛЕКСЮК
Олег СПІРІН

ОСНОВИ ХМАРНИХ ТЕХНОЛОГІЙ

Василь Олексюк, Олег Спірін

ОСНОВИ ХМАРНИХ ТЕХНОЛОГІЙ

Київ – 2023

УДК 004.7,
О-53

Затверджено вченою радою Інституту цифровізації НАПН України, протокол № 15 від 30 листопада 2023 р.

Рецензенти: Марія Шишкіна – доктор педагогічних наук, старший науковий співробітник, завідувач відділу хмаро орієнтованих систем інформатизації освіти Інституту цифровізації освіти НАПН України

Любомир Кривокульський – завідувач центру інформатики, ІКТ та дистанційної освіти Тернопільського обласного комунального інституту післядипломної педагогічної освіти

О-53

Олексюк В., Спірін О. Основи хмарних технологій: Навчальний посібник. Київ: Інститут цифровізації освіти НАПН України, 2023. 188 с.

ISBN
DOI :

У навчально-методичному посібнику розкрито основні поняття технологій хмарних обчислень. Розглянуто процес розгортання хмаро орієнтованого середовища закладів середньої та вищої освіти з використанням сервісів Google Workspace. У посібнику значну увагу приділено вивченню можливостей платформ, які дають змогу розгорнути академічну хмару згідно моделі «інфраструктура як сервіс». З метою опанування практичними навиками управління хмарними сервісами розроблено цикл лабораторних робіт. Для студентів педагогічних спеціальності «014.09. Середня освіта (Інформатика)».

ISBN
DOI :

1. СУТНІСТЬ ПОНЯТТЯ «ХМАРНІ ТЕХНОЛОГІЇ»

Понад два десятиліття епоха інформатизації суспільства створює суттєвий вплив на освітню галузь. Популярним трендом сьогодення стають так звані хмарні технології, які створюють можливості роботи з інформаційними ресурсами, незважаючи на апаратно-програмне забезпечення клієнта, а також його географічне положення. Незважаючи на територіальну віддаленість, хмарні засоби навчання можуть стати складником навчальних середовищ закладів середньої та вищої освіти.

Під хмарними технологіями (cloud computing) розуміють модель забезпечення повсюдного і зручного мережного доступу на вимогу до певної сукупності налаштовуваних обчислювальних ресурсів. Хмарними також вважають програмно-апаратне забезпечення, яке є доступним користувачеві через інтернет або локальну мережу у вигляді сервісу, що дозволяє використовувати зручний інтерфейс доступу до певних обчислювальних ресурсів, програм та даних. «Хмара» – не лише популярний сучасний термін, який застосовують для опису інтернет-технологій віддаленого збереження даних. Його зазвичай описують за допомогою понять: програмне забезпечення, сервіс, сервер. Однак головним критерієм визначення хмарної технології є можливість роботи з її ресурсами, незважаючи на апаратно-програмне забезпечення клієнта, а також його географічне положення. Наприклад, студент, перебуваючи в університеті, дома, у бібліотеці або кафе, для отримання відомостей про модульний контроль може використати ноутбук, планшетний комп'ютер або смартфон.

Технології хмарних обчислень надають новий підхід, який дозволяє знизити складність ІТ-систем, завдяки застосуванню широкого ряду ефективних, доступних на вимогу технологій, що функціонують у межах віртуальної інфраструктури. Заклади освіти у всьому світі використовують хмарні послуги одного і того ж типу від кількох постачальників (сховища даних, електронна пошта, хостинг, системи управління навчанням). Це дає можливість створити динамічне середовище, де постачальники хмарних обчислень конкурують між собою. Конкуренція може бути пов'язана з ціною, вмістом або іншими функціями, які дозволяють налаштовувати взаємодію здобувачів освіти. Комерційний вендор або наднаціональна корпорація, завдяки своїй спеціалізації, створюють кращий продукт за менших витрат. Отож, нині акценти закладу освіти зміщуються на забезпечення належної роботи всіх складників ІТ-інфраструктури та інтеграцію існуючих «локальних» ресурсів з новими хмарними сервісами, які можуть надати конкурентну перевагу у провадженні освітнього процесу. Як наслідок ІТ-інфраструктура ЗВО трансформується відповідно до сервіс-орієнтованої архітектури (рис. 1).

Постачальник послуг може бути в хмарним провайдером, або бути внутрішньою службою. Аналогічно отримувач послуг може бути службою в хмарі, що функціонує відповідно до будь-якої моделі, або внутрішньою службою IT-інфраструктури закладу освіти.

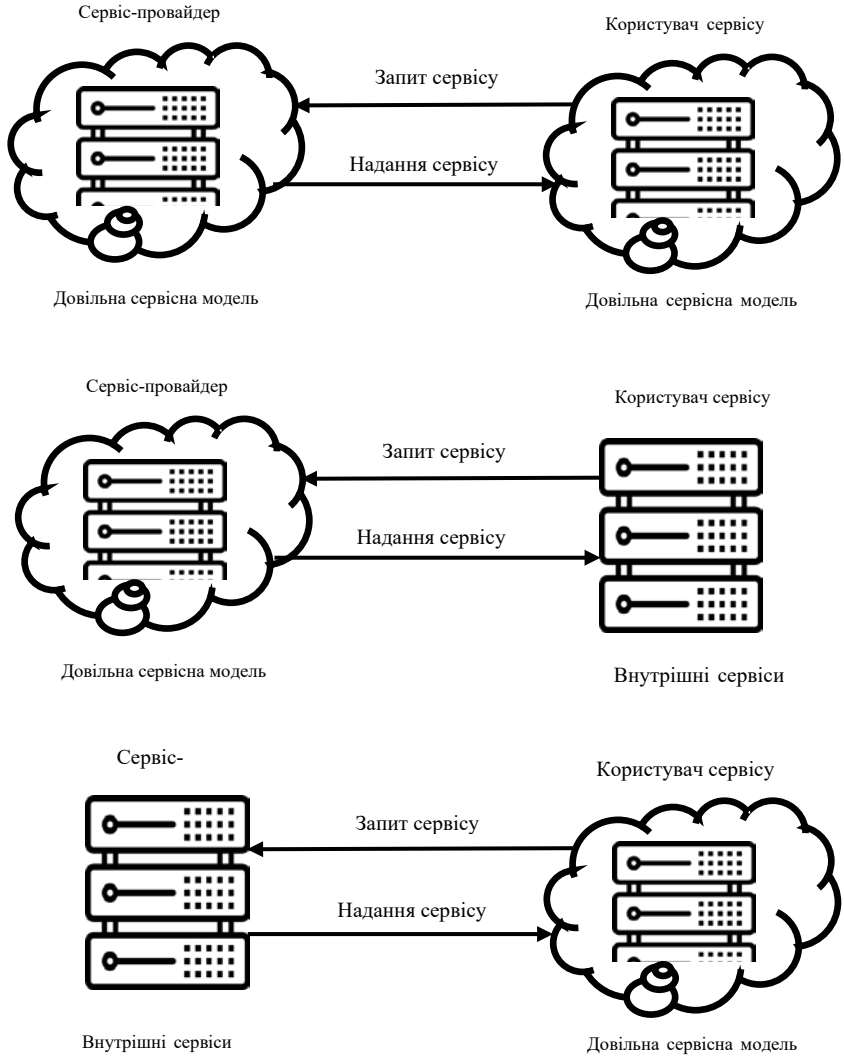

Рис. 1.1. Сервіс-орієнтована архітектура з різними комбінаціями хмарних обчислень

Технологічною основою роботи з хмарними технологіями є веб-технологія, завдяки якій сервери та клієнти взаємодіють за протоколом обміну гіпертексту. Проте, на відміну від традиційного розуміння всесвітньої павутини, як сукупності веб-сторінок, хмарні технології передбачають використання програмного забезпечення як сервісу (SaaS – Software as a Service). SaaS є моделлю розгортання та застосування програмного забезпечення, згідно якої для повнофункціонального його використання клієнту необхідний лише веб-браузер.

Крім SaaS існують такі моделі застосування хмарних технологій:

- IaaS (Infrastructure-as-a-Service) – модель, яка передбачає розгортання у «хмарі» інформаційної інфраструктури організації. Основою для реалізації моделі є технології віртуалізації. Фізично вся інфраструктура корпоративної мережі може бути реалізована на одному або кількох серверах датацентру провайдера.
- PaaS (Platform-as-a-Service) – модель, яка передбачає розгортання певної програмної платформи, яку можуть використовувати не лише користувачі сервісу, а й програмісти та розробники. Тобто така платформа орієнтована на застосування у «хмарному» середовищі мов програмування, наборів бібліотек тощо.
- DaaS (Desktop-as-a-Service) – модель застосування «хмарного» робочого стола. Тобто на зміну «традиційним» засобам та протоколам віддаленого доступу (VPN, RDP, VNC, SSH) в епоху хмарних технологій приходить лише веб-браузер.

Розгортання хмарних технологій можливе відповідно до таких сервісних моделей:

- власна корпоративна хмара, що передбачає побудову, підтримання функціонування і забезпечення розвитку власного центру опрацювання даних (вимагає існування у навчальному закладі потужного ІКТ-підрозділу);
- загальнодоступна хмара, що передбачає використання засобів і сервісів «хмарного» провайдера;
- гібридна (комбінована) модель реалізації ІКТ-сервісів, тобто одночасне використання корпоративних та загальнодоступних хмар.

Хмарні технології є розвитком концепцій ІТ-аутсорсингу. Замість придбання, встановлення та управління власними серверами, можлива оренда сервера у хмарного провайдера (Microsoft, Amazon, Google або іншої компанії). Як наслідок користувач управляє своїми орендованими серверами, одержуючи доступ до них через мережу інтернет, оплачуючи при цьому тільки фактичне використання їх обчислювальних потужностей, які потрібні для обробки і зберігання даних. Хмари, які пропонують провайдери, можуть складатися з тисяч серверів, розміщених в датацентрах, що забезпечують ро-

боту десятків тисяч додатків, які одночасно використовують мільйони користувачів. Неодмінною умовою ефективного управління такою великомасштабної інфраструктурою є максимально повна автоматизація. У зв'язку з цим, для забезпечення надання послуг різним користувачам (операторам, сервіспровайдерам, ІТ-адміністраторам, користувачам додатків) хмарна інфраструктура повинна передбачати можливість делегування повноважень.

У закладах освіти хмарні технології розгортають у формі хмароорієнтованих середовищ навчання, під якими розуміють систему цифрових засобів (апаратних, комунікаційних, віртуалізованих), що функціонують відповідно до принципів хмарних обчислень та забезпечують повсюдний доступ здобувачів до інформаційних, обчислювальних ресурсів, задля розвитку інформатичних компетентностей та досягнення цілей навчання та виховання.

Інформаційно-освітнє середовище загальноосвітнього навчального закладу доцільно проєктувати на основі загальнодоступних хмарних сервісів. У вищих навчальних закладах, що мають розвинену інформаційну інфраструктуру, можна розгортати гібридні хмари, поєднуючи загальнодоступні та корпоративні платформи.

2. ОГЛЯД ХМАРНОГО ПАКЕТУ GOOGLE WORKSPACE ДЛЯ ОСВІТИ

Google Workspace для освіти – це пакет хмарних сервісів для забезпечення комунікації, спільної діяльності в роботі сучасної освітньої установи. Google Workspace є ефективним сервісом розгортання інформаційно-освітнього середовища загальноосвітнього навчального закладу. Незважаючи на те, що будь-яка людина може зареєструвати обліковий запис Google, саме Google Workspace надає хмарні сервіси корпоративного рівня. Цей пакет сервісів, розроблений компанією Google Inc, може бути розгорнутим у освітніх закладах різного рівня та акредитації (школах, коледжах, університетах тощо).

Google Workspace для освіти містить хмарні сервіси, які знаходяться на серверах компанії Google Inc. Сервіси Google направду є хмарними: для їх використання не потрібно встановлювати комп'ютері додаткового програмного забезпечення, досить лише веб-браузера. На корпоративному рівні немає потреби у встановленні серверів організації. Всі вони у пакеті Google Workspace для освіти надаються безкоштовно.

Використання сервісів Google Workspace у інформаційно-освітньому середовищі навчального закладу надає переваги:

- надійності – надані сервіси традиційно мають високу функціональність та захист даних;
- індивідуального доступу до ресурсів та сервісів;
- можливості формування груп та підрозділів користувачів;
- фільтрування небажаного контенту з боку системи, адміністратора а також самого користувача;
- централізованого адміністрування завдяки розширеному набору методів та засобів;
- значного обсягу дискового (хмарного) простору, який надається користувачеві;
- україномовного інтерфейсу;
- доступності з мобільних пристроїв, зокрема якнайкраща підтримка пристроїв, які працюють під управлінням Google Android та Microsoft Windows.
- інтеграції з іншими програмними засобами освітнього закладу.

Будь-яка людина, реєструючи собі власний обліковий запис Google, отримує доступ до інструментів і сервісів, за допомогою яких можна надсилати повідомлення електронною поштою у сервісі Gmail, обмінюватися повідомленнями та відео-дзвінками з використанням сервісу Meet; публікувати відео на сервісі YouTube, і розміщувати свої статті та інші матеріали у блозі, планувати спільну роботу з колегами; створювати документи, редагувати їх

разом зі співавторами тощо. Доцільність розгортання і використання окремого пакету Google Workspace у навчальних закладах визначається перевагами корпоративних облікових записів, основними з яких є:

- централізоване створення облікових записів учнів різного віку (за згодою батьків);
- інтегрованість сервісів у межах одного або кількох інтернет-доменів;
- розвинена підтримка спільної роботи, зокрема завдяки використанню облікових записів груп користувачів та спільних адресних книг;
- значна кількість налаштувань, що дає можливість пристосувати хмарні сервіси до потреб навчального закладу;
- можливість збереження практично необмеженого обсягу даних;
- відсутність реклами на веб-сторінках;
- обмеження доступу до небажаного контенту;
- можливість отримання звітів та аналітичних відомостей про використання сервісів.

Загалом в учня чи вчителя може бути кілька облікових записів, наприклад: один − для особистого спілкування, інший − для професійної або навчальної діяльності. При цьому принциповою вимогою є недопущення передавання даних облікового запису іншим особам.

У хмарному пакеті Google Workspace можна виділити три рівні сервісів:

- основні сервіси, надійну роботу яких гарантує компанія Google Inc. (електронна пошта Gmail, хмарне сховище Google Диск, сервіси для планування подій Google Calendar, відеоконференцзв'язку Google Meet та створення сайтів Google Sites);
- понад 50 сервісів, розроблених компанією Google, які також можна безкоштовно використовуватися у пакеті. До них належать сервіс відеохостингу YouTube, сервіси Блоггер, Google Analytics та інші.
- продукти, розроблені партнерськими компаніями. Їх також можна долучити до сервісів домену, проте їх надійне та безперебійне функціонування компанія Google не гарантує.

Пакет Google Workspace для освіти дає можливості створити власну хмару, наповнення, конфігурування якої здійснюватимуть певне коло фахівців. Доступ до ресурсів хмари також буде надано відповідно до потреб закладу. Наприклад, керівництво школи може отримати повний доступ до управлінських даних, вчителі − до планів уроків та інструментів спільної навчальної діяльності, учні – доступ до перегляду певних навчальних матеріалів, та ресурсів із завданнями. Оскільки Google Workspace для освіти є захищеним пакетом хмарних сервісів, вимога компанії Google щодо вікового обмеження користувачів молодших 13 років не є обов'язковою. Школа, за згодою батьків, може надати облікові записи учням початкових класів.

3. РОЗГОРТАННЯ GOOGLE WORKSPACE ДЛЯ ОСВІТИ

Для розгортання хмарних сервісів у загальноосвітній школі потрібна співпраця адміністрації та вчителів-предметників (передовсім інформатики, а також англійської мови). Бажаною є допомога з боку фахівців у галузі інформаційних технологій, зокрема системних адміністраторів.

З власного досвіду зауважимо, що для розгортання освітньо-інформаційного середовища на основі пакету Google Workspace варто:

- визначити основні освітні проблеми, які слід вирішувати засобами хмарних сервісів;
- проаналізувати, здійснити добір, а також оцінювання хмарних технологій стосовно застосування у навчальному процесі;
- спроектувати структуру самого середовища, змоделювати діяльність його учасників;
- зареєструвати обліковий запис навчального закладу та отримати академічну ліцензію для нього;
- сконфігурувати хмарні сервіси відповідно до поставлених завдань;
- виконати аналіз, узагальнення результатів проектування, прийняття рішення щодо використання.

Як відомо для функціонування хмарних сервісів у пакеті Google Workspace потрібна наявність інтернет-домену. Найбільш простим способом отримання домену є його придбання у інтернет-провайдера. Також піддомени другого та нижчих рівнів можна отримати у реєстратора для власного делегування.

Після реєстрації свого доменного імені потрібно перейти на сторінку Google Workspace для освіти:

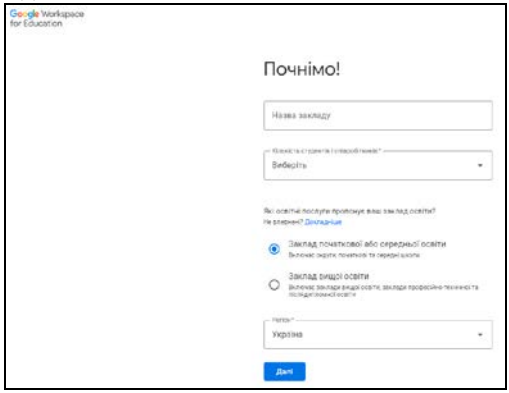

Рис. 3.1 Сторінка реєстрації навчального закладу

Потрібно ввести інформацію про себе, вибрати тип навчального закладу, вказати номер телефону. На наступному кроці слід вказати зареєстроване у провайдера доменне ім'я. Згодом слід увести пароль адміністратора, який буде використовуватися для управління сервісами Google Workspace.

Після додавання домену слід підтвердити право власності на нього (рис. 3.1).

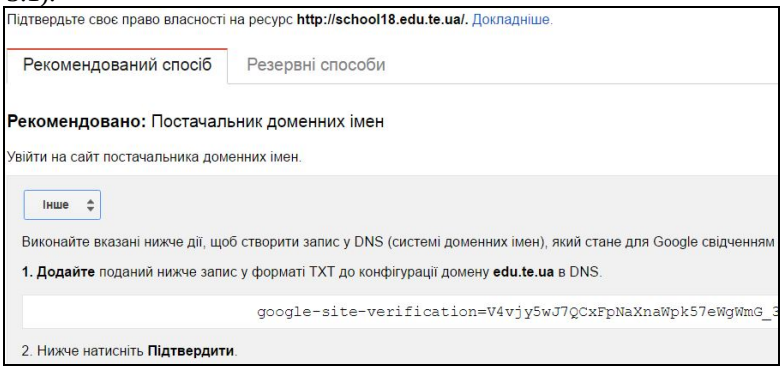

Рис. 3.2 Підтвердження власності домену

Це можна зробити одним із способів:

- внести зміни до сайту навчального закладу, якщо він знаходиться у тому ж домені, редагуючи його веб-сторінки або модифікуючи відповідний запис сервісу Google Analytics (резервний спосіб);
- створити запропонований запис у службі DNS домену (рекомендований спосіб).

Рекомендований спосіб стане у нагоді навчальним закладам, які не мають власного сайту.

За замовчуванням домени, додані у такий спосіб, є доменами Google Workspace для бізнесу. Для їх використання на безкоштовній основі слід перевести їх у режим Google Workspace для освіти, тобто отримати академічну ліцензію.

Для цього у консолі адміністратора слід перейти у розділ «Платежі», в якому обрати академічну підписку. Альтернативним способом є перехід на сторінку запиту академічної підписки за прямим посиланням: https://support.google.com/a/contact/nonprofit

Варто підготувати та ввести опис англійською мовою освітнього закладу та цілей використання хмарних сервісів Google Workspace у ньому. Для підтвердження статусу освітнього закладу бажаною є наявність сайту школи. Проте можливим є отримання ліцензії й без такого сайту. Його подальша розробка можлива на хмарному сервісі Google Sites. Варто своєчасно відповіда-

ти на листи від компанії Google. У таких повідомленнях фахівці можуть просити надати додаткові відомості про школу (скан-копії ліцензій та атестатів випускників).

Наявність академічної підписки можна перевірити у згаданому розділі «платежі» консолі адміністратора (рис. 3.4).

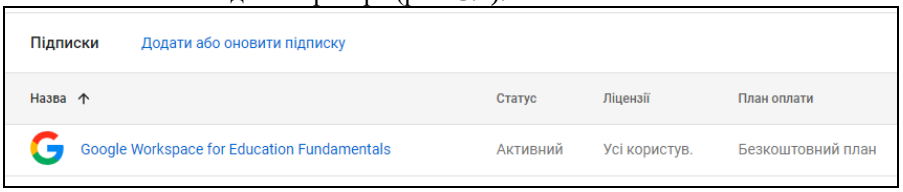

Рис. 3.3 Сторінка, що відображає тип підписки Google Workspace

Хмарна платформа Google Workspace має редакції для бізнесу та освіти. Вона розробляється та удосконалюється впродовж більш як 10 років. Нині є кілька тарифних планів (підписок) цього пакету, зокрема:

- Google Workspace for Education Fundamentals – пропонується базовий, безкоштовний набір хмарних сервісів, зокрема засоби для співпраці, планування, комунікації; підписка є безкоштовною;
- Google Workspace for Education Standard – забезпечується розширений функціонал сервісів, зокрема експорт журналів Classroom та Gmail для аналізу засобами BigQuery. Підписка дає змогу підвищити безпеку хмари завдяки центру виявлення і усунення загроз, також через отримання детальних аналітичних даних щодо використання сервісів;
- Teaching and Learning – надаються удосконалені сервіси для відеозв'язку (окремі кімнати для групової роботи, відеозустрічі зі збільшеною кількістю учасників (до 250 осіб), та глядачів (до 10000 осіб);
- Google Workspace for Education Plus – пропонується найбільш удосконалені інструменти для забезпечення освітнього процесу, зокрема синхронізація сервісу Classroom з будь-якою системою управління навчанням, засоби виявлення плагіату, контроль оригінальності робіт, збільшені кількості учасників відеозустрічей.

Слід зауважити, що у випадку придбання або отримання додаткових ліцензій (відмінних від Google Workspace for Education Fundamentals) вони можуть бути призначені як окремим, так і усім користувачам освітнього закладу.

На підтвердження безпечності хмарних сервісів компанія Google Inc. надає навчальному закладу сертифікат ISO/IEC 27001.

Основним інструментом управління сервісами Google Workspace є консоль адміністратора (рис. 3.4)

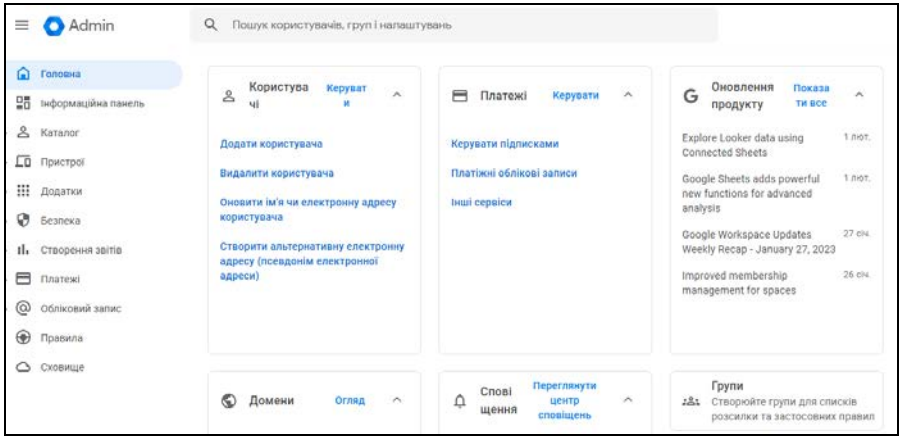

Рис. 3.4. Інтерфейс адміністратора G-Suite

Одним з першочергових завдань щодо управління платформою є створення облікових записів користувачів. Google Workspace підтримує такі способи створення облікових записів:

- введення параметрів у ручному режимі;
- імпорт кількох облікових записів із наперед підготовленої електронної таблиці, зазвичай у форматі csv;
- синхронізація облікових записів користувачів із локальною базою інформаційної інфраструктури (необхідним є увімкнення API-функцій).

Створюючи обліковий запис користувача, можна ввести пароль або згенерувати тимчасовий пароль, який користувач змінить при першому вході.

Усі облікові записи користувачів та груп Google Workspace можна структурувати, розподіливши їх у окремих підрозділах (організаціях та підорганізаціях). Наприклад, у хмарній інфраструктурі школи можна створити такі організації: «адміністрація», «учителі», «учні». У підрозділі «учні» доцільно створити підорганізації, які б відповідали класам (рис. 3.5).

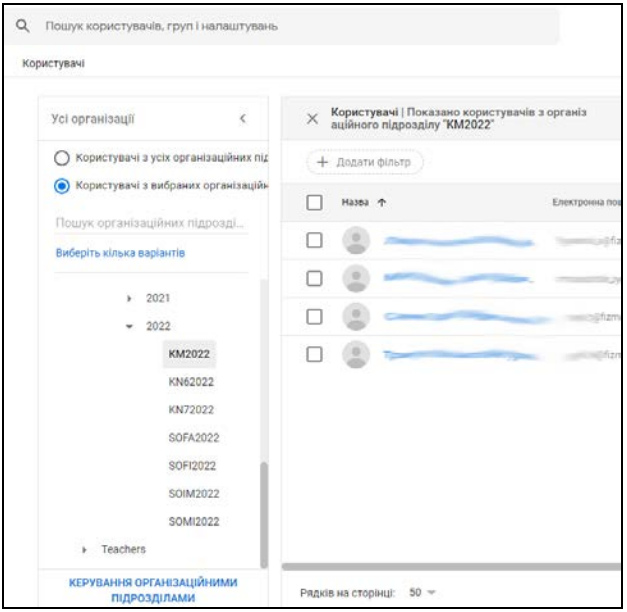

Рис. 3.5 Розподіл облікових записів у підрозділах

Описана структура підрозділів освітнього закладу потрібна для управління як доменом, так і окремими сервісами. Створюючи зазначену структуру, необхідно продумати у чому полягатиме відмінність у повноваженнях різних користувачів, що визначатиме їх розподіл у певних підрозділах. У подальшому це спростить виконання завдань адміністрування домену. Наприклад, можна надати всім учителям права адміністраторів домену або заборонити учням початкової школи користуватися сервісом миттєвих повідомлень Google Meet.

Питання реалізації інфраструктури підрозділів є принциповим. Її проектуванню слід приділити значну увагу, щоб уникнути непорозумінь та зайвої технічної роботи у майбутньому. Доцільно спочатку реєструвати кореневий домен закладу вищої освіти. У ЗВО, що налічує тисячі здобувачів, доцільним вважаємо реєстрацію у системі DNS дочірніх доменів для окремих підрозділів. Кожен з цих доменів можна додати у сервісі Google Admin як додатковий. У подальшому слід делегувати адміністративні повноваження відповідальним працівникам цих підрозділів.

До прикладу, ми мали ситуацію, коли запис Google Workspace для факультету був зареєстрований значно раніше, ніж університетський обліковий запис. На факультеті практикується надання облікових записів усім студентам та працівникам. Натомість, зазвичай, університет надає доступ лише для

працівників. У результаті спостерігали проблеми синхронізації каталогу контактів, надання доступу до документів та електронних курсів, використання раніше зареєстрованих електронних адрес в наукометричних базах даних та сервісах. Розв'язання проблеми вбачається в міграції дочірнього домену в окремий підрозділ з попередньою зміною політики ЗВО щодо використання хмарного пакету Google Workspace. На жаль, станом на 2022 рік повнофункціональна міграція доступна лише для платних підписок Education Standard та Education Plus.

На сторінці облікових записів також можна додавати або редагувати їх атрибути. Для цього вгорі сторінки слід перейти за гіперпосиланням *Керувати атрибутами користувачів* та вказати необхідність створення їх окремої категорії. У вікні, що завантажиться вказують (рис. 3.6):

- назву та опис категорії;
- назву та тип даних, які міститиме атрибут;
- можливість присвоєння йому кількох значень;
- конфіденційність (загальнодоступність) даних атрибута.

Крім облікових записів користувачів, у домені можна створювати групи користувачів, які дають можливість більш ефективно організовувати спільну роботу. Наприклад, лист, надісланий на електронну скриньку групи, буде доставлений усім її учасникам, з папкою чи документом до яких надано доступ групі зможуть працювати усі її учасники, доступ до події календаря також отримають усі учасники запрошеної групи.

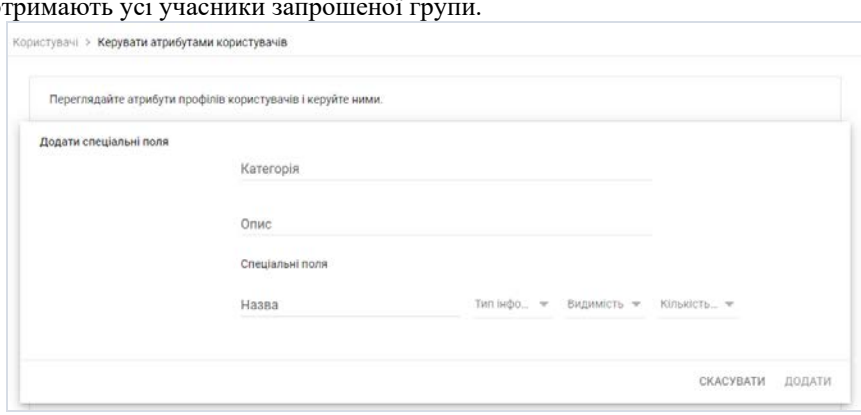

Рис. 3.6. Додавання атрибутів облікових записів користувачів Google Workspace

Між групами і організаціями домену в Google Workspace існує принципова відмінність. Користувач може входити лише в одну організацію, проте його обліковий запис може належати до кількох груп. Так обліковий запис учня, створений у підрозділі «7-А», може бути учасником не лише групи,

створеної для відповідного класу (7-А), а й належать групам «robotics», «football», «art», які включають учасників відповідних гуртків (робототехніка, футбол, мистецтво).

Для створення облікових записів груп необхідно (рис. 3.7):

- перейти у відповідний розділ консолі адміністрування
- обрати послугу «Додати групу»;
- ввести назву та електронну адресу групи;
- визначити рівень доступу до групи.

Електронна адреса групи буде використовуватися для надання доступу до ресурсів та організації діяльності її учасників.

Google Workspace надає такі рівні доступу до груп (рис. 3.7):

- загальнодоступний (Для всіх), який передбачає, що будь-хто з домену може приєднатися до групи, надсилати повідомлення її учасникам тощо;
- командний, який дозволяє запрошувати нових учасників лише менеджерам (власникам) групи, а надсилати повідомлення, переглядати учасників – будь-кому з домену (у цьому режимі можна дозволити усім користувачам за межами домену надсилати повідомлення в групу);
- «лише сповіщення» – надсилати повідомлення можуть лише менеджери групи, а приєднуватися до неї зможе будь-хто з домену;
- обмежений – передбачає, що лише менеджери можуть запрошувати нових учасників. Ніхто, крім учасників не може надсилати повідомлення групі;
- персоналізований набір параметрів.

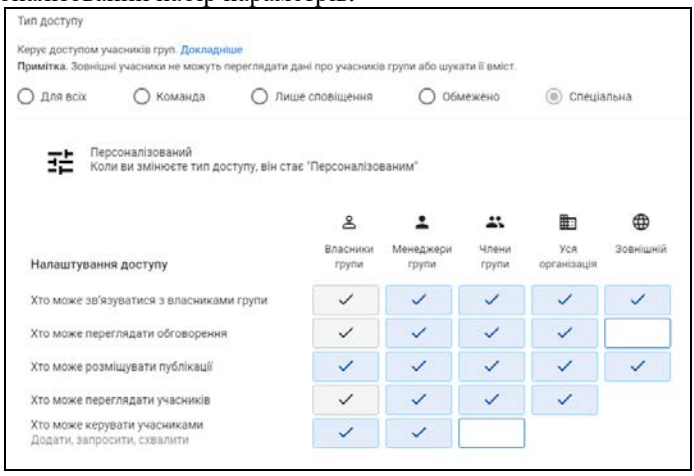

Рис. 3.7. Додавання нової групи Google Workspace

Після створення групи буде запропоновано додати в неї учасників. Можна ввести їх адреси електронної пошти через кому або додати в групу всіх користувачів своєї організації. Існує можливість додавання до групи всіх користувачів домену. Члени групи можуть належати до однієї з таких категорій:

- власник – має повний перелік повноважень. Зокрема, власник може видалити групу, призначити іншого члена групи її власником, змінити налаштування будь-якого учасника групи.
- менеджер – менеджери можуть практично всі ті ж дії, що й власники, за вийнятком видалення групи, зміни власника або його ролі.
- Учасник групи. Має базові дозволи. Залежно від налаштувань облікового запису закладу освіти та групи вони мають повноваження читати обговорення та брати участь у них, а також переглядати інформацію про учасників. Власники та менеджери груп можуть змінювати повноваження учасників.

Для використання користувачами груп Google Workspace адміністратору слід увімкнути сервіс «Групи для бізнесу». Увійшовши до цього сервісу за покликанням https://groups.google.com, користувач може створити групу та вказати налаштування групи (рис. 3.8).

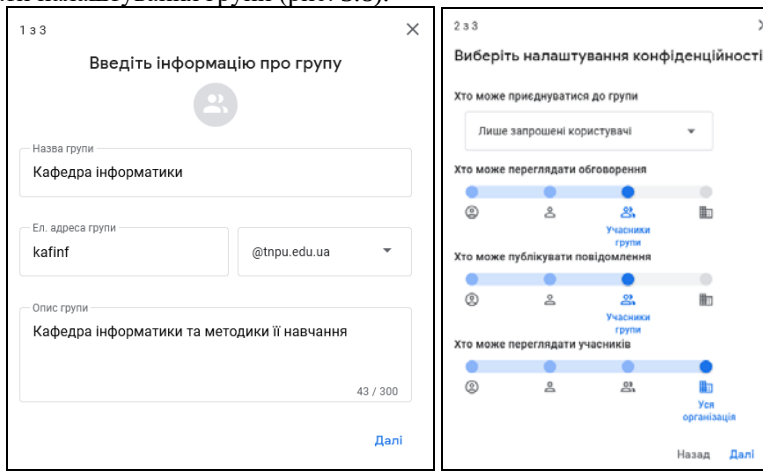

Рис. 3.8. Створення групи у сервісі Google Groups

Як було зазначено вище, сервіси, доступні в домені Google Workspace, умовно поділити на такі категорії: основні, додаткові та додатки сторонніх розробників. Використовуючи розділ консолі адміністратора «Додатки», можна вмикати, вимикати та налаштовувати ці сервіси як для усього домену, так і для окремих його підрозділів. За замовчуванням налаштування додатків успадковуються від батьківської організації до дочірніх (з рівня домену до

підрозділів). У такий спосіб можна гнучко налаштовувати окремі сервіси для певних підрозділів. Наприклад, можна вимкнути сервіс Meet для певного підрозділу (рис. 3.9), заборонити надавати доступ до ресурсів Google Диска стороннім особам (рис. 3.10).

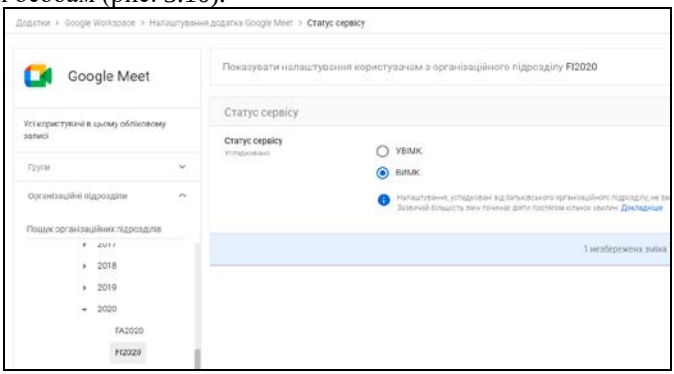

Рис. 3.9. Конфігурування доступу до додатків Google Workspace (Google Meet)

Також існують параметри конфігурування, які можна встановити для усього домену: створити список заблокованих відправників електронної пошти або ж тих, які не будуть ідентифіковані як спам.

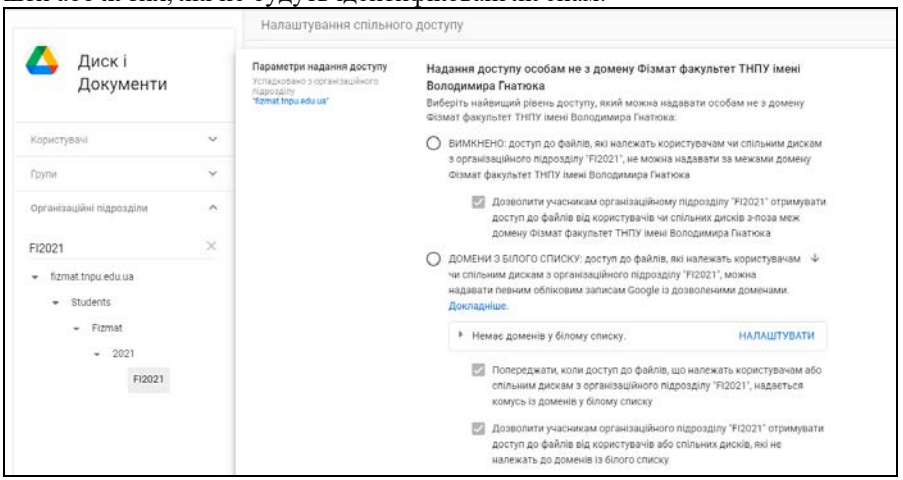

Рис. 3.10. Конфігурування доступу до додатків Google Workspace (Google-диск)

Існує можливість змінювати та застосовувати зазначені параметри не лише до підрозділів, а й до груп користувачів. Завдяки цьому можна застосовувати правила без реструктуризації організаційних підрозділів. Це дає мож-

ливість надавати групам доступ до різних додатків (сервісів), змінювати й оновлювати правила та призначати різні налаштування для користувачів

Для більш гнучкого управління доменом у пакеті Google Workspace передбачено можливість делегування користувачам адміністративних ролей. Зазначені завдання є актуальними для великих закладів освіти. З метою делегування адміністративних повноважень у системі Google Workspace створено такі системні ролі:

- суперадміністратори – мають повний доступ до консолі управління; вони можуть створювати і призначати ролі адміністраторів, а також змінювати їх паролі;
- адміністратори груп мають повний доступ до розділу «Групи» та доступ для перегляду розділів «Користувачі» та «Профіль компанії»;
- адміністратори керування користувачами мають повноваження для повного доступу щодо облікових записів користувачів у всіх підрозділах, а також можуть переглядати вміст підрозділів;
- адміністратори довідкової служби мають доступ читання даних облікових записів користувачів, також повноваження зміни паролів користувачів, що не мають повноважень адміністратора;
- адміністратори служб мають можливість додавати і видаляти служби у межах домену, а також повноваження для перегляду підрозділів домену.

Для того щоб делегувати користувачеві адміністративну роль, слід перейти на сторінку його облікового запису, й у розділі «Ролі» обрати потрібні повноваження (рис 3.10) або створити нову роль.

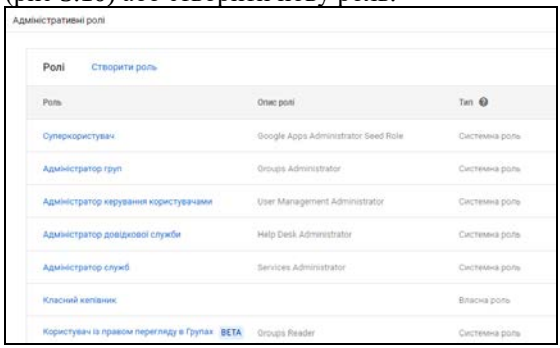

Рис. 3.10. Делегування адміністративних ролей

4. СЕРВІС ЕЛЕКТРОННОЇ ПОШТИ GMAIL

Як відомо, основним сервісом хмарної платформи Google Workspace є електронна пошта Gmail. Електронна пошта є важливим інструментів роботи сучасного педагога. За допомогою адреси електронної пошти проводиться реєстрація на багатьох мережних ресурсах та сервісах.

Перш ніж почати користуватися електронною поштою Gmail, у домені Google Workspace потрібно налаштувати записи типу MX (Mail Exchanger). Це можна виконати на панелі хостингу у реєстратора або на сервері імен домену. Запис необхідний для того, щоб електронні повідомлення маршрутизувалися на поштові сервери компанії Google. Значення записів можна знайти у розділі розширених налаштувань сервісу Gmail (рис.4.1).

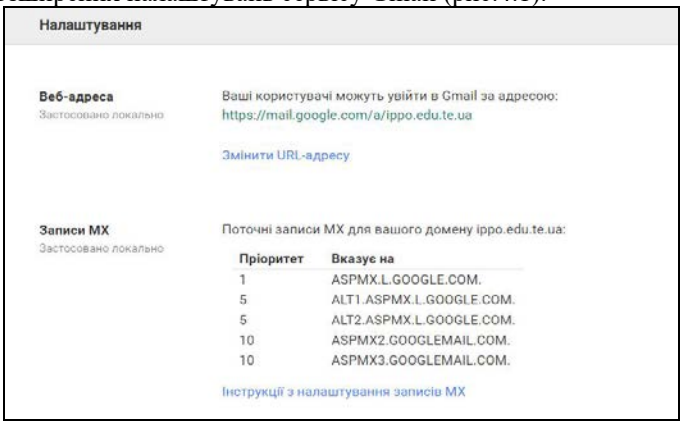

Рис. 4.1. Конфігурування маршрутизації пошти у домені Google Workspace

Для кожного створеного облікового запису Google Workspace для освіти сервіс електронної пошти Gmail є доступним за замовчуванням. Перехід до Gmail можливий через меню вибору сервісів (рис. 4.2):

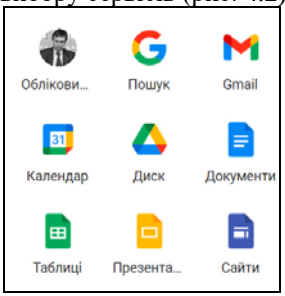

Рис. 4.2. Меню переходу між сервісами

Інтерфейс сервісу Gmail є інтуїтивно зрозумілим. Він містить такі складники (рис. 4.3):

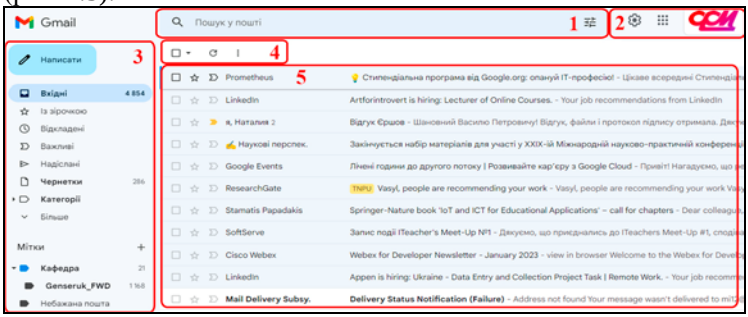

Рис. 4.3. Основні складники інтерфейсу сервісу Gmail

1. Рядок пошуку – дає можливість знайти листи, які містять вказану адресу відправника, тему, вміст повідомлення тощо.
2. Меню облікового запису користувача – забезпечує завершення сеансу роботи або вхід в інший обліковий запис, а також покликання для налаштування сервісу Gmail.
3. Папки поштової скриньки – містять отримані, підготовлені, надіслані листи. Користувач може створити довільну кількість власних папок. Список гіперпосилань «Пошта» забезпечує перехід до контактів або завдань облікового запису.
4. Панель операцій з листами – дає можливість виділяти всі листи. Після виділення на панелі з'являються кнопки для виконання операцій архівування, позначення повідомлення як спам, видалення, перенесення листа до іншої папки, визначення мітки.
5. Область відображення листів.

До основних операцій з електронною поштою належать отримання, створення і надсилання повідомлень. Після завантаження головної сторінки сервісу відображається папка «Вхідні», яка містить отримані повідомлення, що відсортовані за датою отримання.

При створенні нового повідомлення до поля *Кому* слід вказати адресу електронної пошти людини, якій буде адресовано лист. Адресу можна ввести вручну або вибравши зі списку, який буде запропоновано. Сервіс Gmail забезпечує пошук серед адрес, з якими попередньо відбувалося листування. У випадку використання корпоративних сервісів Google Workspace можливий пошук і адрес усіх облікових домену. Для того, щоб така функція була доступна слід у інтерфейсі адміністратора перейти до розділу «Налаштування каталогу». При цьому доступними є такі параметри (рис. 4.4):

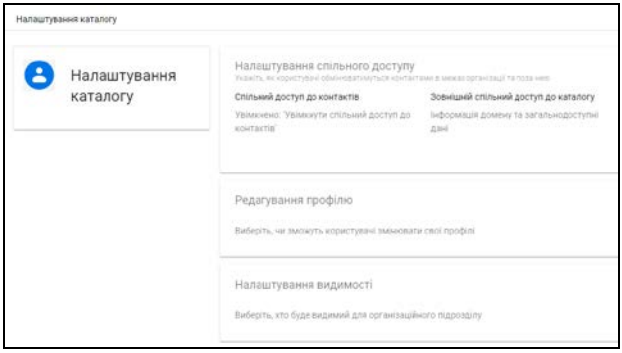

Рис. 4.4 Конфігурування спільного використання контактів

- активувати спільне використання адресної книги (доступ до контактів);
- обмеження на відображення адрес для користувачів, що не належать до організації;
- дозвіл користувачам змінювати власні поля профілю;
- поля, що відображатимуться у спільному каталозі користувачів (рис. 4.5).

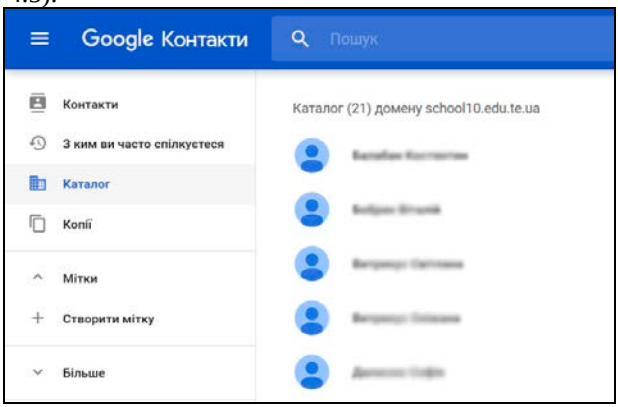

Рис. 4.5 Каталог контактів домену

Крім основного одержувача у листі можна вказати інших адресатів, скориставшись полем *Копія* або *Прихована копія*. Відмінність між ними полягає в тому, що при використанні першого поля всі адресати будуть бачити адреси електронної пошти один одного, а при використанні прихованої копії – тільки власну адресу.

Якщо лист не закінчено, він буде автоматично збережений у папці *Чернетки*. Для цього достатньо вийти з вікна створення листа, не відправляючи його, і не видаляючи його.

У інтерфейсі створення повідомлення є поле *Тема*. У ньому зазвичай пишуть коротку фразу або кілька ключових слів, які розкривають зміст повідомлення. Створюючи новий лист, доцільно вказувати тему повідомлення, адже це допомагає адресату систематизувати вхідні листи і більш ефективно здійснювати пошук потрібних повідомлень. Якщо потрібно відповісти на лист, слід скористатися опцією *Відповісти*. У цьому випадку листи буде згруповано, утворивши ланцюжок із загальною темою. У папці *Вхідні* такий ланцюжок можна відрізнити за цифрою у дужках, яка вказує на сумарну кількість повідомлень. Також червоним написом будуть ланцюжки, у яких при відповіді були збережені чернетки (рис. 4.6). За бажанням групування повідомлень у ланцюжки можна вимкнути у налаштуваннях сервісу.

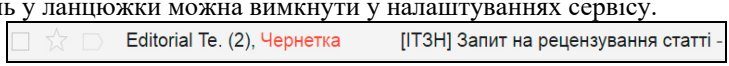

Рис. 4.6 Ланцюжок повідомлень сервісу Gmail

Отримані повідомлення в папці «Вхідні» виділяються напівжирним шрифтом. Якщо в отриманому повідомленні є вкладені файли, їх можна переглянути безпосередньо у вікні браузера або завантажити їх на свій комп'ютер або Google-диск.

Налаштування сервісу Gmail користувач може виконати за допомогою однойменної кнопки (блок 2, рис. 4.3). Перерахуємо основні функції, які можна встановити на сторінці налаштувань (рис. 4.7):

- загальні – дає можливість змінювати мову інтерфейсу, стиль тексту, використання ланцюжків повідомлень, їх підписи, автовідповідач;
- облікові записи й імпорт – дозволяє обрати, від імені якого облікового запису буде надіслано лист, а також додати обліковий запис, повідомлення якого слід опрацьовувати за допомогою сервісу Gmail;
- фільтри й заблоковані адреси – забезпечують автоматичну організацію та обробку пошти (сортування, пересилання, видалення, блокування);
- пересилання та POP/IMAP – дає можливість автоматично спрямувати усі вхідні листи на іншу адресу, а також дозволити їх обробку за допомогою поштових програм;
- розширені – дозволяє налаштувати власні сполучення клавіш та теми оформлення інтерфейсу;
- теми – використовують для зміни зовнішнього вигляду сервісу.

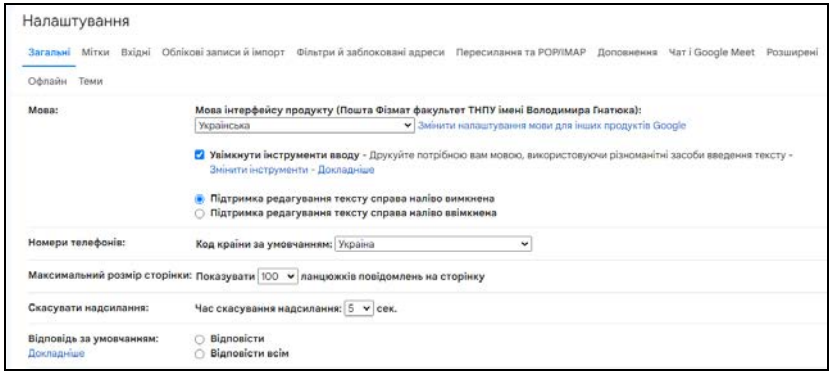

Рис. 4.7 Сторінка налаштувань сервісу Gmail

Слід звернути увагу на папку «Спам», у якій зберігаються небажані повідомлення рекламного або шахрайського характеру. Наприклад, якщо користувач пошти систематично надсилає спам, його обліковий запис може бути заблокований. До цієї папки потрапляють повідомлення у двох випадках: внаслідок їх ідентифікації антиспамовими фільтрами системи Gmail або після того, як їх визначив такими користувач. У останньому випадку слід перейти до повідомлення та обрати покликання у вигляді знаку оклику у панелі операцій (рис. 4.8).

Рис. 4.8 Позначення повідомлення як спам

Система Gmail використовує багатоетапну перевірку повідомлень для їх визначення як спам. Проте трапляються випадки, коли деякі повідомлення будуть помилково ідентифіковані як спам. Така ситуація може трапитися, якщо поштовий сервер відправника налаштований неправильно або скомпрометований (потрапив до списку надсилачів спаму). Консоль адміністратора надає засоби для визначення виняткових правил фільтрування спаму у межах домену. Для їх створення слід перейти у розділ *Додатки*, у якому обрати сервіс Gmail. Серед додаткових (розширених) налаштувань можна ввести список IP-адрес поштових серверів, листи з яких не будуть класифікуватися як спам (рис. 4.9).

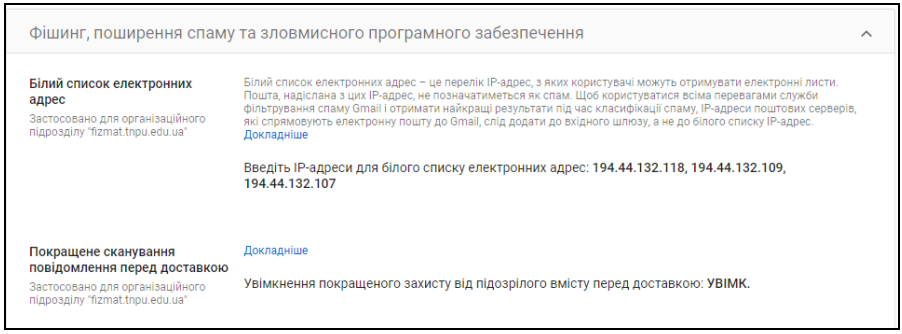

Рис. 4.9 Створення списку дозволених відправників, на основі IP-адрес

Більш ефективна фільтрація спаму можлива через визначення шлюзу імпорту повідомлень. Також у розділі спам можна створити «білий список» дозволених відправників, вказуючи їх електронні адреси або доменні імена (рис. 4.10).

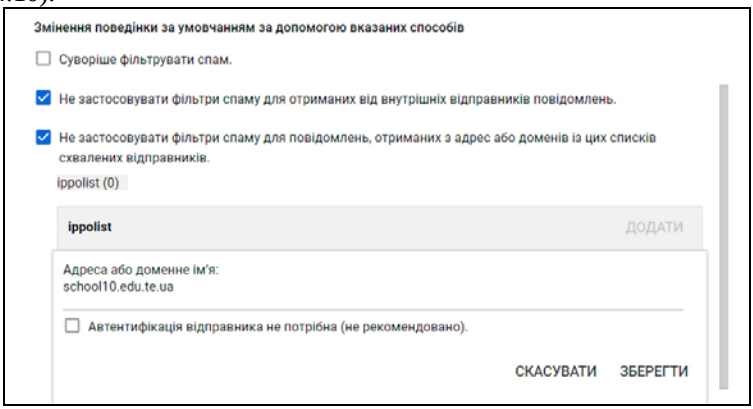

Рис. 4.10 Створення списку дозволених відправників, на основі доменних імен

У цьому ж розділі можна створити списки заблокованих відправників (чорний список). Як відомо листи, які потрапили у папку *Спам*, будуть переміщені до кошика через 30 днів. У згаданому розділі можна визначити дії, які відбуватимуться з листами у папці *Спам*. Наприклад, їх можна остаточно видаляти через певну кількість днів. Також існує можливість фільтрування повідомлень за їх вмістом.

Для того, щоб листи, що надіслані обліковими записами користувачів домені, не визначалися поштовими системами одержувачів, як спам у системі DNS слід налаштувати записи типу DKIM (рис. 4.11). Зазначений запис дає

можливість запобігти загрозам спуфінгу або фішингу. Спуфінг – це різновид атаки, заснований на підробці адреси відправника електронного листа. Підроблені листи мають такий вигляд, наче вони надіслані певною організацією або з певного домену. DKIM дозволяє дізнатися, чи було повідомлення змінено після надсилання.

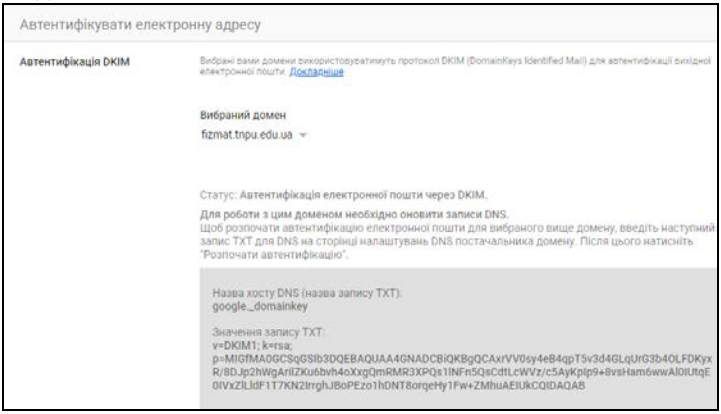

Рис. 4.11. Конфігурування автентифікації листів за допомогою запису DKIM

Починаючи з листопада 2022 року, нові відправники листів на особисті облікові записи Gmail повинні обов'язково використовувати у системі DNS записи SPF або DKIM. Змінюючи будь-які налаштування у інтернет домені, варто пам'ятати, що для їх повного оновлення на всіх DNS-серверах потрібно 48 або й більше годин.

Потужним інструментом конфігурування сервісу Gmail є маршрутизація повідомлень. Вона надає такі можливості (рис. 4.12):

- пересилати повідомлення, надіслані невідомим обліковим записам;
- пересилання повідомлень на інші поштові сервери – використання опції може забезпечити синхронізацію в межах навчального закладу вхідних повідомлень різних поштових систем, наприклад Gmail та Outlook з хмарного пакету Microsoft 365;
- створення графіка періодичної доставки повідомлень із підсумками, які міститимуть відомості про нещодавно отриманий спам;
- визначення детальних фільтрів опрацювання повідомлень.

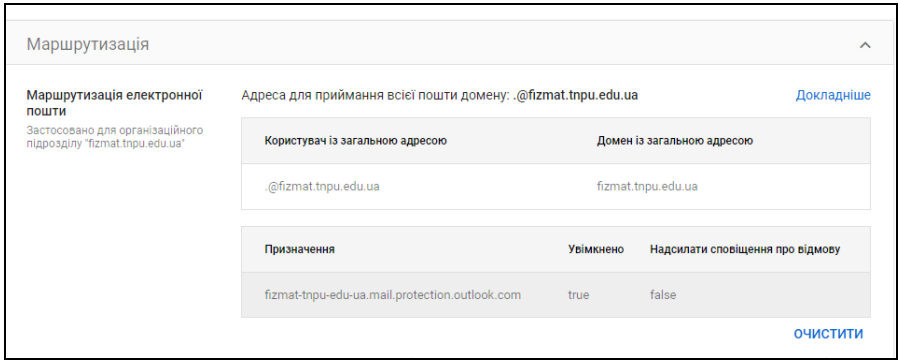

Рис. 4.12 Конфігурування маршрутизації електронних повідомлень

Розглянемо інші налаштування поштового сервісу, які доступні адміністратору домену. На сторінці додатку Gmail вони згруповані за такими вкладками:

- облікові записи користувачів (розширені налаштування);
- адреси електронної пошти;
- лабораторії;
- маршрутизація за замовчуванням;
- автентифікація електронної пошти;
- керування карантином.

На сторінці розширених налаштувань можна змінити URL-адресу входу до сервісу Gmail. Наприклад, можна встановити адресу у форматі *mail.<адреса домену освітнього закладу>*. У цьому ж розділі для користувачів можна увімкнути можливість імпорту пошти й контактів інших вебсервісів або облікових записів за протоколом POP3. Зазначений функціонал буде доступний на сторінці налаштувань сервісу (рис. 4.7). Також користувачам можна дозволити або заборонити змінювати теми оформлення інтерфейсу Gmail.

Корисною функцією багатьох поштових систем є повідомлення відправника про прочитання листа адресатом. Коло відправників, які будуть отримувати сповіщення про прочитання, можна обмежити. Зокрема можна надсилати повідомлення тільки відправникам в межах організації, визначеному переліку електронних адрес або усім. Адміністратор також визначає, чи буде повідомлення про прочитання відправлятися автоматично при відкритті повідомлення або одержувача буде повідомлено з проханням підтвердити його надсилання (рис. 4.13). Для додавання запиту про отримання слід у нижній частині нового листа викликати меню, у якому обрати пункт «Запитати підтвердження про прочитання».

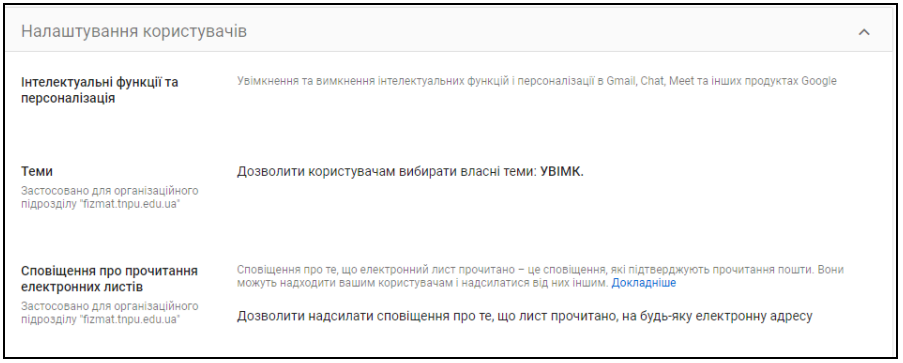

Рис. 4.13. Конфігурування повідомлень про доставляння листа

У цьому ж розділі користувачам можна дозволити делегувати доступ до їх поштових скриньок іншим особам у домені. Користувач, якому делеговано доступ, матиме можливість входити у інший обліковий запис, читати й видаляти повідомлення та навіть надсилати листи від імені власника поштової скриньки. При цьому він не зможе змінювати налаштування облікового запису та пароль.

Після задіяння зазначеної опції у налаштуваннях сервісу користувача на вкладці «Облікові записи» з'явиться можливість надання доступу до свого облікового запису (рис. 4.14). Делегування буде задіяно лише у випадку згоди користувача, якому надають доступ.

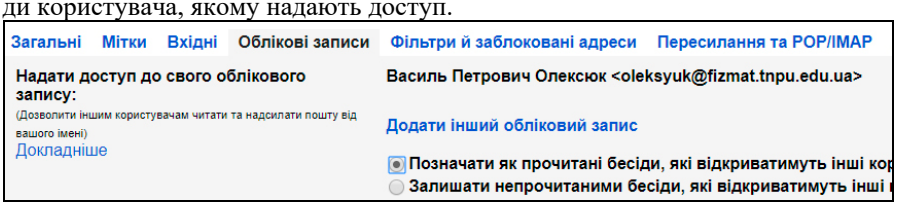

Рис. 4.14. Делегування доступу до поштової скриньки

У розділі додаткових налаштувань задають формат назви облікового запису. Як наслідок при адресуванні листа у полі *відправник* буде використано один з двох форматів: *«Прізвище, ім'я» або «Ім'я, прізвище»*. Проте існує можливість надання дозволу користувачам самостійно визначати цей формат.

Як видно з рис. 4.7 у налаштуваннях сервісу Gmail, які доступні користувачу, доступні параметри, що стосуються отримання повідомлень за стандартними протоколами POP3 та IMAP. Проте у розділі додаткових налаштувань адміністратор має змогу централізовано вимкнути доступ за протоколами POP та IMAP для всіх користувачів. За замовчуванням користувачам до-

зволено налаштовувати в Gmail автоматичне пересилання пошти на іншу адресу. Адміністратор також має змогу вимкнути цю функцію. У цьому випадку параметри автоматичного пересилання більше не будуть показані користувачеві у налаштуваннях сервісу Gmail, а налаштовані правила пересилання або фільтри перестануть діяти. Слід зауважити, що застосування додаткових параметрів Gmail до окремих облікових записів користувачів може займати деяких час (до години). У консолі адміністратора існує можливість переглянути внесені зміни, які ще не відображаються у інтерфейсі користувача. Для цього варто відкрити журнал аудиту (*«Створення звітів» – «Аудит і аналіз» – «Події в журналі адміністратора»*) (рис. 4.15):

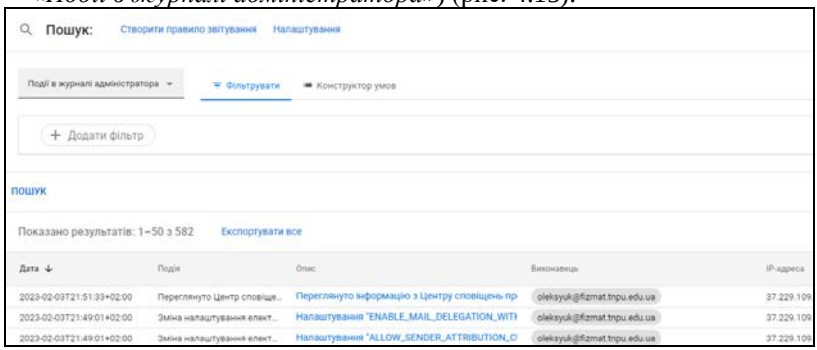

Рис. 4.15. Відображення змінених налаштувань у інтерфейсі адміністратора

У адміністратора сервісу Gmail існує можливість налаштувати використання шлюзу вихідної пошти. Ним є сервер, через який проходять всі повідомлення, що надіслані користувачами домену. Як правило, перед надсиланням шлюз обробляє пошту, наприклад архівує її або фільтрує спам. При використанні шлюзу вихідної пошти сервери Google Workspace передають всі надіслані листи на сервер шлюзу. Перед увімкненням параметра адміністратору необхідно налаштувати сервер шлюзу на приймання повідомлень з поштових серверів Google Workspace. Можливо, адміністратору потрібно буде оновити конфігурацію серверів DNS, створивши для домену записи типу DKIM та SPF.

Корисним безпековим засобом сервісу Gmail є проксі сервер, який застосовується для відображення прикріплених до листа зображень. Такий засіб допомагає захистити користувачів і домен, не даючи зловмисникам використовувати вразливості в системі обробки зображень. Проте іноді через використання проксі-сервера не працюють посилання на зображення, пов'язані з внутрішніми IP-адресами і файлами cookie. Запобігти цьому можна за допомогою схваленого (білого) списку URL дозволених зображень. Він містить внутрішні URL-адреси, для яких не потрібно використовувати проксі-сервер.

Створення зазначеного списку можливе у розділі розширених налаштувань сервісу Gmail. У цьому ж розділі можна налаштувати виведення попередження при надсиланні відповіді на лист, одержаний з-за меж домену. Використання такої опції може запобігти випадковому надсиланню конфіденційних даних. Попередження буде виведено також у випадку, якщо користувач систематично не листується з одержувачем.

У розділі розширених налаштувань доступні параметри опрацювання листів щодо їх відповідності певним критеріям:

- автоматичне видалення або перенесення до кошика електронних листів і повідомлень чату (можна налаштувати термін виконання видалення, а також фільтрацію листів за мітками);
- комплексне збереження повідомлень, яке передбачає окреме зберігання копій усіх отриманих і надісланих повідомлень в поштових скриньках користувачів;
- додавання нижніх колонтитулів (підписів), які будуть додані до вихідних листів;
- обмеження надсилання повідомлень – існує можливість створити списки заблокованих доменів або адресатів;
- фільтрування вихідних та вхідних повідомлень стосовно наявності у них забороненого вмісту (застосовуються фільтри на основі слів, фраз чи шаблонів);
- обмеження неприйнятного вмісту повідомлень на основі списків заборонених слів;
- фільтрування повідомлень на відповідність критеріям вкладених у листи файлів (типу, ім'я та обсяг файлу);
- обробка повідомлень за допомогою захищеного протоколу TLS;
- маршрутизація листів на зовнішні SMTP-сервери;
- співставлення адрес отримувачів – параметр дає змогу для вхідних повідомлень у домені застосовувати псевдоніми до адрес одержувачів;
- обробка журналів вхідної пошти за допомогою сервісу збереження та архівації Google Сейф;
- надсилання повідомлень з мереж організації через SMTP-сервери Google Workspace;
- використання резервного захищеного маршруту для повідомлень, якщо їх передача вимагає підвищеної безпеки.

На рисунку 4.16 наведено приклад електронної адреси до списку заблокованих:

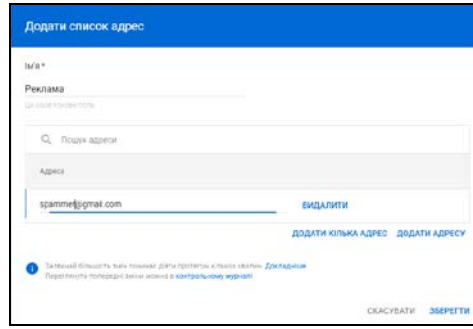

Рис. 4.16. Приклад блокування адресата

Крім відхилення повідомлень існує можливість зміни його змісту – додавання службових заголовків, редагування теми, переспрямування на інші SMTP-сервери, відімкнення спам-фільтрів, видалення вкладень, додавання інших одержувачів тощо.

Ще одним методом опрацювання листів у фільтрах є перенесення їх до карантину. При цьому при обробці вхідного або вихідного листа буде здійснено його переміщення та надсилання адресату або відправнику повідомлення про відхилення. Додатково можливе періодичне нагадування адміністратору про наявну кореспонденцію в карантині. Доступ до карантину можна отримати у розділі «Карантини». Налаштувавши правила карантину, можна переглядати поміщені до нього повідомлення і приймати рішення щодо їх подальшої обробки – дозволяти або забороняти одержання листа (рис. 4.17). Додатково сервіс Gmail надішле повідомлення адміністратору про поміщення листа до карантину.

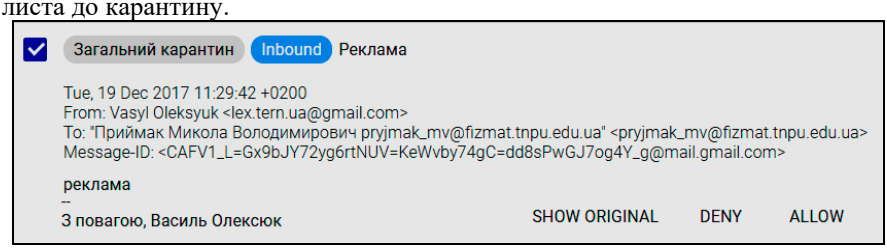

Рис. 4.17. Повідомлення у карантині

Поряд з кожним листом зазначено назву відповідного карантину і тип повідомлення (вхідне або вихідне). Якщо у вхідного повідомлення кілька одержувачів, воно потрапляє в карантин для кожного з них. Наприклад, повідомлення, адресоване п'ятьом користувачам, поміщається в карантин п'ять разів. Вихідне повідомлення, надсилання якого дозволене, поміщається в ка-

рантин тільки один раз незалежно від кількості одержувачів. При опрацюванні повідомлень за допомогою карантину можливе його використання лише для деяких облікових записів користувачів або груп або створення списків виключень, до яких не будуть застосовані правила. Також винятки можуть бути й для відправників листів.

Якщо потрібно налаштувати карантин лише вихідної корпоративної кореспонденції, слід обрати його тип *«внутрішня пошта – надсилання»*. Щоб заощадити обсяг карантинів, розробники Google Workspace не рекомендують створювати великі списки розсилання, до яких можуть надсилати пошту зовнішні користувачі.

Крім псевдонімів користувачів у сервісі Gmail можливе створення додаткових адрес користувача за допомогою співставлення адрес отримувачів. Часто базова модель маршрутизації пошти, яка є таблицею віртуальних облікових записів користувачів, використовується для переадресації повідомлень. Для цього слід у розділі розширених налаштувань поштового сервісу перейти до розділу *«Адреса отримувача на карті»*. Загалом можна створити відповідності для 2000 окремих електронних адрес. Варто зауважити, що адреса одержувача зіставляється лише з однією існуючою адресою (рис. 4.18).

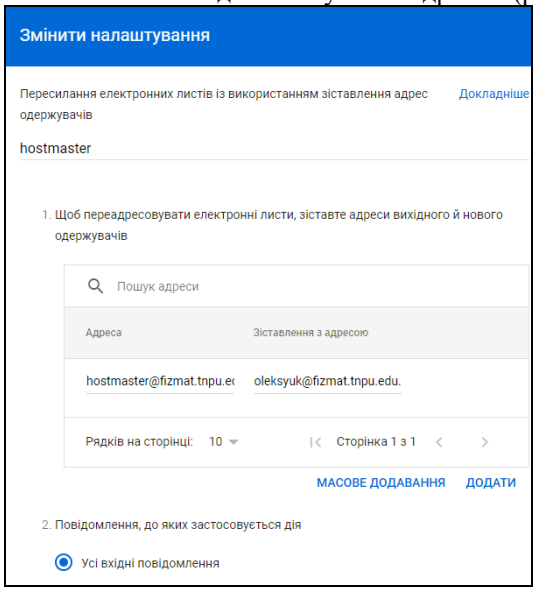

Рис. 4.18 Додавання відповідності для адреси отримувача

Якщо повідомлення має містити відомості про справжнього одержувача (його адреса відправника вказує в поле Кому), то в розділі Параметри в ниж-

ній частині вікна слід встановити прапорець *Додавати заголовок X-Gm-Original-To*. Цей заголовок варто використовувати при повторному пересиланні копії повідомлення, оскільки адреса одержувача при ній також зміниться. Якщо новому одержувачу необхідно знати, кому насправді був відправлений лист спочатку, він побачить адресу одержувача у заголовку (*X-Gm-Original-To*).

Потужним інструментом моніторингу хмарних сервісів Google Workspace є розділ *«Звіти»*. Стосовно поштового сервісу Gmail у ньому можна переглянути статистику надісланих та одержаних листів (рис. 4.19).

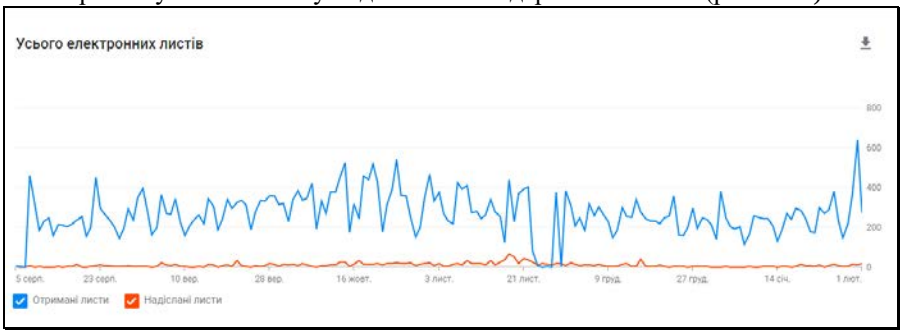

Рис. 4.19 Статистика використання сервісу Gmail

Також у цьому розділі наявний журнал надсилання і отримання повідомлень, використовуючи який адміністратор має змогу віднайти та проаналізувати статус кожного надісланого або одержаного повідомлення у межах домену (рис. 4.20).

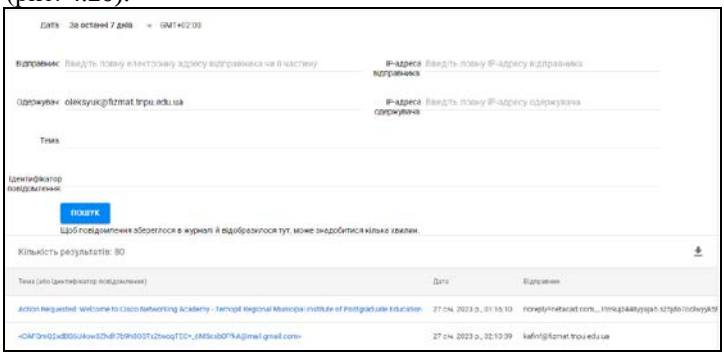

Рис. 4.20 Пошук листа у журналі повідомлень

5. ХМАРНЕ СХОВИЩЕ GOOGLE ДИСК

Google Диск (*англ. Google Drive*) – це хмарний сервіс, що входить до пакету Google Workspace. Google Диск поєднує в собі функції сховища цифрових матеріалів та набору інструментів і сервісів для роботи з ними, а саме додатки: для роботи з документами в текстовому редакторі (Документи Google (Google Docs)), для опрацювання та аналізу даних (Таблиці Google), проведення опитування та тестування (Форми Google), створення зображень (Малюнки Google) і презентацій (Презентації Google), формування власних карт (Google карти), проектування веб-сторінок (Google Сайти). Окрім згаданих базових сервісів до Диску можна підключати додатки, створені партнерами компанії Google, а також розробляти власні програми на основі вбудованого в Google Диск мови сценаріїв Google-скрипт.

Нині Google пропонує всім користувачам початкові 15 Гб онлайн-простору для зберігання, що доступний для трьох найбільш використовуваних послуг: Google Диск, Gmail, Photo). Користувачі можуть розширити обсяг пам'яті через платний місячний план підписки. Документи, що використовують власні формати Google Docs (.gdoc, .gslides і .gsheet) не зараховуються до загального обсягу. У сервісі Google Photo, фотографії з роздільною здатністю менше 2048x2048 пікселів і відео тривалістю менше 15 хвилин також не зараховуються до цієї квоти. У межах корпоративної підписки Google Workspace for Education користувачам безкоштовно надаються значні обсяги дискового простору в хмарі Google (станом на 2022 рік доступно 100 ТБ спільного сховища, що розподіляється серед усіх користувачів). Зазвичай викладачам та студентам не потрібно турбуватися про видалення старих файлів, про переповнення простору даними.

Доступ до Google Диска можна отримати, перейшовши за адресою https://drive.google.com, або за допомогою меню переходу між сервісами (рис. 4.2). Після цього користувач потрапляє на сторінку сервісу, де є можливість завантажувати до нього файли практично будь-яких форматів, редагувати основні типи документів, а також надавати доступ до папок та файлів.

Основними складниками інтерфейсу сервісу є (рис. 5.1):

1. Меню основних складників сховища – усього диску, об'єктів, до яких надано доступ, останніх змінених файлів та папок, фотографій, кошику.
2. Рядок пошуку об'єктів на диску.
3. Гіперпосилання для переходу між сервісами, навігації між профілями користувача, конфігурування параметрів сервісу.
4. Меню, що відображає шлях до поточної папки та забезпечує виконання основних операцій з об'єктами диска (створення, копіювання, перейменування, завантаження на локальний пристрій, видалення, надання спільного доступу, отримання посилання).

5. Блок гіперпосилань, що дають змогу змінити відображення об'єктів (у вигляді списку або таблиці), відобразити інформаційну панель отримати відомості про об’єкт;
6. Робоча область сервісу, що відображає об’єкти хмарного сховища.

Рис. 5.1. Основні складники інтерфейсу сервісу Google диск

Натиснувши у робочій області на заголовок таблиці, можна виконати сортування у порядку зростання чи спадання та за відповідним критерієм (назва, власник, остання зміна, останні змінені мною, останні відкриті мною). У режимі списку файли відображаються у вигляді піктограм із зображенням вмісту документа і його іменем.

При натискуванні на гіперпокликанні у вигляді літери «І» відображається інформаційна панель (рис. 5.2), що містить дані про деталі обраної папки чи файлу (тип файлу, обсяг, розташування, власників, дату зміни, дату відкриття, дату створення, опис). Вкладка «*Дії*» – містить відомості про зміни у файлах чи папках усіма користувачами, які мають доступ до елементу, посилання на елемент та можливість перегляду його у папці.

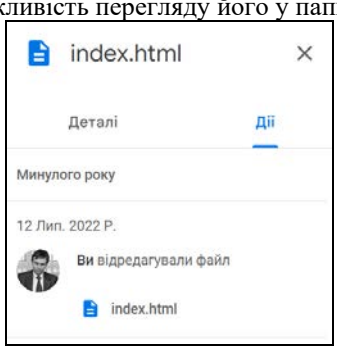

Рис. 5.2. Інформаційна панель сервісу Google диск

Горизонтальне меню (рис. 5.3) містить список гіперпокликань, що вказують місцезнаходження від кореневої до поточної папки та доступ до її контекстного меню.

Рис. 5.3. Меню об'єкта у хмарному сховищі Google Диск

Пункти меню залежать від розташування та типу обраного об'єкта. Тобто кореневому каталогу (папка «Мій диск») відповідає меню, що можна викликати натисканням кнопки *«Створити»*, а при натисканні на меню підпапок або файлів, буде викликано їх контекстне меню (рис.5.4).

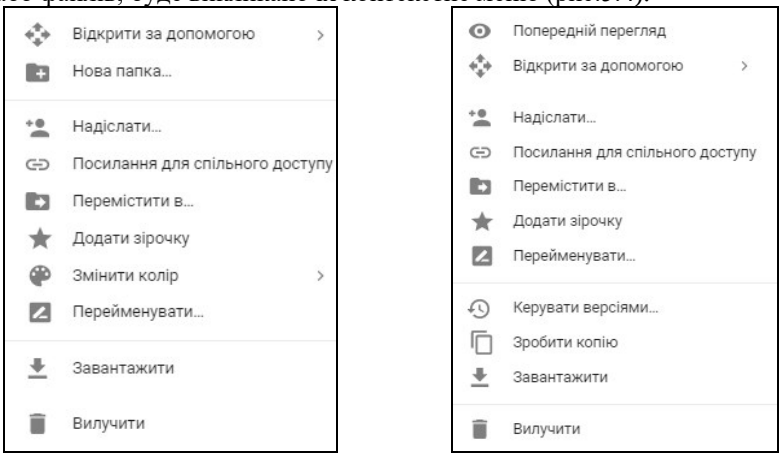

Рис. 5.4. Контекстне меню папки (а) та файла(б)

Основними пунктами контекстного меню є:

- «попередній перегляд» (тільки для файлів) – відкриває вікно попереднього перегляду файлу;
- «відкрити за допомогою» – дає змогу вибрати нестандартний додаток для відкривання папки чи файлу; відображає додатки, якщо такі підключені до диску, також доступним є посилання на сховище додатків;
- «надіслати» – відкриває вікно налаштувань спільного доступу до файлу/папки;
- «посилання для спільного доступу» – дозволяє створити посилання для спільного доступу до файлу/папки;
- «перемістити в» – відкриває меню переміщення обраного файлу або папки в інше місце на диску;

- «додати зірочку» – позначає файл або папку для швидкого доступу з розділу *«Із зірочкою»*;
- «змінити колір» (тільки для папок) – дає змогу змінити колір обраної папки;
- «перейменувати» – перейменовує обрану папку або файл;
- «керувати версіями» (лише для файлів) – відкриває сторінку з версіями файла, якщо такі були створені у процесі його редагування;
- «створити копію» (тільки для файлів) – створює копію вибраного файлу в тій же папці;
- «завантажити» – завантажує обраний файл на локальний пристрій;
- «вилучити» – переміщує вибраний файл або папку в кошик.

За замовчуванням можна створювати документи таких типів: текстові, табличні, презентації, малюнки, форми, карти, сайти. Існує також можливість підключення до Google Диску додаткових сервісів: редакторів діаграм, онлайн-дошок, спеціальних математичних додатків для побудови графіків і геометричних фігур тощо.

Загалом функціонал щодо роботи з файлами та папками на Google Диску є аналогічним до основних операцій у поширених ОС. Причому основні операції можна виконувати за допомогою кількох елементів інтерфейсу. Наприклад, створення файлів можна виконувати за допомогою відповідної кнопки, списку навігації, контекстного меню. Варто зауважити, що на відміну від ОС, в одній і ті й же папці Google Диска, може міститися кілька об'єктів з однаковими назвами.

Копіювання файлів також подібне до ОС – потрібно виділити один об'єкт або їх групу та обрати відповідний пункт з контекстного меню. Копія файлу буде створена в тій же папці. При створенні копій назва скопійованого файла формується за шаблоном «Копія», до якого буде додано назву оригінального файлу. Переміщення об'єктів можливо за допомогою контекстного меню або способом перетягування. Кожну з операцій можна відмінити, натиснувши комбінацію клавіш «Ctrl+Z» або відповідну опцію у діалоговому блоці, який буде відображено одразу після завершення операції (рис. 5.5).

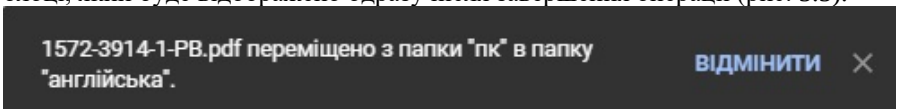

Рис. 5.5. Відміна виконаної операції

Сервіс Google Диск надає можливості завантажувати файли з хмарного сховища на локальний пристрій та у зворотному напрямі. Перед завантаженням файлу здійснюється його тестування антивірусом (файли більше 25 Мб антивірусом не перевіряються проте відображається повідомлення з попередженням).

Завантажити файли на особистий пристрій можна і в режимі перегляду документу. Для цього необхідно скористатися відповідною опцією у правому верхньому кутку вікна перегляду. Передавання (uploading) файлів або папок на Google Диск можливе за допомогою кнопки «Створити», навігаційного меню (рис. 5.1, блок 4) або за допомогою способу перетягування (працює не у всіх браузерах). Для вилучення об'єктів можна скористатися: їх контекстним меню, способом перетягування їх до кошика, клавішею *«Delete»*. Протягом нетривалого часу після операції, її можна скасувати за допомогою спливаючого блока (рис. 5.5). У традиційний спосіб у кошику можна відновити вилучені файли і папки або ж видалити їх назавжди.

З папкою або файлом який розміщений у сховищі Google Диск можуть одночасно працювати кілька користувачів. Для цього для об'єкта треба налаштувати параметри спільного доступу. Він дає змогу організувати групову роботу учасників освітнього процесу. Переглядати документ і вносити в нього зміни можуть відразу кілька людей як одночасно. Наприклад, до загального сховища документів необхідно надати доступ всім працівникам школи, які поряд з адміністрацією беруть участь в поповненні та оновленні даних. Для сповіщення різних цільових груп у документах можуть бути використані різні режими публікації: з відкритим доступом для всіх, з обмеженим доступом (для всіх у межах домену), з персональним (іменним) доступом. Для різних категорій користувачів або груп можна надати різні права доступу до папок або файлів. У таблиці 5.1 наведено основні категорії користувачів та їх відповідні повноваження для виконання певних операцій.

Таблиця 5.1. Категорії користувачів та їх повноваження щодо виконання операцій на Google Диску

Користувач	**Повноваження**
Власник	додавання та видалення елементів з папки; надання та вилучення повноважень доступу; позбавлення будь-яких співавторів доступу; налаштування терміну дії доступу; надсилання запрошень іншим користувачам; передача права володіння іншому користувачеві; видалення папок.
Редактор	запрошення і видалення інших співавторів (якщо власник надав редакторам такий дозвіл); завантаження файлів і їх синхронізація з іншими пристроями; перегляд списку співавторів; створення копій файлів; завантаження й вилучення версій файлів;

	додавання та видалення файлів з папки.
Коментатор	додавання коментарів (лише для файлів); перегляд документів і презентацій; завантаження документів і презентацій на комп'ютер і їх синхронізація з іншими пристроями; створення копій документів і презентацій на власний Диск.
Читач	перегляд файлів, папок і документів Google; завантаження файлів і синхронізація з іншими пристроями; створення копій на власний Google Диска.

Існують такі способи надання доступу до своїх матеріалів іншим користувачам:

- перейти за гіперпокликанням, що розташоване праворуч від навігаційного меню (блок 4, рис. 5.1);
- обрати пункт *«Надіслати»* у контекстному меню об'єкта;
- скористатися гіперпосиланням *«Спільний доступ»* у вікні редагування документа (для того, щоб спільно працювати над файлами Microsoft Office, їх слід перетворити у формат документів Google Диска, відкривши у сервісах Google Docs, Таблиці або Презентації).

У вікні, що відкриється, слід вказати імена або електронні адреси користувачів, а також обрати режим доступу (редагування або перегляд). Перейшовши за гіперпосиланням *«Додатково»*, можна переглянути та змінити параметри доступу до файла або папки (рис. 5.6):

- посилання для спільного доступу (доступно тільки для співавторів);
- перелік користувачів та їх повноваження доступу до об'єкта;
- надання користувачам спільного доступу;
- сповіщення користувачів про надання їм доступу;
- заборону редакторам змінювати параметри доступу й додавати доступ для користувачів.

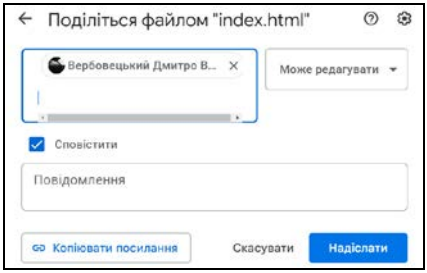

Рис. 5.6. Параметри спільного доступу до файла

Надаючи доступ до об'єкта, у вікні параметрів присутня опція для визначення терміну дії доступу (рис. 5.6). Для пришвидшення надання доступу

до об'єктів сховища, сервіс Google Диск містить засіб для надання доступу за гіперпосиланням. Для того, щоб ним скористатися, власнику достатньо перейти за відповідним гіперпосиланням у контекстному навігаційному меню. Наприклад, обравши у контекстному меню папки пункт *«Отримати посилання»*, можна зробити об'єкт доступним за покликанням.

Додаючи доступ для певних користувачів, можна обрати один з режимів доступу за посиланням (гіперпосилання *«Змінити»* на рис. 5.6);

- «Для всіх» – файл або папка буде індексуватися пошуковими системами і брати участь в загальному пошуку; як наслідок усі користувачі інтернету зможуть знаходити об'єкт й отримувати доступ до нього, при цьому входити до облікового запису Google не обов'язково;
- «Для всіх, хто має є посилання» – файл або папка буде доступний тільки за посиланням, після переходу за яким документ з'явиться у пункті меню «Відкриті для мене» Google диска;
- «Для користувачів домену» – файл або папка з'явиться в розділі «Відкриті для мене» у всіх користувачів організації;
- «Для користувачів домену, які мають посилання» – об'єкт буде доступним тільки за покликанням у межах організації. Після авторизації користувача на сервісі Google Диск спільний документ буде доступним у розділі «Відкриті для мене»;
- «Для певних користувачів» – файл або папка буде доступний тільки користувачам лише для визначених облікових записів (рис. 5.6).

Користувач, який має доступ до файла або папки, завжди може зробити їх копію на власний диск. Для цього у розділі *«Доступні для мене»* досить викликати контекстне меню та обрати пункт *«Додати до диска»*.

Для того, щоб оперативно надавати доступ до ресурсів різним категоріям учнів або вчителів, їх доречно об'єднати у групи. Наприклад, надаючи доступ до спільної папки для користувачів групи «7class», вчитель або адміністратор забезпечить відповідний доступ до неї усім учням. Це дасть змогу практично відмовитися від записників, USB-флеш-накопичувачів та зовнішньої пам'яті.

Для збереження фотографій доречно скористатися можливостями сервісу Google Фото. Завантажені до нього файли будуть доступні на Google диску у папці *«Фотографії Google»*.

Для організації пошуку у серед об'єктів Google Диска використовують відповідну форму (блок 2, рис. 5.1). Ввівши текст у рядок пошуку, виконують так званий простий пошук. У цьому випадку пошуковий вираз буде проводитися одночасно у назвах усіх типів файлів. Додатково пошук також проводиться у повному тексті файлів та документів. Знайдені результати можна відсортувати за релевантністю або за останніми внесеними змінами. Звуження пошуку за тими чи іншими критеріями виконується у розширеному режи-

мі. Викликати режим розширеного пошуку можна натиснувши гіперпосилання у вигляді трикутника у рядку пошуку. У формі, що відкриється можна вказати:

- тип об'єкта (фотографія, документ, таблиця, презентація, папка, форма, файл у форматі PDF тощо);
- власник (сам користувач або вказаний обліковий запис);
- місцезнаходження файла або папки (на Google Диску користувача або на всіх доступних сховищах у межах домену);
- атрибут (позначений зірочкою або видалений до кошика);
- дата останньої зміни об'єкта;
- назва файла або папки;
- слова, які мітить файл;
- обліковий запис, якому надано доступ.

У пошуковому запиті можна вказати кілька слів. У цьому випадку будуть знайдені документи, що містять будь-яке з вказаних слів При використанні фрази в лапках виконується пошук файлів, що містять вказану фразу. Перелічуючи слова або фрази, можна вказати, які з них не повинні зустрітися у матеріалі. Для цього треба перед словосполученням слід вказати символ «мінус» («-»). Поряд з введенням даних у форму розширеного пошуку, можна використовувати пошукові конструкції. Наприклад, оператор «owner: from:» допомагає знайти файли або папки, до яких доступ відкрив або власником яких є вказаний користувач. Конструкція «to:» допомагає знайти документи, до яких надано доступу вказаному після оператора «to:» користувачеві.

Для конфігурування сервісу користувачеві слід перейти за покликанням у вигляді шестерні (блок 5, рис. 5.1). На сторінці, що завантажиться, будуть доступні такі основні параметри (рис. 5.7):

- «обсяг пам’яті» – дає змогу переглянути інформацію про обсяг даних збережених у сховищі (окремо виводиться статистика для сервісів Gmail, Google Диск, Google Фото);
- конвертування завантажених файлів у формат Google Drive (опція дозволяє заощадити місце, але може призвести до втрати даних, якщо документи містять скрипти, макроси, зведені таблиці);
- «мова» – дозволяє налаштувати мову веб-інтерфейсу;
- «офлайн» – забезпечує роботу з файлами, які синхронізовані на локальному пристрої, без доступу до мережі інтернет;
- «щільність» – змінює масштаб інтерфейсу;
- «швидкий доступ» – дозволяє налаштувати відображення панелі швидкого доступу.

- «сповіщення» – забезпечує виведення у браузері або надсилання електронних листів, які містять сповіщення про онолення об'єктів Google диску.

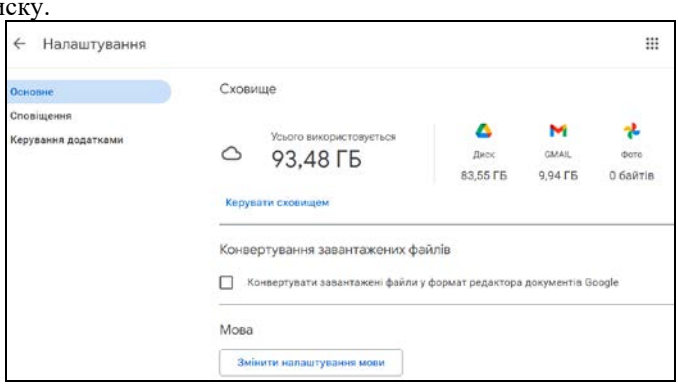

Рис. 5.7. Параметри сервісу Google диск

У межах домену конфігурування параметрів сервісу Google Диск здійснюється за допомогою інтерфейсу адміністратора. Для цього у ньому на сторінці додатків слід обрати гіперпосилання на сервіс *«Диск і документи»*. Нижче наведені параметри можуть бути застосовані до усього домену або до будь-якого його підрозділу. Серед доступних налаштувань сервісу виділимо:

- налаштування спільного доступу;
- параметри переміщення;
- опції керування спільними дисками;
- управління передаванням прав власності;
- параметри доступу до даних, що розміщені на Google Диску;
- опції використання спеціальних шаблонів для організації.

Адміністратор може налаштувати такі режими використання спільного доступу користувачами організації:

- заборона надавати доступ користувачам, які не належать домену (окремо можна дозволити або заборонити отримувати файли від осіб, які не належать організації);
- дозвіл надавати доступ користувачам, які належать наперед визначеному «білому» списку доменів (окремо можна дозволити або заборонити отримувати файли від осіб, які не належать зазначеному списку доменів);
- дозвіл надавати доступ користувачам, які не належать домену.

У останньому випадку можна увімкнути виведення попереджень про надання доступу за межами організації та передбачити необхідність обов'язкової автентифікації сторонніх користувачів. Також можна дозволити корис-

тувачам з організації змінювати налаштування доступу (загальнодоступний режим або для всіх, хто має посилання). Засобом адміністратора сервісу є перевірка доступу, який надано за межами сервісу Google Диск. Наприклад, додаючи посилання в Gmail), система може перевірити, чи мають отримувачі доступ до нього. Якщо доступ, не надано, сервіс запропонує користувачеві надіслати файл:

- усім, кому надано доступ;
- одержувачам та користувачам, які належать організації;
- лише стороннім одержувачам.

Адміністратор має змогу налаштувати за замовчуванням доступ за посиланням. Тобто до всіх об'єктів на дисках у межах організації можуть автоматично надаватися такі параметри доступу за посиланням:

- увімкнено – доступ мають усі користувачі домену;
- увімкнено – доступ мають усі користувачі домену, що мають посилання;
- вимкено – доступ відсутній.

Однією з додаткових можливостей хмарного сховища є спільні диски, які дають змогу зручно зберігати і шукати файли команди, а також відкривати їх з будь-якого пристрою. Файли загального диска належать команді, а не окремому користувачеві. Навіть якщо учасники залишають команду, файли залишаються на місці, тому інші користувачі зможуть і далі працювати зі спільними даними.

Для використання спільних дисків адміністратор хмарного пакету Google Workspace повинен дозволити їх використання. Після цього у меню основних складових сервісу з'явиться відповідне посилання (рис. 5.1, блок 1). Створивши спільний диск, його власник може додати користувачів (Рис. 5.8).

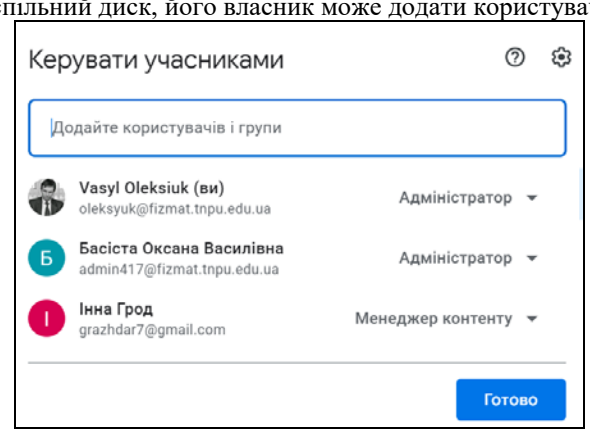

Рис. 5.8 Додавання учасників до спільного диска

Існують такі режими доступу користувачів до спільного диска:

- повний доступ – користувач може керувати учасниками, завантажувати, змінювати та видаляти будь-які файли;
- редагування – користувач може завантажувати та змінювати будь-які файли;
- коментування – користувач може залишати коментарі;
- перегляд – користувач може відкривати та читати файли.

Подібно до основного на спільному диску буде доступним окремий кошик. Користувачами спільних дисків можуть бути облікові записи з-за меж домену. Адміністратор домену має змогу переглядати, змінювати параметри доступу, а також відновлювати стан спільних дисків на певну дату.

Ще однією корисною можливістю є передавання прав власності на диск іншому користувачеві. Попередній власник файлів, як і раніше, матиме доступ до них. Зазначена функція стане у нагоді у випадку видалення користувача, адже дає змогу не втратити створені ним файли.

Серед параметрів доступу до даних виділимо:

- дозвіл на використання офлайного доступу до файлів;
- дозвіл на використання клієнта Google Диска – програми, яка дає змогу працювати з Диском і спільними Дисками, не завантажуючи їх на комп’ютер$
- дозвіл користувачам доступ на до Google Диска за допомогою його API-функцій;
- дозвіл користувачам встановлювати доповнення для Google Документів з магазину доповнень.

Користувачі можуть використовувати спеціальні шаблони організації. Адміністратор визначає категорії та параметри публікування шаблонів (рис. 5.9):

- дозвіл усім створювати шаблони;
- обов'язкове затвердження створених шаблонів адміністратором;
- створення шаблонів лише адміністратором.

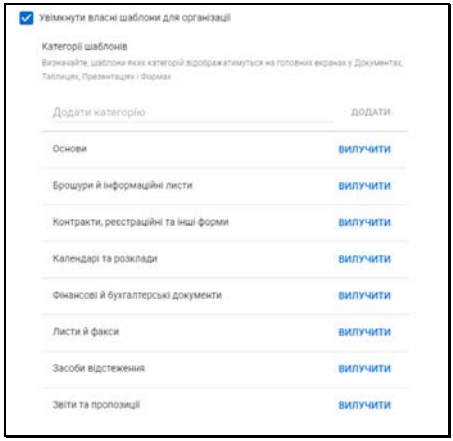

Рис. 5.9. Параметри створення шаблонів сервісу Google Диск

Створюючи новий документ, користувач може обрати шаблон, на основі якого буде створено файл. На сторінці створення документа, можна додати новий шаблон.

6. СЕРВІС GOOGLE CALENDAR

Google Calendar є хмарним сервісом для організації часу та планування виконання подій або завдань. Сервіс є частиною хмарного пакету Google Workspace. Він забезпечує виконання завдань планування на корпоративному рівні. Крім того сервіс є доступним для всіх, хто має особистий обліковий запис Google. Для початку роботи із сервісом слід перейти за посиланням https://calendar.google.com/ або скористатися відповідним пунктом у меню переходу між сервісами (рис. 4.2).

Основними складовими інтерфейсу сервісу є (рис. 6.1):

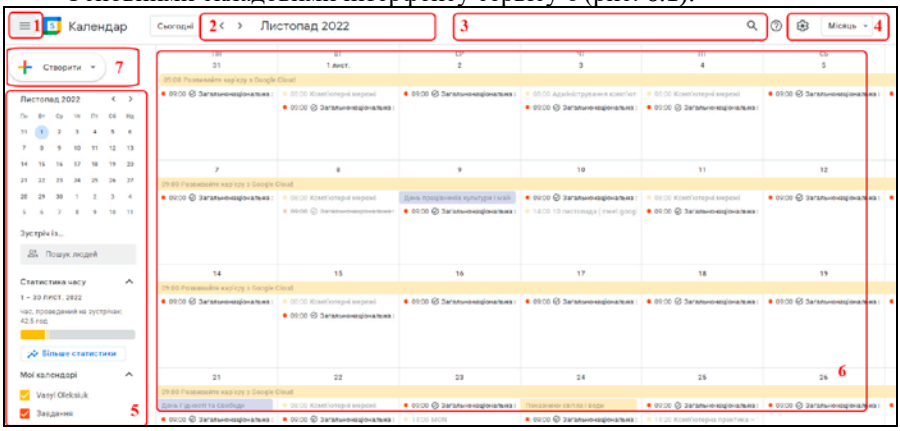

Рис. 6.1. Основні складові інтерфейсу сервісу Google Calendar

1. Гіперпокликання, що використовується для відображення (приховування) списку календарів користувача.
2. Блок навігації за датами.
3. Рядок пошуку подій.
4. Список, який дає змогу змінити відображення календаря (у денному, тижневому або місячному форматі).
5. Список календарів користувача.
6. Робоча область сервісу, що відображає події.
7. Гіперпокликання для додавання подій.

При першій авторизації користувача сервіс пропонує до використання календар, ім'я якого відповідає імені користувача-власника. Загалом у користувача сервісу існує можливість створення значної кількості окремих календарів. Створення календаря здійснюють за допомогою гіперпосилання у вигляді символу «плюс» («+») (блок 5, рис. 6.1). Додаючи новий календар, слід вказати його назву та опис, а також часовий пояс, відносно якого опрацьову-

ватимуться події. Зазначене гіперпосилання також дає змогу переглянути наперед налаштовані «цікаві календарі» (свята, спортивні змагання тощо), використовувати спільні ресурси організації, додати загально доступний календар, вказавши його URL-адресу, або імпортувати календар із файла у форматі iCal або CSV. Остання послуга також містить гіперпосилання для експорту усіх календарів у один файл (рис. 6.2).

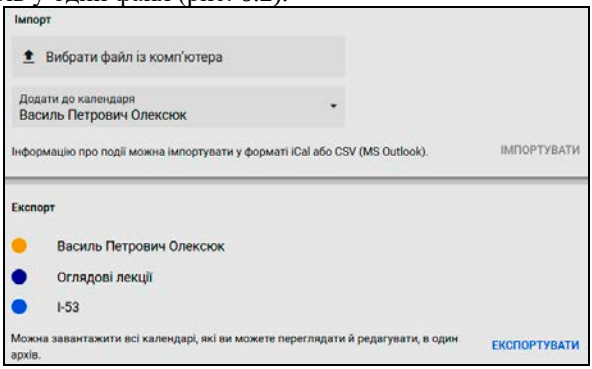

Рис. 6.2. Сторінка імпорту-експорту календарів сервісу Google Calendar

У цьому ж блоці присутній рядок введення, який дає змогу додати календар колеги. Якщо облікові записи обох користувачів належать до однієї організації (одного домену), то доступ до календаря може бути одержаний без будь-яких інших дій (відповідні налаштування можна змінити у панелі адміністратора). У іншому випадку необхідним буде заповнення та надсилання форми із запитом на одержання доступу.

Для створення запису можна обрати у календарі день або час відповідної події. Альтернативним способом є використання гіперпосилання у вигляді круга, що містить символ «плюс». У першому випадку сервіс запропонує обрати тип запису – подія або нагадування. Відмінність між ними полягає у тому, що подія обов'язково створюється у певному календарі та містить додаткові налаштування. Спільними їх параметрами є дата, можливість уточнення часу та періодичності повторення (рис. 7.3).

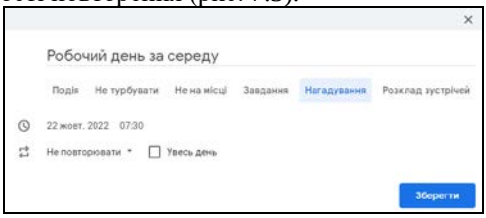

Рис. 6.3. Створення нагадування сервісу Google Calendar

Додавання події за допомогою гіперпосилання у вигляді круга, що містить символ «плюс» (блок 7, рис. 6.1) дає можливість визначити такі її додаткові параметри (рис. 6.4):

- місце проведення події;
- необхідність здійснення відеодзвінка;
- нагадування про подію;
- календар, у якому буде збережено запис;
- статус користувача та видимість події для інших;
- опис;
- перелік запрошених користувачів-гостей.

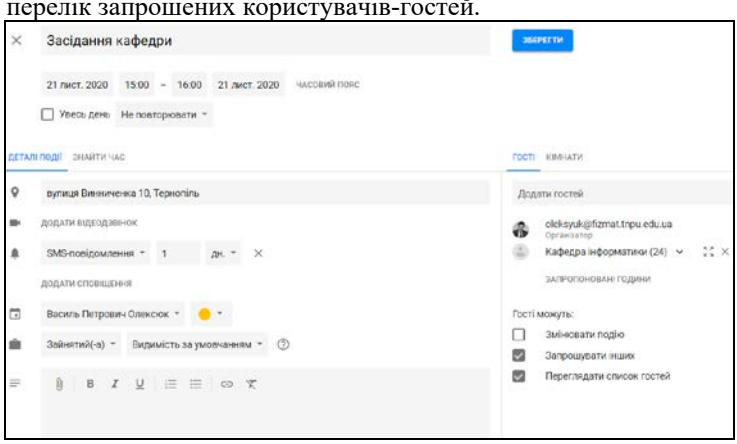

Рис. 6.4. Додаткові параметри події сервісу Google Calendar

Введення місця проведення події можливе з використанням геосервісів компанії Google. Покликання *«Додати відеодзвінок»* дає змогу запланувати та створити відеоконференцію. Важливим додатковим параметром події є нагадування. Загалом залежно від власних потреб користувач може додати чималу їх кількість. Нагадування можуть надходити у формі листа електронної пошти, вікна повідомлень на сторінці сервісу Google Calendar або мобільного додатку. У опис події її власник крім тексту, зображень, гіперпосилань може долучити потрібні файли.

За замовчуванням для події використовуються налаштування доступу відповідного календаря. Тобто відомості про подію бачитимуть усі, хто має доступ до інших подій у цьому календарі. Якщо до календаря не надано жодного доступу, то подія буде доступна лише його власнику.

За допомогою покликання *«Знайти час»* можна узгодити записи, які містяться у різних календарях, та події, до яких власник календаря запрошений

як гість. У такий спосіб користувач може гнучко планувати свій час, уникаючи співпадань у запланованих заходах.

До кожної події можна долучити її учасників (у інтерфейсі сервісу Google Calendar вони називаються гостями). У корпоративному обліковому записі можливе запрошення як окремих користувачів, так і їх груп. Для додавання гостей слід ввести назву або електронну адресу облікового запису. Якщо було запрошено групу користувачів, то при збереженні запису кожному її учаснику буде запропоновано надіслати електронного листа із запрошенням до заходу та можливістю вказати чи погоджується він брати у ній участь. Також існує можливість видалення окремих учасників групи або позначення їх як необов'язкових гостей події. Це можна зробити за допомогою покликання *«Запросити кожного учасника групи індивідуально»*.

Налаштування параметрів окремого календаря його власник може здійснювати, використовуючи контекстне меню. Основними параметрами календарів є (рис. 6.5):

- назва та опис календаря;
- автоматичний прийом запрошень до інших подій;
- права спільного доступу до записів;
- можливість спільного використання календаря;
- налаштування сповіщень про події;
- параметри інтеграції календаря;

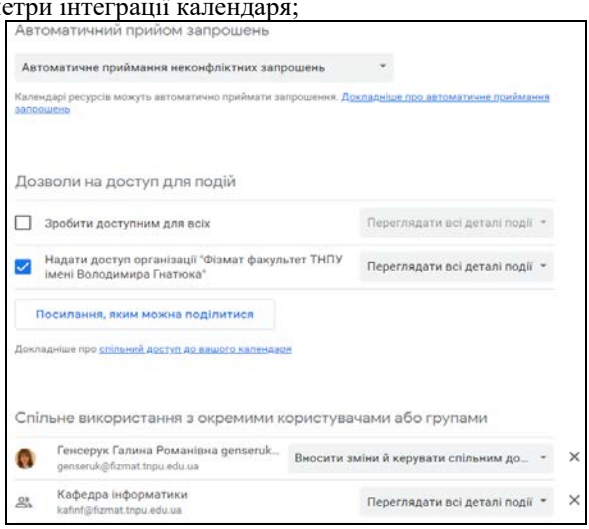

Рис. 6.5. Основні параметри календаря сервісу Google Calendar

Існує можливість налаштувати календар для опрацювання запрошень до подій інших користувачів. Зокрема можна вказати такі параметри:

- автоматичне приймання запрошень, які не конфліктують з іншими записами у календарі;
- автоматичне додавання до календаря подій із запрошень;
- відхилення усіх запрошень.

Зміна прав доступу до календаря дає змогу зробити його загальнодоступним у мережі інтернет. Існує можливість надати доступ лише користувачам організації. Власник календаря визначає дозвіл для перегляду деталей подій або відображення власного статусу зайнятості. Більш детально налаштувати параметри доступу до календаря можна у розділі *«Спільне використання з певними особами»*, де вказують обліковий запис користувача або групи, які зможуть спільно використовувати календар з його власником. Сервіс пропонує такі режими спільного використання календарів:

- перегляд статусу власника (зайнятий або вільний);
- перегляд деталей подій;
- внесення змін до подій;
- внесення змін до подій та управління спільним доступом.

Доступність зазначених режимів залежать від налаштувань, які визначає адміністратор організації.

Налаштування нагадувань в календарі не відрізняються цих параметрів у окремому записі (електронна пошта, інформаційне вікно). Проте можна окремо налаштувати сповіщення для подій, які тривають цілий день. Також можна налаштувати сповіщення про такі зміни у календарі – нові, змінені, скасовані записи, відповіді учасників подій. Існує окремий вид нагадування – електронний лист із порядком денним, який містить усі заплановані на день події.

Інтеграція календаря передбачає доступ до його записів з інших додатків або сервісів. Сервіс Google Calendar пропонує такі параметри інтеграції календарів:

- ідентифікатор календаря, який використовується для доступу у додатках або API-функціях;
- загальнодоступна URL-адреса – буде дійсною у випадку надання відповідного доступу;
- код для вставлення календаря на інші веб-сторінки, який можна персоналізувати або вбудувати декілька календарів;
- прихована адреса у форматі iCalc, використовуючи яку можна отримати доступ до календаря, не роблячи його загальнодоступним.

Серед параметрів календаря доступні гіперпосилання для його вилучення. Також існує можливість скасування підписки, яка відмінить підписку користувача на календар, проте збереже записи про події.

Як було зазначено вище, конфігурування деяких параметрів сервісу Google Calendar здійснюється за допомогою інтерфейсу адміністратора. Для цього у ньому на сторінці додатків слід обрати гіперпосилання на сервіс Календар. Подібно до інших сервісів пакету Google Workspace нижче наведені параметри, які можуть бути застосовані до усього домену або до будь-якого його підрозділу. Серед доступних налаштувань сервісу виділимо:

- налаштування спільного доступу;
- визначення ресурсів, які доступні користувачам у процесі планування подій;
- загальні налаштування;
- управління даними користувачів.

У межах організації (домену) адміністратор може дозволити спільний доступ до усіх календарів, обмежити його лише переглядом статусу зайнятості користувача або взагалі заборонити. За межами домену доступними є такі параметри:

- перегляд відомостей щодо статусу (зайнятий/вільний) користувача;
- доступ для лише для перегляду подій (незареєстровані користувачі не зможуть змінювати записи);
- доступ для зміни подій (незареєстровані користувачі матимуть змогу змінювати записи);
- повний доступ до записів та дозвіл на управління календарями для незареєстрованих в межах організації користувачів.

Додатково можна встановити режим попередження про надання доступу користувачам, за межами організації. У налаштуваннях сервісу можна перебачити автоматичне додавання відеодзвінків до подій, що створюють користувачі домену.

Крім планування заходів у сервісі Google Calendar, користувачі Google Workspace в організації можуть резервувати ресурси загального користування. Насамперед це стосується приміщень (аудиторій, конференцзалів), але резервувати можна й інші об'єкти, такі як обладнання, спорядження тощо.

Для створення ресурсу потрібно у інтерфейсі адміністратора, на сторінці сервісу Google Calendar, відкрити розділ *«Ресурси»* та перейти за круглим гіперпосиланням, яке містить символ «+». На сторінці, яка завантажиться заповнюють такі поля (рис. 6.6):

- тип ресурсу – нині доступні такі типи: конференц-зал (приміщення для проведення навчання, переговорів), інше (матеріальні засоби, обладнання, транспорт);
- будівля, де буде відбуватися захід, (потрібно створити заздалегідь);
- назва ресурсу;
- функції, доступні користувачам заходу, (потрібно створити заздалегідь);

- опис, який бачитимуть користувачі, які будуть додавати ресурс до власного календаря.

Ресурси краще створювати дотримуючись ієрархічного принципу, наприклад, такого: Організація – Будівля – Приміщення–…

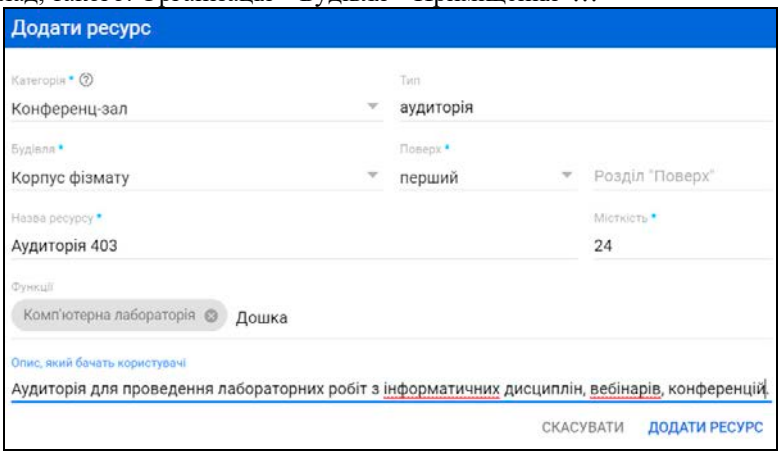

Рис. 6.6. Створення ресурсів календаря сервісу Google Calendar

Змінення полів, що містять дані про ресурс, такий як будівля, поверх або місткість, впливає на створювані назви ресурсів і пошук приміщень. Перед додаванням ресурсів адміністратору доречно створити вище згадані об'єкти: будівлі та функції. Вони будуть використовуватися як поля ресурсів. Додавання об'єкту типу будівля здійснюють на сторінці ресурсу (рис. 6.7).

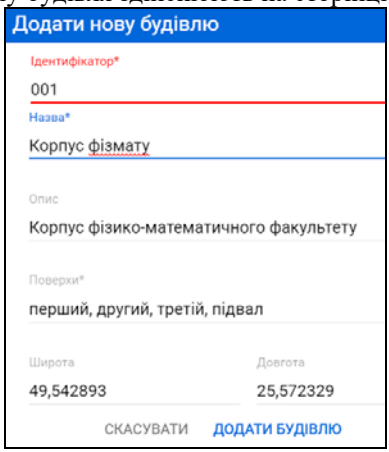

Рис. 6.7. Створення ресурсів календаря сервісу Google Calendar

Аналогічно додають об'єкти, які визначають функціонал ресурсів. Наприклад, функціями можуть бути наявність комп'ютерів, дошки, доступу до мережі інтернет тощо. У інтерфейсі передбачено конкретизацію типу функції, проте поки що реалізовано їх лише два – відео- та аудіозв'язок. Якщо існує потреба у додаванні багатьох ресурсів чи будівель, їх можна імпортувати, підготувавши таблицю у форматі csv. Аналогічно на сторінці ресурсів існує можливість їх масового завантаження на комп'ютер адміністратора.

Додавання ресурсу на сторінці сервісу здійснюють у списку календарів користувача (блок 5, рис. 6.1), обравши пункт меню *«Перегляд ресурсів»*. На сторінці, що завантажиться, у переліку будівель можна обрати потрібний ресурс (рис. 6.7).

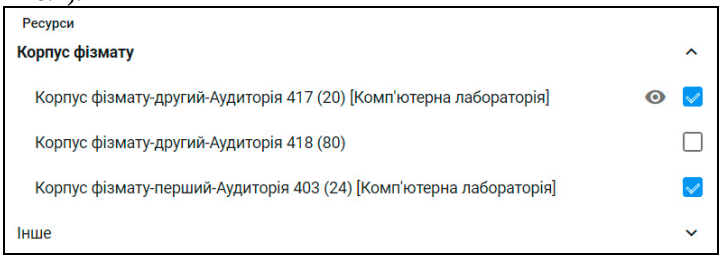

Рис. 6.7. Створення ресурсів календаря сервісу Google Calendar

Варто зауважити, що після додавання ресурсу він буде доступний користувачів не відразу (затримка може тривати до 24 годин). Після додавання користувачі матимуть змогу резервувати ресурси, не турбуючись про те, що хтось із них припуститься помилки і на одне і те ж приміщення претендуватимуть одразу кілька осіб. На сторінці додаткових параметрів події з будь якого календаря буде доступним покликання *«Кімнати»*, яке забезпечує можливість переглянути перелік доступних ресурсів. Сервіс сформує список тільки вільних у даний момент ресурсів, а користувач зможе зарезервувати потрібний ресурс, щоб у певний момент скористатися ним.

Якщо для нового ресурсу не задані правила доступу, він успадкує параметри загального доступу за замовчуванням, встановлені для календарів організації. Аналогічно до налаштування календаря, у параметрах ресурсу, користувач може налаштувати повідомлення, які надійдуть у таких випадках:

- ресурс задіяний у новій події;
- захід змінено або скасовано;
- користувачі прийняли запрошення до події .

Додатково для ресурсу можна налаштувати формування порядку денного його використання усіма користувачами.

У розділі *«Налаштування спільного доступу»* присутні параметри надання доступу до додаткових календарів стороннім користувачам та тим, які

належать організації. Додатковими календарями є і створені адміністратором ресурси. Аналогічно до основних календарів користувачів можливі такі рівні доступу: перегляд деталей подій або відомостей про статус зайнятості, внесення змін до записів та дозвіл на управління додатковими календарями. У цьому ж розділі адміністратор може дозволити користувачам резервувати ресурси, для яких вибрано параметр доступу *«Переглядати лише інформацію щодо статусу (вільний/зайнятий)»*. Суперадміністратор має повноваження для резервування будь-якого ресурсу організації незалежно від параметрів доступу до нього.

У розділі *«Передача подій»* доступні скасування усіх майбутніх події користувача або передання право власності його календарів іншому користувачі (рис. 6.8). Зазначену функцію доцільно використовувати у випадку призупинення облікового запису користувача для того, щоб важливі події не залишалися без власника, а ресурси календаря не блокувалися.

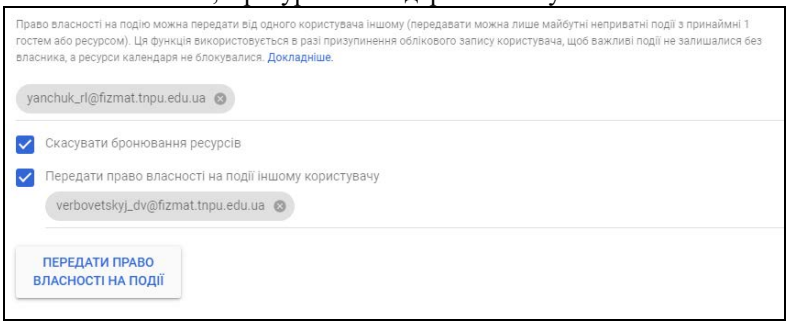

Рис. 6.8. Зміна власника календарів користувача

Також у цьому розділі можна скасувати заплановані події усіх видалених користувачів домену. Якщо в організації існує позитивне ставлення до новацій, то адміністратор може увімкнути для користувачів експериментальні опції сервісу та визначити спосіб переходу на його нові версії.

Подібно до інших хмарних сервісів пакету Google Workspace Google Calendar є доступним на мобільних пристроях. Це робить його потужним засобом організації урочної та позаурочної навчальної діяльності, оповіщення батьків про події школи, а також добрим інструментом для організації проєктної роботи.

7. СЕРВІС GOOGLE CLASSROOM

Google Classroom – це хмарний сервіс для підтримки змішаного навчання. У сучасній педагогіці такий підхід передбачає поєднання традиційних методів очного навчання із широким застосуванням навчальних матеріалів у мережі інтернет. Використання сервісу дає змогу спростити процеси створення, публікування навчальних ресурсів та завдань, а також оцінювання рівня навчальних досягнень учнів. Подібно до інших хмарних сервісів, збереження даних учасників освітнього процесу відбувається у інфраструктурі провайдера. Це дає можливість одержувати доступ до них у будь-який час і з будь-якого пристрою, з подальшим збереженням на пристрій користувача, а також роботою з даними у «хмарі». Сервіс є частиною хмарного пакету Google Workspace for Education. Серед переваг сервісу можна виділити:

- інтуїтивно зрозумілий процес створення курсів, навчальних матеріалів та завдань;
- зручність планування навчального процесу – учні та вчителів можуть переглядати завдання у календарі курсу або на сторінці *«Список справ»*;
- розширені засоби комунікації, які дають змогу викладачам публікувати завдання, розсилати оголошення починати їх обговорення, а учням – обмінюватися матеріалами, додавати коментарі в стрічці курсу і спілкуватися через електронну пошту.
- інтеграція з популярними сервісами – Google Диском, Документами, Календарем, Формами тощо.
- доступність і безпека – Classroom є безкоштовним сервісом, не містить реклами, а матеріали і дані учнів не використовуються в маркетингових цілях.

Робота з сервісом можлива через браузер або через мобільні додатки для платформ Android чи iOS. Для початку роботи із сервісом слід перейти за посиланням https://classroom.google.com/ або скористатися відповідним пунктом у меню переходу між сервісами. Для автентифікації можна використовувати особистий або корпоративний обліковий запис. Останній традиційно пропонує кращу інтеграцію в межах освітнього закладу, через використання спільного каталогу, груп користувачів, додаткових адміністративних налаштувань. Після автентифікації користувача буде перенаправлено на сторінку *«Заняття»*, яка містить доступні для нього курси (рис. 7.1).

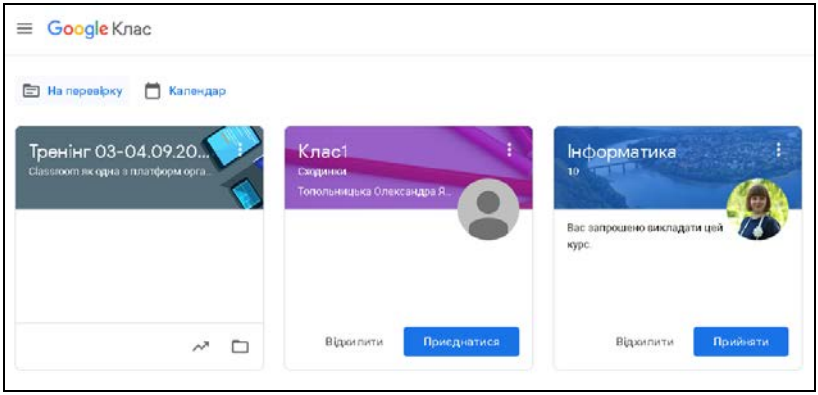

Рис. 7.1 Сторінка курсів користувача

Слід зауважити, що зазначена сторінка може містити курси, у яких користувач виконує роль викладача або ж такі, до яких він може приєднатися як учень. У останньому випадку біля курсу можна побачити відповідне посилання у вигляді кнопки *«Прийняти»*.

При першому вході до сервісу Google Classroom користувач може вказати чи він є викладачем чи слухачем (учасником). Облікові записи викладачі додаються до відповідної групи

Адміністратор Google Workspace for Education повинен підтвердити облікові записи викладачів, та налаштовує потрібні дозволи для них на рівні домену (організації). Користувачі, які не є викладачами, не можуть створювати нові курси. Для підтверджених викладачів доступна контактна інформація про облікові записи батьків чи представників (опікунів).

Для навігації між курсами слугує меню, яке знаходиться у лівому верхньому куті сторінки. Як видно з рисунка меню дає можливість переглянути спільний календар подій у всіх курсах. Розділ *«Викладає»* містить специфічні для викладача пункти:

- «невиконані» − види діяльності, які вимагають уваги викладача, наприклад, завдання, які потребують оцінювання;
- перелік курсів, у яких користувачеві надано роль викладача (на рис.7.2 це курс «10 Клас, Інформатика»);
- архівовані курси.

Пункт налаштування містить кілька опцій, які стосуються отримання сповіщень електронною поштою про події в курсах. Такими подіями є коментарі, повторно чи запізно здані на оцінювання завдання учнів, заплановані зміни статусів у публікуванні навчальних матеріалів. Також на сторінці на-

лаштувань можна увімкнути або вимкнути сповіщення електронною поштою або у мобільних додатках для окремих курсів викладача.

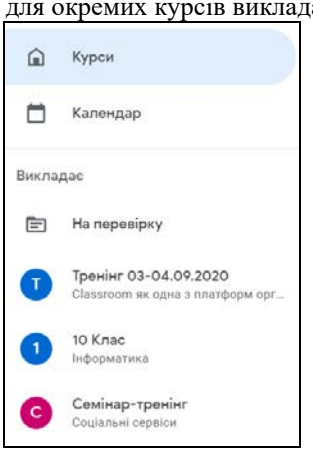

Рис. 7.2 Меню курсу

За допомогою кнопки «+» у верхній частині сторінки курсів можна приєднатися до існуючого курсу або створити власний (рис. 7.1). Для створення курсу слід ввести його назву, опис, клас, який вивчатиме дисципліну (рис. 7.3).

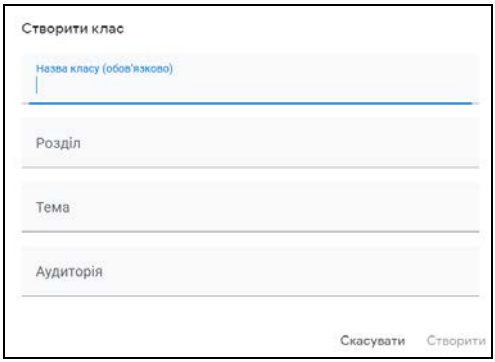

Рис. 7.3 Створення нового курсу

Слід зауважити, що розробники сервісу Classroom під курсом зазвичай розуміють клас, як сукупність учнів, які вивчають певну дисципліну. Отож, при створені у поле «*Назва класу*» доцільним вважаємо введення назви дисципліни.

Кожному класу система автоматично присвоює унікальний ідентифікатор, що містить літери та цифри. Одним із способів масового приєднання учнів до курсу є повідомлення їм цього коду. Слід зауважити, що цей спосіб не є безпечним, оскільки за ним до курсу можуть приєднатися сторонні особи.

У верхній частині сторінки курсу бачимо чотири гіперпосилання у вигляді закладок (рис. 7.4):

- потік – відображає хід навчального процесу (навчальні матеріали, завдання, події);
- завдання – містить основні складники курсу, зокрема навчальні матеріали, безпосередньо завдання, тести тощо.
- люди – дає змогу запросити до курсу викладачів та студентів – для цього слід ввести адресу кожного нового учасника або групи;
- оцінки – містить відомості про курс, а також дозволяє їх змінити.

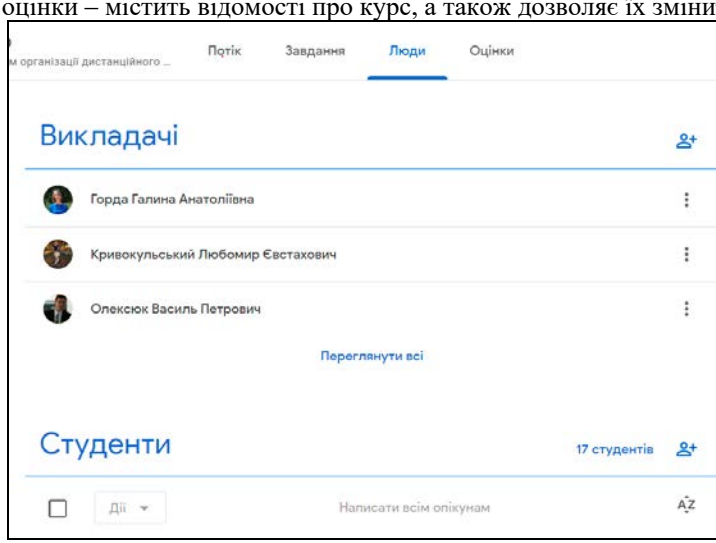

Рис. 7.4 Учасники курсу Google Classroom

Використовуючи групи Google Workspace, на вкладці «Студенти», можна одночасного запросити усіх учнів класу. Для цього у полі запрошення слід ввести електронну адресу групи. Після цього кожному члену групи буде надіслано листа із запрошенням до участі в курсі. На зазначеній сторінці прізвища студентів, які не прийняли запрошення будуть виділені більш світлим кольором (рис. 7.4). Виділяючи користувачів на вкладці «Студенти», адміністратор може видалити їх з курсу або скасувати надіслане запрошення. Адмі-

ністратору або учителю також доступна сторінка, що відображає результати діяльності студента в усіх курсах (рис. 7.5).

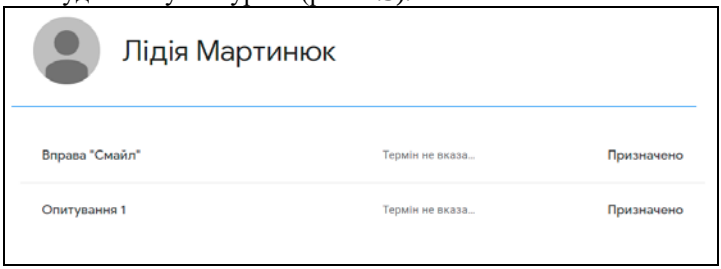

Рис. 7.5 Результати навчальної діяльності студента у всіх курсах

Адміністратор, який створив курс, може створювати завдання та пропонувати їх до виконання усім або студентам. На вкладці «Інформація» адміністратор може запросити викладачів курсу. Курси, у яких ще немає вчителів, знаходяться в резервному стані.

Запрошуючи викладачів до курсу, слід враховувати:

- видалити курс може тільки основний викладач;
- основного викладача не можна видалити з курсу, і він не може видалити сам себе;
- список викладачів, що приєдналися до курсу, не можна приховати;
- папка курсу на Google Диску належить основному викладачеві;
- після того, як новий вчитель приєднається до курсу, він отримає доступ до спільної папки курсу на Google Диску.

Після завершення вивчення курсу викладач, щоб зберегти матеріали, завдання та коментарі до них, може помістити курси в архів. Після цього курс не буде доступним для студентів. Заархівований курс є доступним в розділі «*Архіви курсів*». Після відновлення курс знову з'явиться в списку активних, і вчитель зможе вносити в нього зміни. Курси, які не були архівованими все ще будуть відображаються для учнів як активні.

Сторінка курсу сервісу Google Classroom має вигляд як на рис. 7.6. Опитування і завдання учнів можна відстежувати в календарі курсу. Після створення курсу його учні отримують доступ до календаря класу, у якому вони бачать свої завдання і терміни їх виконання. Також до календаря учитель може додавати заходи, наприклад консультації, контрольні роботи, екскурсії тощо. Адміністратор Google Classroom може відключити календар курсу для окремого облікового запису.

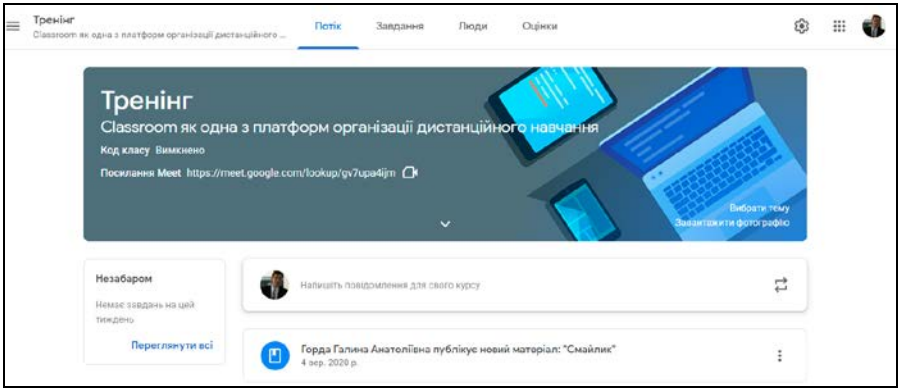

Рис. 7.6 Головна сторінка курсу Google Classroom

Події курсу можна відстежувати у відповідному календарі. Після створення курсу його учні отримують доступ до календаря класу, у якому вони бачать свої завдання і терміни їх виконання. Також до календаря учитель може додавати заходи, наприклад консультації, контрольні роботи, екскурсії тощо. Створені викладачем завдання разом із термінами їх виконання додаються до календаря курсу. Учитель та учні можуть переглядати події курсів на сервісах Google Classroom (рис. 7.7) та Google Календар.

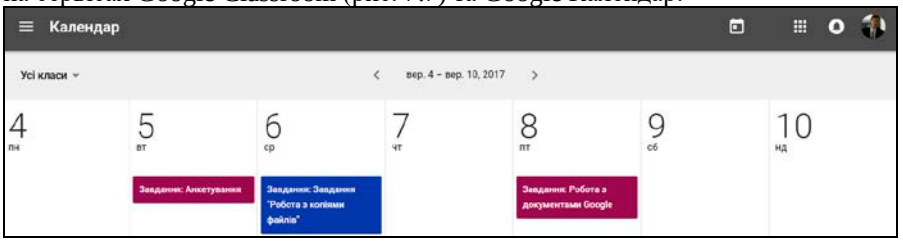

Рис. 7.7 Календар курсів Google Classroom

На вкладці «*Потік*» учасники курсу можуть обмінюватися новинами, враженнями та іншою інформацією (рис. 7.8). Учням доступне коментування повідомлень викладача. У процесі публікування повідомлення викладач може обрати студентів, яким воно має бути адресоване. Також сервіс дозволяє планувати час публікування повідомлень та інших навчальних ресурсів.

Рис. 7.8 Додавання повідомлення (оголошення) у курсі Google Classroom

Для створення або додавання навчальних ресурсів слід перейти на вкладку «*Завдання*» та обрати гіперпосилання «+ Створити» . У завантаженому меню слід обрати тип ресурсу, який буде створено (рис. 7.9).

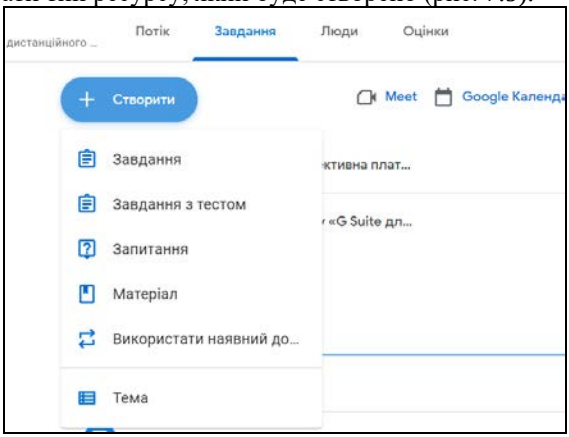

Рис. 7.9 Меню додавання навчальних ресурсів

Нині основними ресурсами, які доступні у Google-класах є такі:

- тема – дає можливість структурувати навчальний матеріал за розділами (темами);
- матеріал – є основним ресурсом курсу, який може містити документи, презентації, таблиці, форми, а також гіперпосилання, файли з локального диска або Google Диска, відеоролики з сервісу YouTube тощо. При створенні ресурсу вчитель має можливість обрати курс (клас), його учасників та тему, в якій буде опублікований матеріал (рис. 7.10). При створенні ресурсу вчитель має можливість обрати

курс (клас), його учасників та тему, в якій буде опублікований матеріал.

Рис. 7.10 Сторінка додавання навчального матеріалу

- завдання –передбачає надсилання студентом відповіді у форматі повідомлення або файла. Крім вище зазначених параметрів учитель повинен вказати максимальну кількість балів, якими буде оцінено виконання завдання (рис. 7.11);

Рис. 7.11 Сторінка додавання завдання

- завдання з тестом – дає можливість створити тест за допомогою сервісу Форми. Додатковим параметром цього засобу є можливість імпорту оцінок з тесту до журналу курсу. Зазначений параметр автоматично обмежує кожну форму до однієї відповіді студента, збирає їх електронні адреси та приймає відповіді лише від користувачів організації (для Google Workspace).
- наявний допис – дає можливість використати існуючий ресурс або створити його копію; варто зауважити, що за допомогою зазначеної послуги можна копіювати навчальні ресурси з інших курсів;
- запитання – дає змогу створити відкрите (з короткими відповідями) або закрите (з варіантами відповіді) запитання. У випадку використ-

тання коротких відповідей додатковими параметрами є опції редагування учнями власних дописів та можливість надсилання коментування робіт інших учасників (рис. 7.12);

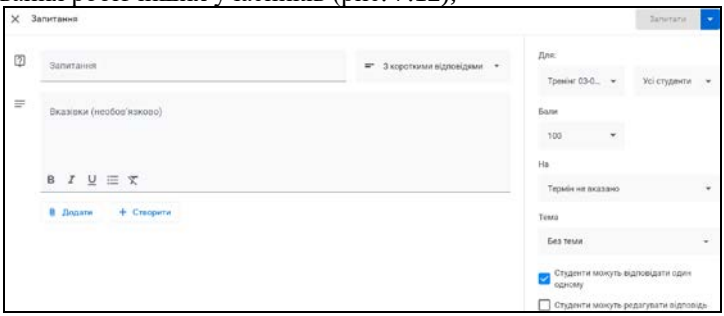

Рис. 7.12 Сторінка створення запитання

Усі з вищенаведених типів навчальних ресурсів можуть бути призначені до виконання як усіма, так і окремими студентами класу.

Використання завдання як складника курсу у сервісі Google Classroom передбачає виконання учасниками освітнього процесу деяких дій:

1. Викладач створює завдання і прикріплює файли. Він може призначити завдання одному або декільком курсам, а також усім або окремим учням. Крім того, можна вказати термін виконання роботи, до завершення якого, викладач має змогу відстежувати статус виконання, додавати коментарі і вносити зміни у документи.
2. Учень завантажує як відповідь власні матеріали або редагує файли та надсилає їх на перевірку. До роботи учень може прикріплювати файли, посилання і зображення. Виконавши завдання, учень повинен надіслати його. До закінчення встановленого терміну він може скасовувати надсилання завдання, вносити зміни й повторно надсилати відповідь.
3. Викладач оцінює відповідь. Він може додати до завдання коментар, виставити оцінку або повернути його учневі на доопрацювання
4. Учень бачить коментар викладача та оцінку й має можливість редагувати відповідь. Якщо до роботи викладачем прикріплений файл, учень, при необхідності, має можливість знову внести зміни до нього.

Перш ніж створити завдання, викладач повинен налаштувати параметри доступу до файлів, які містяться у ньому. Додаючи файл з диска (наприклад, документ, презентацію або таблицю), викладач має змогу:

- дозволити учням відкривати файл – у цьому випадку учні зможуть лише переглядати документ;
- дозволити учням редагувати файл – у цьому випадку учні зможуть вносити зміни в документ;

- створити копію для кожного учня – у цьому випадку кожен учень отримає власну копію документа для редагування; ім'я учня буде додано до назви документа, викладач отримає окремий файл з відповідним іменем.

Нині проведення тестування у сервісі Google Classroom можливе з певними обмеженнями. Для використання тесту у курсі вчитель має додати завдання. Для створення запитань викладачеві слід використовувати зовнішні сервіси, найбільш функціональним та інтегрованим з яких вважаємо Google Форми. Крім додавання форм безпосередньо у курсі можна використати меню сервісів або створити її на сервісі Google Диск.

Інтерфейс Google Форми містить такі складники (рис. 7.13):

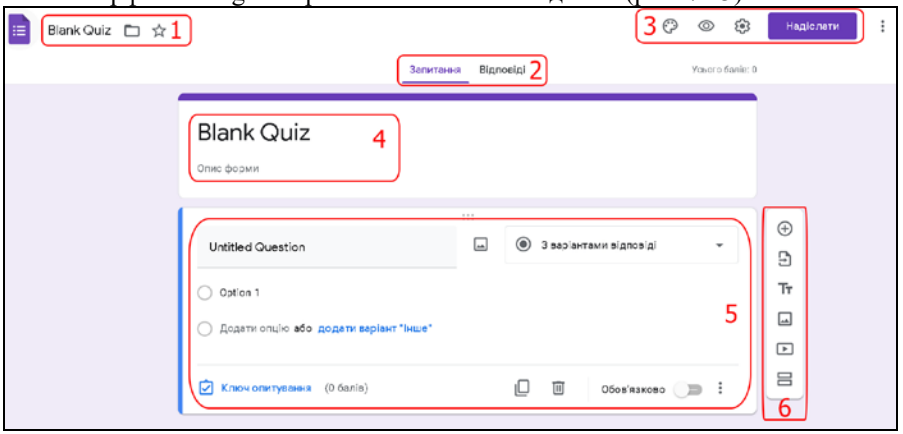

Рис. 7.13 Інтерфейс сервісу Google форми

1. Меню, за допомогою якого можна змінити назву форми, перенести її до іншої папки на Google Диску та додати до обраних (помітити зірочкою);
2. Вкладки, які перемикають режими редагування форми та перегляду результатів опитування.
3. Кнопки конфігурування – дають змогу долучити додатки до форми, змінити її оформлення, перейти в режим перегляду, налаштувати параметри, надати доступ до форми для респондентів.
4. Поле для введення назви та опису форми.
5. Поле введення змісту запитання.
6. Панель інструментів, які дають змогу додати нове запитання, його опис, а також вставити у нього зображення або відео.

Використовуючи сервіс Google Форми, викладач може створити різні типи запитань: з одним або кількома правильними варіантами відповіді, відк-

риті запитання з короткими або розгорнутими відповідями, завдання, що вимагають надсилання файла. Зазвичай, при використанні запитань, які вимагають введення відповіді, оцінювання може здійснюватися сервісом або учителем. Google Форми дають змогу використовувати й інші типи запитань: лінійна шкала, таблиця з варіантами відповідей, «сітка відповідей», запитання на введення дати й часу. Зауважимо, що оцінювання зазначених типів запитань можливе лише викладачем. Розглянемо параметри основних типів запитань.

Для того, щоб використовувати Google Форми в режимі тестування слід за допомогою кнопки зміни параметрів увімкнути відповідний режим (рис. 7.14).

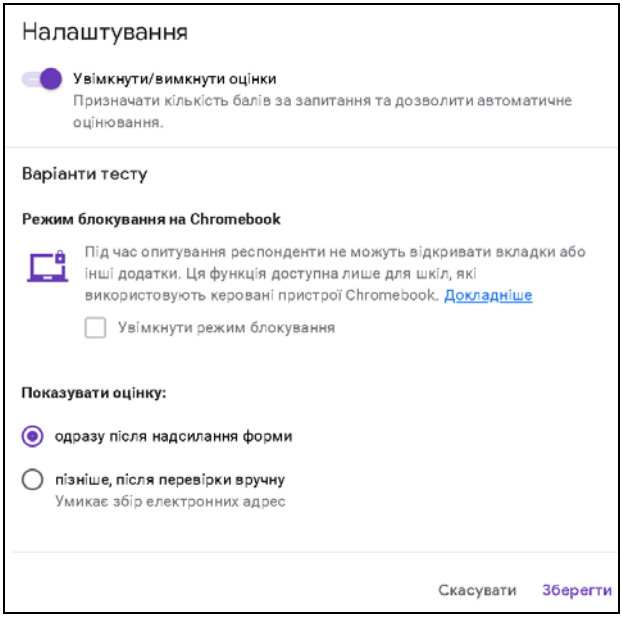

Рис. 7.14 Увімкнення режиму тестування в сервісі Google Форми

Як видно з рисунка викладач може дозволити перегляд оцінки учнем одразу після надсилання форми (тесту) або після того, як викладач перевірить тест вручну. У останньому випадку учневі буде запропоновано ввести свою електронну адресу. Варто зауважити, що на сьогоднішній день між сервісами Google Форми та Classroom немає достатньої інтегрованості стосовно контенту та роботи з обліковими записами користувачів. Наприклад, учень, який зареєструвався на сервісі Classroom може ввести іншу електронну адресу на сторінці тесту, який створено за допомогою Google Форми. Додатково у

вікні налаштувань тесту можна вказати:

- обов’язкове введення та збирання електронних адрес учнів;
- сповіщення викладача про завершення тестування кожним учнем;
- лише одну спробу виконання тесту;
- дозвіл учня редагувати відповіді пісня надсилання тесту;
- можливість перегляду учнями відкриті відповіді та підсумкові діаграми, які стосуються усього класу;
- відображення для учня правильних та неправильних відповідей;
- виведення кількості балів за кожне запитання.

Створення запитання з одним правильним варіантом відповіді (рис. 7.15) передбачає введення його тексту, варіантів відповіді.

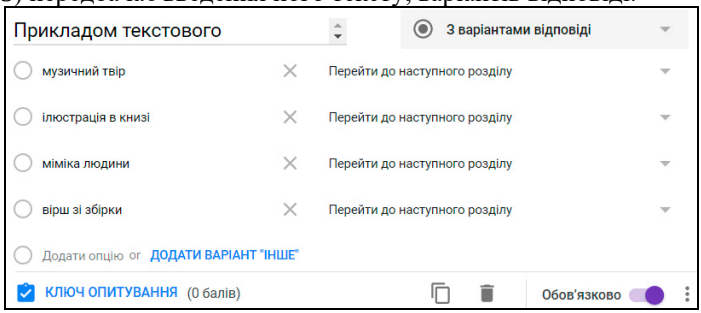

Рис. 7.15 Запитання з одним правильним варіантом відповіді

До самого запитання та кожного варіанта відповіді можна додати зображення. Використовуючи зазначений тип запитань, викладач може додати варіант відповіді з назвою «інше». Учень, обравши такий варіант, матиме змогу ввести власну відповідь. У цьому випадку оцінювання має здійснюватися викладачем в ручному режимі. Після варіантів відповіді, у нижній частині блоку введення запитання, розміщені елементи керування, які дають змогу скопіювати, видалити або встановити запитання обов'язковим. У правому нижньому куті розміщене гіперпосилання у вигляді трьох вертикальних крапок, за допомогою якого можна додати опис запитання, перемішати варіанти відповіді та перейти до іншого розділу тестів залежно від вибору варіанта відповіді.

Після введення запитання за допомогою гіперпосилання *«Ключ опитування»* вчитель має змогу вказати правильний варіант та кількість балів, яка буде нарахована за правильну відповідь. Зауважимо, що для цього типу запитань викладач, має змогу встановити кілька правильних варіантів, хоча учень зможе обрати лише один варіант. Якщо слід обмежити таку можливість, то варто обрати тип подібний запитання, який у сервісі Google Форми називається *«Спадний список»*.

Створення запитання з кількома правильними варіантами (рис. 7.16) передбачає введення його тексту, варіантів відповіді.

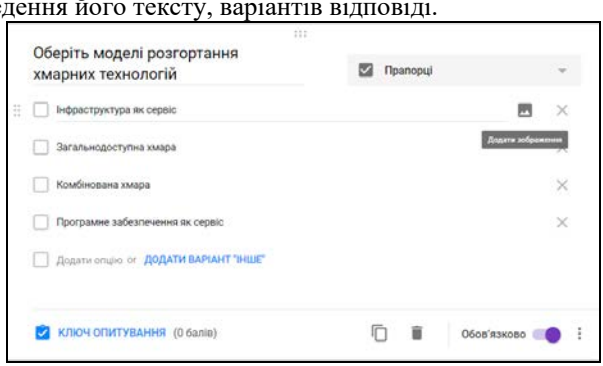

Рис. 7.16 Запитання з кількома правильними варіантами відповіді

До особливих параметрів цього виду запитань належить мінімальна кількість варіантів відповіді, яку повинен обрати учень. Також викладачеві слід врахувати, що бал за правильну відповідь буде нараховано випадку правильного вибору учнем усіх визначених варіантів й відсутності обраних неправильних варіантів.

Відкрите запитання може бути створене у сервісі Google Форми за допомогою запитань з короткими відповідями або таких, які передбачають введення абзацу тексту. Додаючи відкрите запитання, викладач у параметрі *«Перевірка відповіді»* може визначити формат введених учнем даних (рис. 7.17).

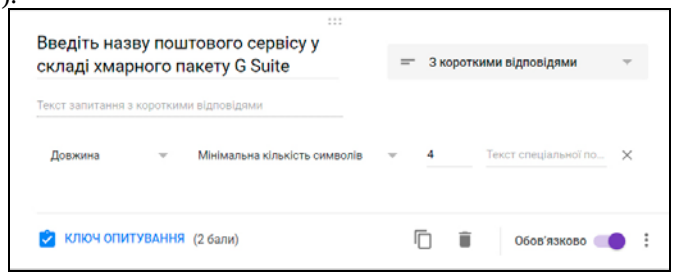

Рис. 7.17 Відкрите запитання з короткими відповідями

Наприклад, якщо відповідь вимагає введення числових даних , можна встановити правила його перевірки, якщо слід ввести текст, можна перевірити його довжину або присутність або відсутність у ньому певних слів.

Використовуючи запитання з короткою відповіддю, слід розуміти, що оцінювання буде здійснено на основі порівняння двох рядків, а сервіс Google

Форми не дає змоги визначити кілька можливих варіантів введеної учнем відповіді.

Вчитель може спілкуватися з учнями віртуального класу, використовуючи оголошення, або, надсилаючи індивідуальні повідомлення зі сторінки учасників курсу. Також у кожному класі існує можливість проводити відеозустрічі. Їх можна запланувати з різних сервісів, зокрема Google Classroom, Meet, Календар та Gmail. Посилання на відеозустріч доступне у параметрах курсу та відображається на його головній сторінці. Викладач може вимкнути зазначену опцію. При інтегрованому використанні сервісів Google Meet, Classroom та Календар викладачеві варто враховувати такі обмеження та особливості:

- Кількість учасників відеозустрічі є обмеженою та залежить від обраного тарифного плану у підписці Google Workspace. Зокрема, для найпопулярнішого, безкоштовного плану Google Workspace for Education Fundamentals максимальна кількість учасників однієї відеозустрічі дорівнює 100.
- Організатором відеозустрічі у класі (курсі) є перший учасник або викладач, що перейшов за її посиланням на відеореєстрацію. Стосовно учнів ця особливість буде діяти і якщо учень просто перейшов не сторінку відеозустрічі, навіть якщо він не приєднався до неї першим.
- Організатором відеозустрічі, яка створена у сервісі Google Календар є той користувач, що її створив. У цьому випадку неважливо, хто першим приєднається до неї.
- Учень може записати відеозустріч, навіть якщо для нього сервіс Google Meet є вимкненим. Проте адміністратор може вимкнути відповідний параметр через сервіс Google Admin (рис. 7.18).

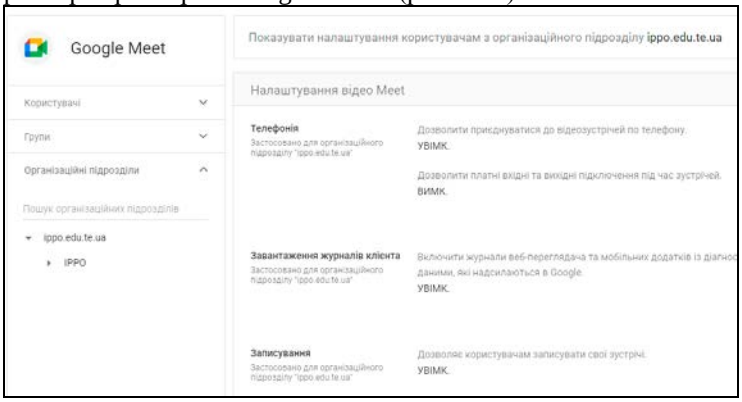

Рис. 7.18 Параметр дозволу записування відеозустрічей

Однією з цікавих можливостей сервісу Google Classroom є інформування батьків учня або інших відповідальних осіб (кураторів, опікунів) про його діяльність у курсі. Кураторів можна додати тільки для учнів, які використовують Google Classroom в корпоративному обліковому записі Google Workspace для освіти. Прийнявши запрошення, куратор учня отримує повідомлення про невиконані роботи, найближчі терміни виконання навчальних завдань, а також оголошення та новини курсів. Зауважимо, що куратор отримуватиме повідомлення з усіх курсів, у яких зареєстрований його учень.

На рисунку 7.19 наведено приклад повідомлення про необхідність виконання завдання:

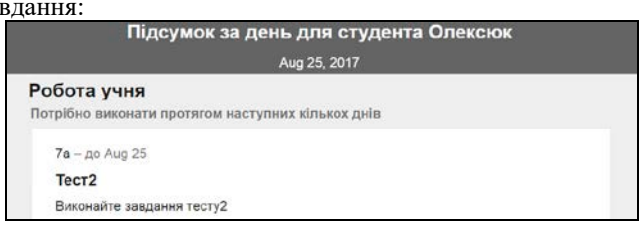

Рис. 7.19 Повідомлення куратору про події в курсі

Для того, щоб використовувати зазначену можливість адміністратору корпоративного облікового запису Google Workspace слід увімкнути відповідний параметр. Для цього у консолі адміністратора у розділі «Додатки» слід перейти до сервісу Google Classroom, у загальних налаштуваннях якого дозволити батькам та опікунам переглядати дані в електронних курсах (Рис. 7.20).

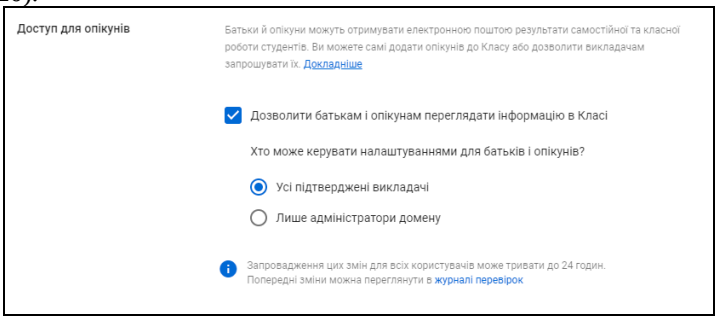

Рис. 7.20 Увімкнення доступу кураторів до курсів сервісу Google Classroom

Для додавання батьків викладачу на вкладці «*Люди*» слід обрати обліковий запис учня та перейти за гіперпосиланням «*Запросити опікунів*». Також на цій сторінці можна вказати параметр, який задіює формування та над-

силання електронних зведень (звітів) батькам та кураторам щодо курсу (рис. 7.21).

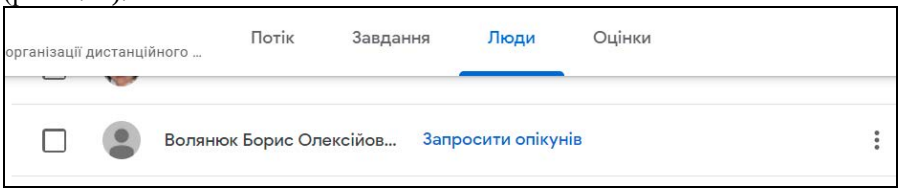

Рис. 7.21 Запрошення батьків або опікунів учасників курсу

Під час додавання облікового запису опікуна викладач може увімкнути опцію надсилання батькам зведених даних про навчання підопічних і оголошення курсу. Крім того викладач може додати всі курси, на яких він чи вона викладає, до надсилання підсумків електронною поштою.

Після цього на вказану адресу буде надіслано листа із запрошенням стати куратором учня (рис. 7.22). Зауважимо, щоб прийняти запрошення, батькам не потрібен обліковий запис Google.

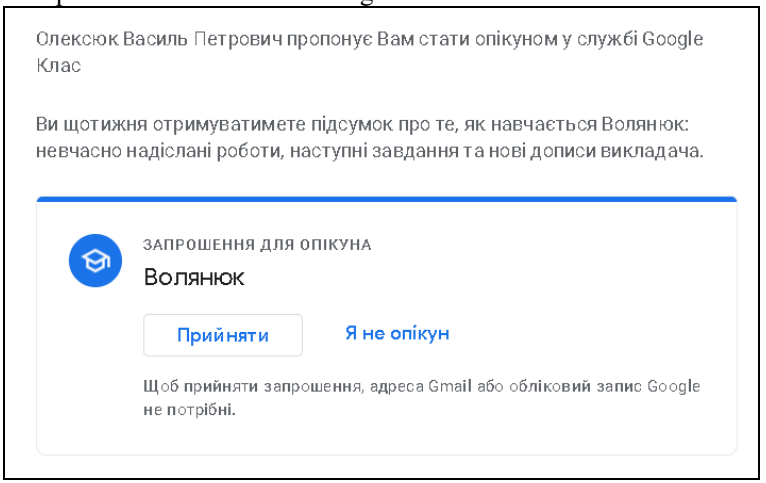

Рис. 7.22 Лист із запрошенням стати куратором

Якщо користувач приймете запрошення стати куратором, то його контактна інформація буде доступною відповідному учневі, викладачам усіх курсів, у яких навчається останній, адміністраторам домену, а також (додаткам) сервісам , які дозволено використовувати з сервісом Classroom. У таблиці 7.1 наведено перелік даних, які є доступними для перегляду користувачам курсів.

Таблиця 7.1 Доступ до персональних даних учасників курсу

Роль	Дані, доступні для перегляду
Учень	Учасники курсу переглядають ім'я, фото та адресу електронної пошти. Інші учасники курсу переглядають ім'я та фото. Якщо адміністратор Google Workspace включає спільне використання контактів, інші учасники переглядають адресу електронної пошти. Представники (батьки або куратори) переглядають ім'я та фото. Адміністратори Google Workspace або домену переглядають ім'я, фото та адресу електронної пошти.
Викладач	Адміністратори Google Workspace або домена, мають доступ для перегляду ім'я, фото та адреси електронної пошти викладача. Інші викладачі курсу переглядають ім'я, фотографію та адресу електронної пошти. Інші учні мають доступ для перегляду імені та фото. Представники учнів (батьки чи опікуни) переглядають ім'я. Користувачі, які отримують доступ до курсору, бачать у запрошенні ім'я та адресу електронної пошти викладача. Якщо адміністратор Google Workspace увімкнув спільне використання контактів, учасники будуть переглядати електронну адресу у інших службах Google, наприклад Документи та Gmail. Якщо викладач надав доступ до курсу стороннім додаткам, то у них також буде доступною контактній інформація викладача.
Представник учня (лише для Google Workspace for Education)	Викладачі курсу і інші викладачі учня переглядають ім'я та адресу електронної пошти представника. Учень бачить лише куратора. Адміністратори Google Workspace мають доступ для перегляду імені, фото та адреси електронної пошти.

У межах домену конфігурування параметрів сервісу Google Клас здійснюється за допомогою інтерфейсу адміністратора. Для цього у ньому на сторінці додатків слід обрати гіперпосилання на сервіс *«Classroom»*. Нижче наведені параметри можуть бути застосовані до усього домену або до будь-якого його підрозділу. Коротко запинимося на деяких з них.

Загальні налаштування дають можливість визначити категорії користувачів, які мають повноваження для створення курсів. Ними можуть бути підтверджені викладачі, ті, що очікують на розгляд або усі користувачі організації (рис. 7.23).

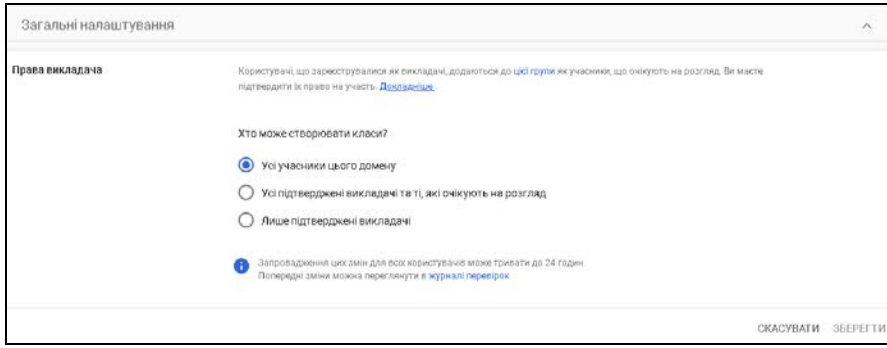

Рис. 7.23 Зміна прав для створення курсів

Як вже було зазначенно при першій авторизації на сервісі Google Classroom користувач вказує, ким він є: викладачем або учням. Облікові записи викладачів автоматично додаються в окрему групу. Адміністратор Google Workspace для освіти підтверджує акаунти викладачів, щоб у них був доступ до потрібних їм функцій сервісу, а також налаштовує для них дозволу в домені. Завдяки цьому користувачі, які не є викладачами, не можуть створювати курси, а також доступ до інформації про батьків чи кураторів учнів отримують тільки підтверджені викладачі.

Для того, щоб працювати з групою викладачів у розділі «*Додатки*» консолі адміністратора потрібно активувати сервіс *«Google Групи для бізнесу»* та перейти на сторінку групи викладачів за адресою https://classroom.google.com/teacher-group. У розділі *«Викладачі (Клас)»*буде доступний список користучів, що підтвердження адміністратора (рис. 7.24). Праворуч від обілікового запису користувача є гіперпосилання, яке дозволяє схвалити або відхилити запит.

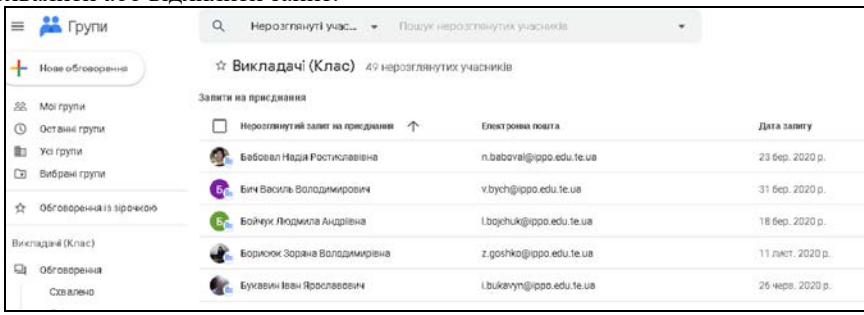

Рис. 7.24 Сторінка підтвердження повноважень викладача

У схожий спосіб налаштовуються параметри участі в курсах в ролі учня

(рис. 24). Зокрема можна обмежити приєднання до курсів, які створені в організації, для користувачів з власного чи визначених доменів. Також існує можливість надати відкрити доступ до курсів.

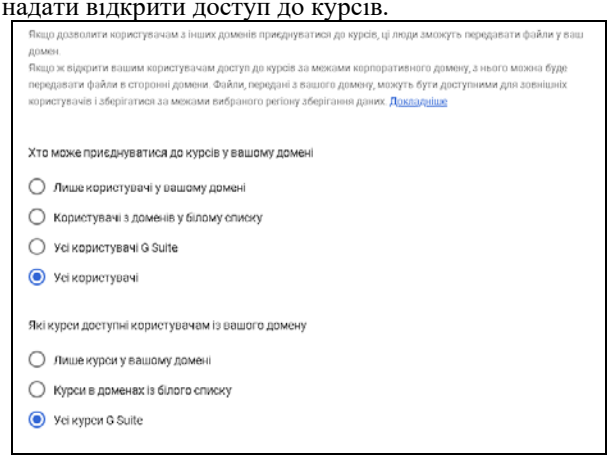

Рис. 7.25 Параметри участі в курсах Google Classroom

Додатково можна обмежити доступ до сторонніх курсів для користувачів організації. Слід зауважити, що поки для користувачів корпоративних облікових записів Google Workspace є недоступними курси, що створені за допомогою персональних облікових записів Google.

8. СЕРВІС ВІДЕОЗВ'ЯЗКУ GOOGLE MEET

Google Meet – це хмарний сервіс для обміну миттєвими повідомленнями та проведення відеоконференцій. Він дає змогу спілкуватися двом і більше користувачам у форматі групових відеоконференцій. За допомогою сервісу у школі можна проводити навчальні вебінари, онлайн-заняття, обмінюватися повідомленнями, демонструвати презентації, надавати доступ файлів завантажені додатків на екрані комп'ютера доповідача. Meet також доступний через інші хмарні сервіси Google Workspace: Gmail, Calendar, YouTube, а також мобільні додатки для операційних систем Android та IOS. Розробники сервісу називають сеанс спілкування відеозустріччю. Повідомлення та відеозустрічі сервісу Meet автоматично синхронізуються на всіх пристроях. Наприклад, можна почати спілкуватися на комп'ютері і продовжити на смартфоні. Нині для корпоративних клієнтів, зокрема й академічної підписки Google Workspace для освіти (підписка Fundamentals), сервіс забезпечує одночасну роботу 100 учасників відеоконференції, а для підписки Teaching and Learning Upgrade ця кількість зростає до 250.

Для початку роботи з сервісом слід перейти за покликанням http://meet.google.com. У випадку використання корпоративного облікового запису існує можливість пошуку облікових записів користувачів та груп у спільному каталозі. У цьому випадку користувачеві необхідно підтвердити власний номер.

Після авторизації на головній сторінці сервісу користувач потрапляє на сторінку, де пропонується створити нову або приєднатися до існуючої зустрічі. При створенні нової зустрічі користувачу надається код для приєднання. Якщо потрібно запланувати нову зустріч на майбутнє слід вказати відповідні дату та час. Також можна скористатися сервісом Google Calendar. Робота із сервісом передбачає використання двох панелей, перша з яких стосується участі користувача (рис. 8.1), а інша – відеозустрічі (рис. 8.2).

Рис. 8.1 Інтерфейс сервісу Google Meet

Покликання у вигляді кнопок першої панелі дають можливість:

1. Вимкнути або увімкнути мікрофон або камеру.
2. «Підняти руку», звернувши увагу учасників зустрічі.
3. Надіслати стилізоване графічне зображення – смайлик.
4. Увімкнути демонстрацію екрану (доступні трансляції окремого вікна, вкладки браузера Google Chrome або усього робочого стола).

5. Викликати меню зустрічі.
6. Завершити або покинути зустріч.

Панель, що стосується відеозутрічі (рис. 8.2) дає можливість:

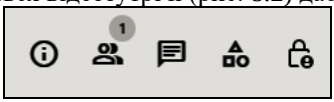

Рис. 8.2 Панель отримання інформації про зустріч

- Отримати інформацію для приєднання.
- Переглянути, додати або вилучити учасників зустрічі.
- Відкрити меню та почати спілкування у чаті.
- Почати використання дошки за допомогою сервісу Jamboard.
- Змінити параметри керування зустріччю.

До останніх параметрів належить можливість організаторів керувати зустріччю. За замовчуванням організатором зустрічі є користувач, що її створив. Додати співорганізатора можна у вікні учасників зустрічі. Організатор зустрічі має повноваження для вимикання мікрофонів як окремих, так і всіх учасників (рис. 8.3). Іншими параметрами управління є дозвіл або заборона учасників використовувати мікрофон, камеру, демонстрацію екрану, надсилання повідомлень до чату та реакцій (смайликів).

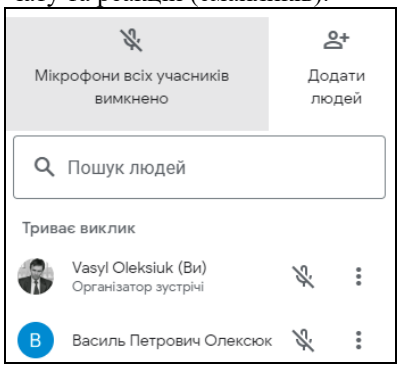

Рис. 8.3 Вікно управління учасниками зустрічі

Організатор має можливість вийти, залишивши учасників зутрічі або завершити зустріч для усіх водночас. Платна підписка Teaching and Learning, яка доступна для ЗВО України у 2022 році забезпечує додаткові опції, зокрема, відеозапис зустрічей із їх збереженням на Google-диску, розподілу учасників за окремими кімнатами, створення для них опитувань тощо

9. КОРПОРАТИВНІ ХМАРНІ ПЛАТФОРМИ

9.1 Огляд корпоративних хмарних платформ

Як показує досвід нині середній рівень завантаження процесорних потужностей у серверів під управлінням ОС Windows не перевищує 10%, у Unix-систем цей показник не перевищує 20%. Низька ефективність використання серверів має наслідком розвиток технологій віртуалізації, яка забезпечує більш гнучкий розподіл між додатками обчислювальних ресурсів фізичного сервера. Технологій віртуалізації дають можливість запускати на одному фізичному комп'ютері різні ОС за допомогою емуляції їх системних викликів до апаратних ресурсів. Крім енергозбереження та скорочення витрат, завдяки більш ефективному використанню апаратних ресурсів, віртуальна інфраструктура забезпечує високий рівень доступності ресурсів, більш ефективну систему управління, підвищену безпеку і вдосконалену систему відновлення у критичних ситуаціях.

У комп'ютерних технологіях під терміном «віртуалізація» зазвичай розуміють абстракцію обчислювальних ресурсів і надання користувачеві системи, яка «інкапсулює» (приховує в собі) власну реалізацію. Простіше кажучи, користувач працює з зручним для себе поданням об'єкта, і для нього не має значення, як насправді влаштований об'єкт.

До основних переваг технологій віртуалізації належать:

1. Ефективне використання обчислювальних ресурсів. Замість 3-х, а то і 10-ти серверів, завантажених на 5-20% можна використовувати один, який використовується на 50-70%.
2. Скорочення витрат на інфраструктуру: віртуалізація дозволяє скоротити кількість серверів і пов'язаного з ними IT-обладнання в інформаційному центрі. Як наслідок скорочуються потреби в обслуговуванні, електроживленні, охолодженні обладнання.
3. Зниження витрат на програмне забезпечення. Виробники програмного забезпечення пропонують окремі схеми ліцензування віртуальних середовищ.
4. Підвищення гнучкості і швидкості відновлення системи: Віртуалізація пропонує новий метод управління IT-інфраструктурою та допомагає адміністраторам витрачати менше часу на виконання повторюваних завдань, до яких належать встановлення, налаштування, моніторинг та технічне обслуговування ОС. За умови використання віртуального сервера можливий його «миттєвий» запуск на будь-якому апаратному забезпеченні.

Завдяки можливості абстрагування обчислювальних ресурсів та гнучкості їх розподілу віртуалізація знайшла широке застосування у хмарних технологіях.

Незважаючи на наявність потужних комерційних хмарних платформ (Windows Azure, Amazon EC2, C3), вважаємо можливим є розгортання корпоративної хмари на основі вільно поширюваних платформ. Серед них найбільш популярними є:

- Eucalyptus;
- Openstack;
- Proxmox VE;
- Cloudstack.

Eucalyptus – ще одна програмна платформа для розгортання корпоративних хмарних обчислень на комп`ютерних кластерах, що дозволяє створити сумісну з відомою платформою Amazon EC2 інфраструктуру. Основними програмними компонентами Eucalyptus є:

- контролер хмари (cloud controller) – є інтерфейсом управління хмарою; відповідає за розподіл основних віртуальних ресурсів;
- контролер кластера (cluster controller) – керує контролерами вузлів, визначає на якому вузлі буде завантажена віртуальна машина;
- контролер вузла (node controller) – відповідає за завантаження і функціонування кожного екземпляру віртуальної машини;
- walrus – забезпечує збереження даних, організованих у вигляді об'єктів.

OpenStack – це комплекс проектів вільного програмного забезпечення для створення обчислювальних хмар. Основними програмними складовими OpenStack є:

- OpenStack Compute (Nova) – інструментарій, що дозволяє автоматично створювати і управляти роботою груп віртуальних серверів;
- OpenStack Image Service (Glance) – реєстр образів віртуальних машин, який дає можливість реєструвати нові образи віртуальних машин і забезпечувати їх передавання для виконання на потрібні вузли;
- OpenStack Object Storage (Swift) – розподілене, завадостійке сховище об'єктів;
- OpenStack Identity (Keystone) – пакет для уніфікації засобів автентифікації і забезпечення інтеграції компонентів OpenStack з існуючими системами автентифікації;
- OpenStack Dashboard (Horizon) – веб-інтерфейс для управління системою;
- Networking (Quantum) – структура, призначена для створення, конфігурування і супроводу мереж.

Apache CloudStack є проектом компанії Apache Software Foundation, у межах якого розробляється програмне забезпечення з відкритим вихідним кодом, що може бути застосоване для розгортання загальнодоступних і корпоративних хмар згідно моделі «інфраструктура як сервіс» (IaaS). За допомо-

гою CloudStack можна сконфігурувати службу хмарних обчислень, яка надаватиме ресурси за запитом користувача.

Платформа Proxmox VE VE забезпечує готовим для застосування на корпоративному рівні гіпервізором. Перевагами платформи є:.

- ліцензування на умовах загальної публічної ліцензії GNU;
- адміністрування через веб-інтерфейс та за допомогою командного рядка локально і з використанням протоколу SSH;
- екземпляри віртуальних машин та вузли Proxmox VE можуть бути об'єднані в кластери, які можна централізовано адмініструвати через уніфікований веб-інтерфейс;
- забезпечення міграції в реальному часі без порушення її функціонування.

Отож, програмні складові розглянутих платформ практично однакові. Як видно з таблиці 1 їх функціональні можливості також є подібними.

Таблиця 9.1. Функціональні можливості платформ для розгортання корпоративних хмар

Платформи / Можливості	CloudStack	Eucalyptus	OpenStack	Proxmox VE
Консоль управління ВМ	+	+	–	+
Веб-інтерфейс консолі ВМ	+	–	–	+
Робота з гіпервізорами	Kvm, Xen	Kvm, Xen	Kvm, Xen	Kvm
Підтримка технології VLAN	+	+	+	+
Розширення через API-функції	+	+	+	+
Створення «миттєвих знімків» ОС	+	+	+	+
Повідомлення та зауваження	+	–	–	+
Інтеграція з Active Directory	+	+	+	+
Безкоштовне поширення	+	+	+	+

9.2.1 Огляд можливостей системи Apache Cloudstack

Apache CloudStack дає можливість виконувати віртуальні машини у хмарній інфраструктурі. Під віртуальною машиною (ВМ) розуміють програмне або апаратне середовище, яке приховує справжню реалізацію будь-якого процесу або об'єкта від його видимого уявлення. Тобто віртуальну машину можна уявити як ізольований програмний контейнер, який працює з власною ОС і додатками. ВМ функціонує подібно до фізичного комп'ютера: містить власні віртуальні складові (центральний процесор, оперативну пам'ять, жорсткий диск, мережний адаптер).

Апаратне або програмне забезпечення, яке забезпечує одночасне і паралельне виконання кількох віртуальних машин називають гіпервізором. Кожна окрема реалізація хмари може містити декілька реалізацій гіпервізора. На сьогодні Apache CloudStack підтримує роботу таких гіпервізорів: Hyper-V, KVM, LXC, vSphere, Xenserver. CloudStack. Платформа може управляти багатьма фізичними серверами, які географічно розподілені в різних центрах обробки даних. Технічне обслуговування чи інші помилки сервера керування можуть здійснюватися без впливу на віртуальні машини у хмарі.

Apache CloudStack дає змогу налаштовувати параметри мережі та зберігання кожної віртуальної машини. Внутрішньо, пул віртуальних пристроїв підтримує роботу конфігурації самої хмари. Платформа надає такі мережні послуги, як брандмауер, маршрутизація, DHCP, VPN, консольний проксі, тощо. Широке використання горизонтально масштабованих віртуальних машин спрощує встановлення та поточне обслуговування хмари.

Для управління хмарою адміністратором, а також для роботи користувачів з віртуальними машинами, CloudStack надає веб-інтерфейс. Він може бути налаштований відповідно до потреб користувачів. Для удосконалення функціональних можливостей платформи усіма бажаючими, її розробники пропонують використання REST-подібного API інтерфейсу.

У платформі Apache CloudStack реалізовано ряд функцій, які дають змогу покращити доступність системи. Сервер керування може бути розгорнений на кількох фізичних серверах, які балансуватимуть навантаження. Сервер баз даних MySQL може бути налаштований на використання реплікації, щоб забезпечить відмовостійкість у випадку виходу з ладу одного з серверів. Між окремими сховищами даних Apache CloudStack підтримує з'єднання з використанням стандартів локальних мереж або за допомогою протоколу зберігання даних iSCSI.

9.2.2 Архітектура хмарної платформи Apache Cloudstack

Загалом, архітектура хмари, розгорнутої на основі Apache CloudStack складається з сервера керування та ресурсів для керування. Під час розгортання сервер керування налаштовують для роботи з ресурсами: блоки IP-адрес, пристрої для зберігання, віртуальні локальні мережі (VLAN) тощо.

Проста конфігурація системи мітить два комп'ютери – один з яких виконує функції сервера управління (сервіс CloudStack Management), а інший виконує роль хмарної інфраструктури. У цьому випадку інфраструктура містить один хост, на якому виконується програмне забезпечення гіпервізора (рис. 9.1). У найпростішому випадку один комп'ютер може виконувати функції сервера керування і гіпервізора (у реалізації KVM).

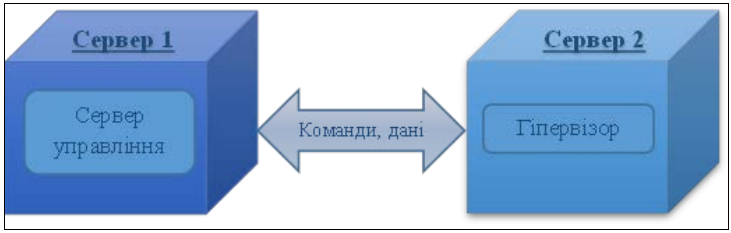

Рис. 9.1 Проста архітектура хмари Apache CloudStack

Більш функціональні реалізації хмари містять сервер управління, який виконується на кількох фізичних комп'ютерах, та чималої кількості хостів, які використовують різні гіпервізори, мережеві стандарти та технології збереження даних.

Основним завданням сервера керування є управління та розподіл апаратних ресурсів хмарної інфраструктури. Сервер керування, як правило, виконується на окремо виділеному комп'ютері. Також можливим є його реалізація у вигляді віртуальної машини. Сервер керування контролює створення та завантаження віртуальних машин, призначення їх для виконання на певних хостах, виділення IP-адрес для віртуальних комп'ютерів. Сервер керування є сервлетом, що написаний на мові Java, та працює в контейнері Apache Tomcat. Для збереження даних сервер керування використовує СУБД MySQL.

До інших функцій сервера керування належать:

- надання веб-інтерфейсу для адміністраторів та користувачів;
- забезпечення API-інтерфейсів для виконання внутрішніх API-функцій та для інтерфейсу EC2;
- управління виділенням віртуальним машинам певних обчислювальних ресурсів;
- виділення публічних та приватних IP-адрес.
- виділення сховища під час створення, перенесення чи експорту віртуальних машин;
- управління шаблонами, архівами, ISO-образами дисків;
- забезпечення інтерфейсу конфігурування хмари.

9.2.3 Основні поняття платформи Apache CloudStack

У хмарній інфраструктурі ресурси можуть бути розподілені всередині таких об'єктів: регіони, зони, стійки, кластери, хости, первинні та вторинні сховища.

Регіон є найбільшим організаційним підрозділом, який використовується при розгортанні Apache CloudStack. Він містить кілька зони доступності,

кожна з яких є еквівалентною центру обробки даних. Кожен регіон містить власний кластер серверів управління, який функціонує в одній із його зон. Регіони є корисною технологією забезпечення надійності та аварійного відновлення великих хмарних інфраструктур. Облікові записи користувачів можуть належати кільком регіонам. Як наслідок користувачі мають змогу розгортати власні віртуальні машини у кожному з них. У випадку, якщо один із регіонів стає недоступним, послуги залишаються доступними через віртуальні машини, які розгорнуті в іншому регіоні. Адміністратор може отримувати статистику використання обчислювальних ресурсів на рівні регіону. Регіони є видимими користувачам. Завантажуючи віртуальну машину на певному хості, користувач неявно обирає для неї відповідний регіон.

Наступною за масштабом організаційною величиною під час розгортання Apache CloudStack є зона. Вона, як правило, відповідає одному центру обробки даних. Перевагою організації інфраструктури в зоні є забезпечення фізичної ізоляції та відмовостійкості обчислювальних ресурсів. Наприклад, кожна зона може мати власне джерело живлення окремо виділені канали зв'язку. Кожна зона містить (рис. 9.2):

- однин або кілька стійок (pods), який аналогом серверної стійки;
- кластери (clusters) – сукупність фізичних серверів, розміщених у одній стійці;
- хостів (hosts) – серверів, на яких виконуютьться гіпервізори;
- первинні сховища (primary storages) та одне вторинне сховище, які є доступними у межах усіх стійок зони; сховища містять розділи та диски віртуальних машин.

Якщо користувач створює віртуальну машину, він повинен обрати зону для неї. Користувачі мають змогу копіювати їх власні шаблони у інші зони.

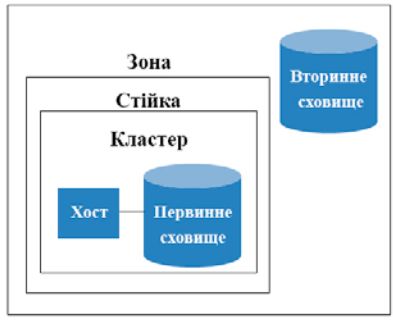

Рис. 9.2 Основні складники хмарної архітектури Apache CloudStack

Зони можуть бути загальнодоступними або приватними. Загальнодоступні зони є видимими для всіх користувачів. Це означає, що будь-який користувач у ній може створювати свої віртуальні комп'ютери. Приватні зони є

зарезервованими для певного домену. Тільки користувачі цього домену або його субдоменів можуть створювати ВМ у такій зоні.

Передання даних між хостами однієї зони відбувається безпосередньо, без фільтрування брандмауерами. Хости в різних зонах можуть мати доступ до один одного через налаштовані тунелі віртуальних приватних мереж (VPN).

Розгортаючи хмарну інфраструктуру, адміністратор повинен спроектувати її архітектуру, тобто визначити:

- кількість стійок, які має містити кожна зона;
- кількість кластерів, які має містити кожна стійка;
- кількість хостів, які потрібно розмістити в кожному кластері;
- кількість первинних сховищ у кожній зоні та кожному кластері, а також загальний обсяг їх дисків чи дискових масивів;
- обсяг та розміщення вторинного сховища зони.

У процесі створення нової зони у веб-інтерфейсі Apache CloudStack потрібно налаштувати її фізичні мережі та додати основні складові інфраструктури – кластер, хост, первинні та вторинні сховища.

Хости, що належать одній і тій же стійці, повинні знаходитися в одній підмережі. Кожна зона може містити одну або кілька стійок, які в свою чергу містять однин або кілька кластерів, хостів та одне або кілька первинних сховищ. Стійки не є видимими для користувачів.

Кластер дає змогу групувати хости. Хости в кластері повинні мати однотипне обладнання, і виконувати один і той же гіпервізор, знаходитися в одній підмережі та мати доступ до серверів первинних сховищ. У межах одного кластера можна переміщувати екземпляри ВМ з одного хоста на інший.

Платформа Apache CloudStack дозволяє розгортати кілька кластерів. У найпростішому випадку, коли використовуються локальні сховища (гіпервізори виконуються на серверах, які містять первинні й вторинні сховища), кластери є необхідними для організаційного забезпечення архітектури хмари.

Як було зазначено вище, хост – це один комп'ютер, який виконує гіпервізор. Хости надають обчислювальні ресурси для системних віртуальних машин та ВМ користувачів. На кожному хості повинно бути встановлене програмне забезпечення гіпервізора. Наприклад, хостом може бути сервер Citrix XenServer, сервер із встановленим гіпервізором KVM, сервер ESXi або сервер Microsoft Hyper-V. Хост є найменшим організаційним підрозділом в межах розгортання Apache CloudStack.

Хости в розгортанні CloudStack забезпечують:

- виділення обчислювальних ресурсів (процесорного часу, оперативної пам'яті, ресурсів мережі), які необхідні для функціонування ВМ;
- високошвидкісне з'єднання ВМ та їх підключення до інтернету;

Існує можливість додавання хостів у хмарну інфраструктуру Apache CloudStack. Платформа визначає кількість процесорів і загального обсягу оперативної пам'яті, які надаються хостами.

Хости не є видимими для користувачів. Користувач, на відміну від адміністратора, не може обрати, на якому хості слід виконувати його ВМ.

Для того, щоб хост працював у CloudStack, слід:

- встановити у його ОС програмне забезпечення гіпервізора;
- призначити йому IP-адресу;
- додати хост до сервера управління.

Первинне сховище пов'язано з кластером та містить віртуальні диски всіх віртуальних машин, що працюють на хостах у цьому кластері. Адміністратор хмари має змогу додати до кластера або зони кілька первинних сховищ. Для функціонування зони потрібне щонайменше одне первинне сховище. Його слід розташовувати поруч з хостами, щоб забезпечити достатню швидкість передавання та обробки даних. Apache CloudStack керує розподілом віртуальних дисків користувачів на кілька основних сховищ.

Щоб уникнути додаткових операцій копіювання даних, у зоні доцільно налаштувати загальну область зберігання. За допомогою неї дані первинного сховища будуть доступними лише для віртуальних машин кластера. У випадку якщо дані будуть потрібні в іншому кластері, їх доведеться копіювати.

Apache CloudStack забезпечує доступ сховищ за різними протоколами, підтримка яких залежить від типу гіпервізора. Наприклад, для Microsoft Hyper-V підтримується сховища та протоколи ОС Windows SMB/CIFS. Основними для платформи Apache CloudStack є стандартні протоколи для роботи із сховищами iSCSI та NFS. Платформа також підтримує використання на хостах локальних сховищ.

Вторинні сховища призначені для зберігання:

- шаблонів віртуальних машин – наперед налаштованих архівів ОС, які можна використовувати для швидкого розгортання віртуальних машин; вони можуть містити додаткові дані, наприклад, встановлене програмне забезпечення;
- ISO-образи дисків – містять дані завантажувальних носіїв, з яких відбувається встановлення операційних систем;
- архіви (так звані знімки (snapshots) дисків) – збережені копії даних віртуальних машин, які можуть бути використані для відновлення даних або для створення нових шаблонів.

Об'єкти вторинного сховища є доступними для всіх хостів у межах зони або регіону. Подібно до первинних сховищ, Ahache CLoudStack підримує роботу з вторинними сховищами за протоколами iSCSI, NFS, SMB/CIFS, а також сумісність із сховищами платформ OpenStack та Amazon Simple Storage Service.

9.2.4 Мережі у хмарній інфраструктурі Apache CloudStack

За допомогою Apache CloudStack можна розгорнути інфраструктуру з різноманітним з'єднанням мереж, але вони, як правило, реалізують один з двох сценаріїв:

- базовий, що забезпечує єдину «плоску» мережу, у якій ізоляція віртуальних машин здійснюється системним мостом на мережному рівні;
- розширений, який зазвичай використовує ізоляцію на канальному рівні, наприклад, за допомогою віртуальних локальних мереж (VLAN).

Одним з етапів створення зони є конфігурування фізичної мережі. З кожною зоною може бути асоційовано одна або кілька мереж. Кожна мережа відповідає окремому мережному адаптеру на хості гіпервізора. Кожна фізична мережа може передавати один або більше типів мережевого трафіку. Вибір типу трафіку для кожної мережі залежить від типу зони (базового або розширеного).

У процесі конфігурування зони адміністратор має змогу:

- додавати, видаляти, оновлювати фізичні мережі, які їй належать;
- конфігурувати віртуальні локальні мережі у фізичній мережі;
- визначати типи трафіку, які генеруються у фізичних мережах;
- змінювати імена мереж, щоб забезпечити їх розпізнавання гіпервізорами;
- виділяти діапазони IP-адрес, що будуть арендовані ВМ користувачів;
- конфігурувати додаткові мережні сервіси зони (брандмауери, балансувачі навантаження тощо).

Платформа Apache CloudStack дає змогу об’єднувати в одній інфраструктурі фізичні та віртуальні мережі, у яких передаються такі види трафіку:

- гостьовий – трафік, який генерується між віртуальними комп’ютерами користувачів. Кожна стійка у зоні, що працює у базовому режимі, є широкомовним доменом. Як наслідок для різних стійок адміністратору слід виділяти різні діапазони IP-адрес;
- управляючий – генерується у процесі взаємодії між сервером управління та хостами в кластерах, зокрема його утворюють і системні віртуальні машини, які використовуються платформою для виконання системних завдань у хмарі);
- публічний – трафік, який передають віртуальні машини у процесі доступу до інтернету; користувачі можуть використовувати вебінтерфейс Apache CloudStack, щоб одержати додаткові IP-адреси з публічного діапазону;
- трафік сховища – передається у процесі роботи зі вторинним сховища, наприклад при роботі з шаблонами та архівами (знімками) віртуальних машин.

З метою підвищення швидкодії хмари, розробники платформи радять використовувати окремі мережні адаптери для передавання різних видів трафіку. Для кожного виду трафіку адміністратор повинен виділити окремі діапазони IP-адрес.

У випадку використання базового режиму, у хмарі можна використовувати лише одну фізичну мережу. Зазвичай, у цьому випадку не викликає особливих проблем, оскільки потрібно налаштувати лише одну гостьову мережу. Apache CloudStack автоматично призначить IP-адреси з інших діапазонів та співставить їх з відповідними підмережами. Усі IP-адреси гостьової мережі належатимуть одній віртуальній мережі. Загалом розгортання хмари залежить від її архітектури та обраних гіпервізорів. Наприклад, невелика реалізація хмарної інфраструктури може бути такою (рис. 9.3):

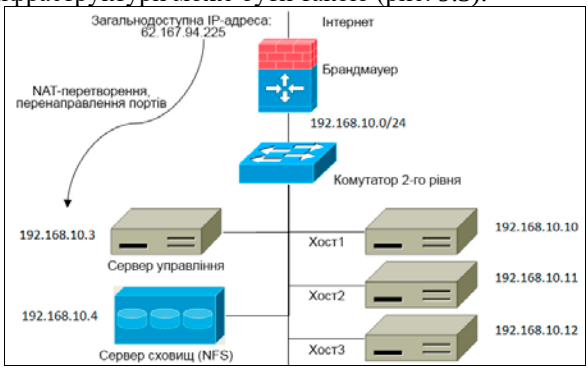

Рис. 9.3 Реалізація хмарної інфраструктури у базовому режимі

Оскільки, усі складові наведеної на рис. 9.3 інфраструктури знаходяться в одній мережі з адресою 192.168.10.0/24, то наведена реалізація хмари передбачає використання базового режиму мережі. У розгорнутій хмарі присутні: сервер управління, три хости, на яких виконуються гіпервізори, один сервер, на якому знаходяться первинне та вторинне сховища. Брандмауер забезпечує фільтрування трафіку, який передається між хмарою та мережею інтернет, зокрема він може забезпечити обмеження доступу віртуальних комп'ютерів до певних інтернет-сервісів, а також, використовуючи технологію перенаправлення портів (DNAT), надати доступ до них з інтернету.

Розширений режим дає змогу використовувати у зоні кілька фізичних мереж, кожна з яких може передавати один або кілька типів трафіку. У цьому випадку гостьові мережі можуть бути загальнодоступними або ізольованими. Створюючи додаткові гостьові мережі, адміністратор хмари може налаштувати їх як загальнодоступні або обмежити доступ для певних облікових записів. Такі віртуальні локальні мережі ідентифікуються номером VLAN, діапазоном IP-адрес, та адресою шлюзу. Існує можливість резервування частини

простору IP-адрес для віртуальних або фізичних комп'ютерів, які не належать хмарній інфраструктурі. У розширеному режимі реалізація хмарної інфраструктури може мати вигляд (рис. 9.4):

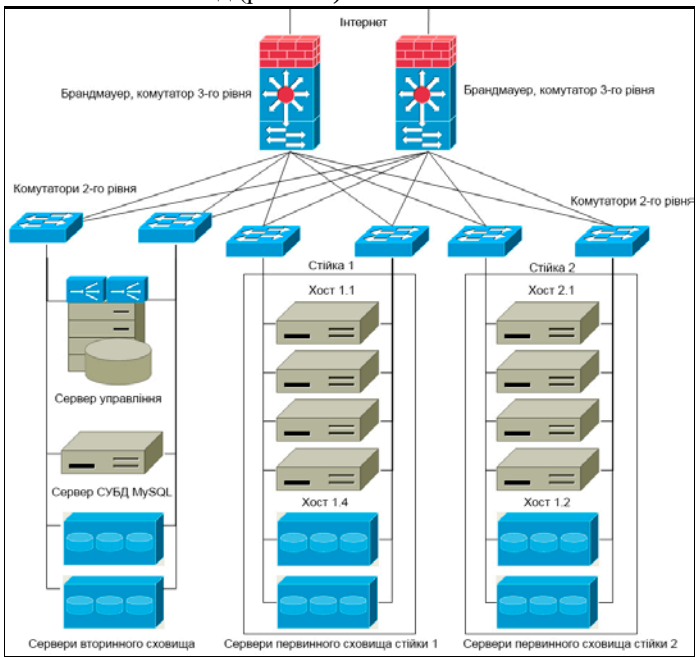

Рис. 9.4 Реалізація хмарної інфраструктури у розширеному режимі

З рисунка 9.4 видно, що хмарна інфраструктура має доступ до мережі інтернет через два окремих маршрутизатори (брандмауер1 та брандмауер2), які, крім фільтрації трафіку, виконують функції комутаторів 3-го рівня (забезпечують розподіл стійок у віртуальних локальних мережах). Сервери вторинних сховищ знаходяться в одній мережі із сервером керування. Кожна стійка містить по два первинні сховища та по чотири хости. Кожен сервер у стійці має додаткові мережні адаптери, що підключені до окремих комутаторів другого рівня. У великій хмарній інфраструктурі доцільно налаштувати кілька серверів керування та баз даних.

У кожній зоні потрібно налаштувати діапазон зарезервованих IP-адрес для передавання управляючого трафіку. Відповідна мережа забезпечуватиме зв'язок між сервером управління та різними системними віртуальними машинами. Платформа Apache CloudStack передбачає функціонування таких видів системних ВМ:

- консольний проксі (console proxy) – забезпечує виведення інтерфейсу віртуальної машини у веб-браузер;
- ВМ вторинного сховища (CloudStack secondary storage VM) – відповідає за доступ до ISO-образів та шаблонів;
- віртуальний роутер – забезпечує маршрутизацію та виділення публічних IP-адрес;

Залежно від призначення, системним ВМ виділяються IP-адреси з різних діапазонів (гостьового, публічного, приватного). Проте усі вони мають бути унікальними в межах усієї хмари. Системним ВМ присвоюються зарезервовані приватні IP-адреси згідно стандарту RFC1918, який регламентує використання IP-адрес у локальних мережах. Отож, сервери керування чи ВМ користувачів не повинні використовувати приватні IP-адреси. Наприклад, якщо таким зарезервованим діапазоном є 192.168.1.2 – 192.168.1.127, то для серверів керування та гіпервізорів можна використовувати діапазон 192.168.1.128 – 192.168.1.254.

Для зон, які використовують розширений режим, рекомендовано виділяти надлишкову кількість приватних IP-адрес, як для комп'ютерів клієнтів, так і для системних ВМ. Як правило, для них потрібні близько 10-ти додаткових IP-адрес. Кількість приватних IP-адрес також залежить від гіпервізора. Наприклад, KVM та Xen підримують адресування у мережах з маскою 255.255.0.0, що забезпечує роботу близько 65000 пристроїв. З метою структурування хмарної інфраструктури доцільно створювати кілька стійок, кожній з яких виділяти окремий діапазон.

9.2.5 Встановлення платформи Apache CloudStack

Встановлення сервера управління Apache CloudStack можливе як з інсталяційних пакетів, так і через компілювання вихідного коду. Будемо розглядати випадок встановлення платформи з інсталяційних пакетів на популярну ОС Ubuntu Linux. Загалом процес встановлення системи проходить упродовж таких етапів:

1. Встановлення серверів управління та СУБД.
2. Встановлення серверів первинного та вторинного сховищ.
3. Встановлення гіпервізорів та конфігурування хостів.

Для встановлення сервера управління в ОС Ubuntu слід додати репозитарій пакетів Apache CloudStack до списку інсталяційних серверів операційної системи. Для цього слід створити файл */etc/apt/sources.list.d/cloudstack.list,* у який додати рядок:

deb http://cloudstack.apt-get.eu/ubuntu precise 4.X,

де X – версія платформи Apache CloudStack. Далі потрібно завантажити та додати відкритий ключ репозитарія до довірених ключів за допомогою команди:

wget -O - http://cloudstack.apt-get.eu/release.asc|apt-key add –

Після успішного виконання останньої команди слід оновити індекс пакетів ОС та почати встановлення сервера управління:

apt-get update

apt-get install cloudstack-management

Apache CloudStack використовує сервер MySQL для зберігання даних. Для невеликої хмарної інфраструктури, яка містить одну зону, можна встановити сервер MySQL на той же комп'ютер, що й сервер управління. На момент написання посібника платформа працює з серверами MySQL версій 5.1 та 5.5. Встановлення сервера MySQL у ОС Ubuntu виконують за допомогою команди:

apt-get install mysql-server

Програма інсталяції створить системні бази даних та виведе запит на введення пароля адміністратора сервера баз даних – користувача root.

Конфігурування сервера MySQL вимагає внесення змін до файла */etc/mysql/my.cnf,* до якого слід додати рядки:

innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'

Зазначені зміни встановлюють параметри обробки помилок у базі даних, задають обмеження на кількість з'єднань та формат запису подій у журнал сервера.

Запуск або перезапуск сервера MySQL здійснюють командою:

service mysql start

Наступним кроком встановлення є створення бази даних платформи, яку виконують за допомогою команди:

*cloudstack-setup-databases cloud:<dbpassword>@localhost *
*--deploy-as=root:<password> *
*-e <encryption_type> *
*-m <management_server_key> *
*-k <database_key> *
-i <management_server_ip>, де

- cloud – обліковий запис користувача сервера MySQL;
- dbpassword – пароль облікового запису cloud;
- --deploy-as=root:<password> – привілегії суперкористувача (root), необхідні для створення бази даних, та його пароль;

- -e – тип шифрування, може набувати значення file або web;
- -m – ключ шифрування конфіденційних параметрів у файлі конфігурації Apache CloudStack;
- -k – ключ шифрування конфіденційних параметрів у базі даних;
- -i – IP-адреса сервера управління.

Apache CloudStack зберігає та шифрує кілька паролів і секретних ключів: пароль та ключ доступу до бази даних, ключі віддаленого доступу за протоколом SSH, паролі адміністратора ОС, на якій виконується гіпервізор, паролі сервісів VNC та VPN. Наприклад, якщо у команді використано опцію *-e=file*, то адміністратор хмари повинен знати шлях до цього файлу.

Останньою командою, яка завершує встановлення сервера управління та завантажує його сервіс, є:

cloudstack-setup-management

Зазвичай, функцію сервера первинного та вторинного сховищ в ОС Ubuntu виконує сервіс мережної файлової системи NFS (Network File System). Він може функціонувати на тому ж фізичному комп'ютері, що й сервер управління, або окремо. Встановлення сервера NFS в ОС Ubuntu виконують командою:

apt-get install nfs-kernel-server

Після цього слід створити папки, які будуть використані для розміщення спільних мережних ресурсів первинного та вторинного сховищ:

mkdir -p /export/primary
mkdir -p /export/secondary

Для створення спільних ресурсів редагують конфігураційний файл */etc/exports*, у який додають рядок:

*/export *(rw,async,no_root_squash,no_subtree_check)*

Наведені параметри конфігурації дозволяють доступ до спільного ресурсу export у режимі читання та запису з будь-якого комп'ютера. Після зміни файла */etc/exports* слід перезавантажити NFS-сервер командою:

service nfs-kernel-server restart

На сервері управління слід приєднати спільний ресурс вторинного сховища, наприклад, у папку /mnt/secondary:

mount -t nfs <IP_NFS-server>:/export/secondary /mnt/secondary

У подальшому необхідність їх автоматичного приєднання можна описати у файлі */etc/fstab*.

Для доступу до вторинного сховища Apache CloudStack використовує системну віртуальну машину (Secondary Storage VM). Зазначена ВМ залежить від типу обраного гіпервізора. Наприклад, для підготовки ВМ вторин-

ного сховища, яке працюватиме з гіпервізором KVM, на сервері управління слід виконати команду:

*/usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt *
*-m /mnt/secondary *
*-u http://cloudstack.apt-get.eu/systemvm/4.6/systemvm64template-4.6.0-kvm.qcow2.bz2 *
-h kvm -s <optional-management-server-secret-key> -F,

у якій використано опції:

- -m – каталог, до якого буде завантажено шаблон системної ВМ;
- -u – URL завантаження (він може бути різним для різних версій);
- -h – тип гіпервізора;
- -s – ключ шифрування параметрів конфігурації (не обов'язковий).

Зауважимо, що у останній команді символ «\» використано для перенесення рядків. Оскільки шаблон має значний обсяг (понад 5 Гб), то команда може виконуватися деякий час. Якщо сервер управління та NFS-сервери виконуються на різних фізичних комп'ютерах, то для завершення підготовки вторинного сховища необхідно від'єднати відповідну спільну папку:

umount /mnt/secondary

Встановлення та конфігурування хоста опишемо на прикладі гіпервізора KVM (Kernel-based Virtual Machine). На офіційному сайті Apache CloudStack можна знайти перелік рекомендованих версій гіпервізора KVM, а також необхідних для нього пакета Qemu та бібліотек libvirt.

Перед встановленням гіпервізора KVM виконують підготовку ОС. За допомогою команди *hostname --fqdn* слід перевірити правильність відображення повного доменного імені комп'ютера. Комп'ютер повинен мати доступ до мережі інтернет, у чому можна пересвідчитися за допомогою утиліти *ping*. Для синхронізації часу слід встановити пакет openntpd, який буде виконувати роль NTP-сервера (NTP – Network Time Protocol).

Для управління екземплярами гіпервізора KVM, який виконується на хості, у платформі Apache CloudStack реалізовано агент. Взаємодіючи з сервером керування, він виконує команди та повертає результати їх виконання. Встановлення агента виконують за допомогою команди:

apt-get install cloudstack-agent

Агент CloudStack надає можливість серверу управління контролювати процесор хоста, який виконує екземпляр KVM. За замовчуванням агент використовує версію віртуального процесора QEMU. Для кожного хоста адміністратор може вказати конфігурацію процесора у файлі */etc/cloudstack/agent/agent.properties* за допомогою параметра *guest.cpu.mode*, який може набувати значень:

- host-passsthrough – сервіс libvirt буде використовувати модель процесора без змін;
- host-model –сервіс libvirt визначить модель процесора на основі файла */usr/share/libvirt/cpu_map.xml*;
- custom – адміністратор може самостійно вказати модель процесора.

Для управління віртуальними машинами Apache CloudStack використовує бібліотеку libvirt. Для обміну даними з KVM libvirt повинен прослуховувати незахищені TCP-з'єднання. Також потрібно вимкнути можливість використання багатоадресних DNS запитів (multicast DNS). Зазначені параметри містяться у файлі */etc/libvirt/libvirtd.conf*:

listen_tls = 0
listen_tcp = 1
tcp_port = «16509»
auth_tcp = «none»
mdns_adv = 0

Також для забезпечення повної підтримки протоколу TCP у файлі */etc/default/libvirt-bin* слід змінити рядок до вигляду:

libvirtd_opts=«-d -l»,

та перезавантажити сервіс:

service libvirt-bin restart

Функціонування агента CloudStack може бути блоковано з боку сервісу Apparmor, який є програмним інструментом захисту ОС Ubuntu.

Передовсім слід перевірити чи встановлено AppArmor. У ОС Ubuntu це можна виконати використовуючи команду:

dpkg --list 'apparmor'

Вимкнути профіль AppArmor для бібліотеки libvirt можливо за допомогою таких команд:

ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/
ln -s /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper /etc/apparmor.d/disable/
apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd
apparmor_parser -R /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper

Для передавання трафіку до екземплярів гіпервізорів Apache CloudStack використовує технологію мостів. Нагадаємо, що мостом є пристрій, що з'єнує сегменти локальних мереж, передаючи дані на основі даних канального рівня моделі OSI (MAC-адрес). На комп'ютері, що виконує функції хоста, слід налаштувати щонайменше два мости, які відповідають за передавання загальнодоступного та приватного трафіку. За замовчуванням ці мости назви *cloudbr0* і *cloudbr1*. Важливим фактором є підтримка конфігурації мостів усі-

ма гіпервізорами, які використовують у хмарі. У ОС Ubuntu програмна реалізація функціоналу мостів може бути встановлена разом з пакетом bridge-utils.

Процес конфігурування мостів розглянемо на прикладі. Нехай комп'ютер, що виконує функцію хоста оснащено одним мережним адаптером, на якому налаштовано роботу 3-ох віртуальних мереж, які передають такі види трафіка:

- vlan1 –управляючий трафік;
- vlan2 –загальнодоступний трафік;
- vlan3 –приватний трафік.

Адміністратору слід налаштувати мостові інтерфейси *cloudbr0* та *cloudbr1* для роботи з віртуальними мережами vlan2 та vlan3. У такій реалізації гіпервізор та сервер керування повинні бути в різних IP-мережах.

Конфігурування мережних з'єднань на сервері, який працює під управлінням ОС Ubuntu, здійснюють через редагування файла */etc/network/interfaces*. Для нашого прикладу він матиме вигляд:

```
auto lo
        iface lo inet loopback

auto eth0.1
iface eth0.1 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        gateway 192.168.1.254
        dns-nameservers 8.8.8.8 8.8.4.4


auto cloudbr0
iface cloudbr0 inet static
        address 192.168.2.2
        netmask 255.255.255.0
        bridge_ports eth0.2
        bridge_fd 5
        bridge_stp off
        bridge_maxwait 1
auto cloudbr1

iface cloudbr1 inet manual
        bridge_ports eth0.3
        bridge_fd 5
        bridge_stp off
        bridge_maxwait 1
```

У наведеному фрагменті маємо на увазі, що мережний інтерфейс має назву *eth0*, а його віртуальні екземпляри – *eth0.1, eth0.2* та *eth0.3*. У різних

версія ОС Ubuntu зазначені інтерфейси можуть мати інші назви. Мостовий інтерфейс *cloudbr0* передає загальнодоступний трафік та використовує статично призначену IP-адресу. За адресування приватних мереж відповідає Apache CloudStack, отож для інтерфейсу cloudbr1 не призначено жодної IP-адреси.

Після внесення змін до файлу */etc/network/interfaces* слід перезавантажити сервіс *networking* або всю ОС Ubuntu.

9.2.6 Інтерфейс платформи Apache CloudStack

Для роботи користувачів з хмарною інфраструктурою платформа Apache CloudStack використовує веб-інтейфейс. Для входу до нього у веб-браузері потрібно ввести URL-адресу *http://<IP-адреса_сервера_управління>:8080/client*. На сторінці, що завантажиться користувачеві буде запропоновано пройти автентифікацію (рис. 9.5):

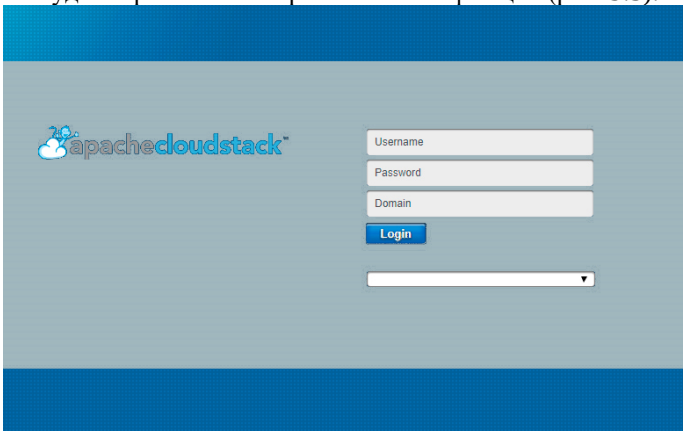

Рис. 9.5 Сторінка автентифікації Apache CloudStack

Крім полів введення логіна та пароля користувач може обрати мову інтерфейсу, а також вказати домен, до якого належить його обліковий запис. Домени є аналогом груп або підрозділів користувачів у ОС, а їх використання спрощує деякі операції адміністування хмари.

Веб-інтерфейс Apache CloudStack (рис. 9.6) дає змогу користувачам переглядати та використовувати свої хмарні ресурси: віртуальні машини, їх шаблони та архіви, ISO-образи, гостьові мережі та IP-адреси, які використовують їх ВМ.

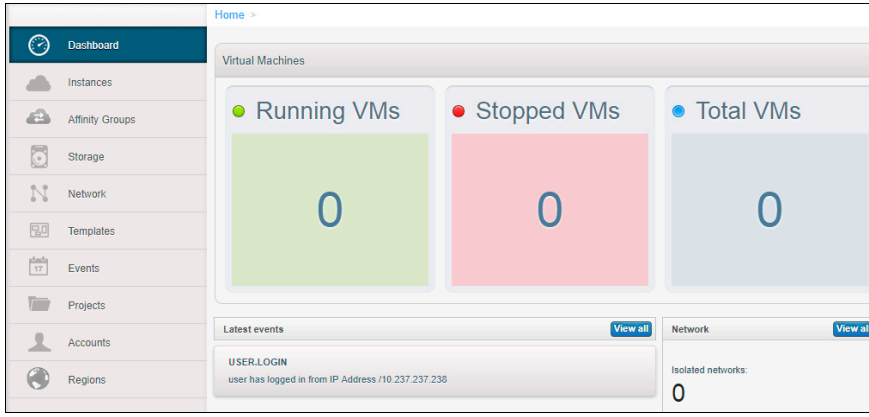

Рис. 9.6. Інтерфейс користувача платформи Apache CloudStack

Ліворуч знаходиться меню, яке забезпечує навігацію між об'єктами хмарної інфраструктури. Робоча область відображає вміст обраного пункту меню. Як видно з рис. 9.6 пункт *Інструментальна панель (Dashboard)* відображає відомості про віртуальні машини користувача, а також події, які виникають внаслідок виконання ним операцій.

Після першого входу до системи користувачеві слід створити власну віртуальну машину. Це можна зробити за допомогою пункту меню *Instances (Машини)*. У правому верхньому куті сторінки, що завантажиться потрібно обрати кнопку *Add Instance (Додати машину)*. Створюючи віртуальну машину слід вказати:

- зону, у якій буде створено машину;
- шаблон або ISO-образ, з якого буде створено машину;
- обчислювальну продуктивність віртуального комп'ютера;
- необхідний обсяг диска;
- групу спорідненості (Affinity Groups), з якою буде асоціюватися ВМ;
- приналежність віртуального комп'ютера до однієї або кількох мереж;
- назву ВМ.

Якщо було обрано створення машини з шаблона, то системою буде підготовлено віртуальний комп'ютер з тією ОС, яка була наперед налаштована у шаблоні (рис. 9.7). Якщо ж користувач обрав варіант використання ISO-образа, то йому доведеться встановлювати ОС самостійно.

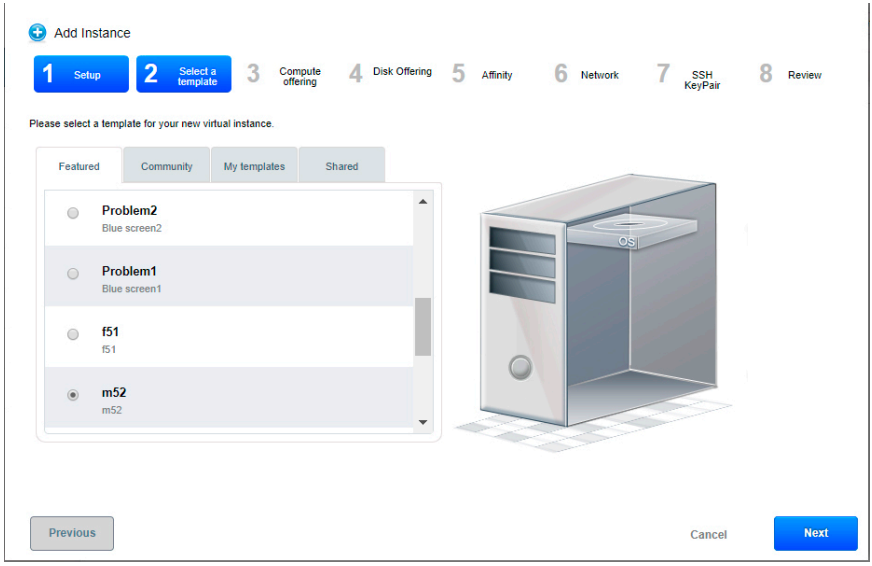

Рис. 9.7. Створення ВМ: вибір шаблона

Шаблони продуктивності забезпечують гнучкий розподіл обчислювальних ресурсів (насамперед частоти та кількості ядер процесора, а також обсягу оперативної пам'яті). Apache CloudStack надає такі вбудовані шаблони продуктивності *Мала Машина (Small Instance), Середня Машина (Medium Instance), Продуктивна машина (Advanced Instance))*. Наприклад, у навчальному процесі для ненавантажених Unix-подібних ОС з командним інтерфейсом можна використовувати шаблон *Мала машина (Small Instance)*. Для сучасних ОС Windows мінімально необхідним є шаблон *Середня Машина (Medium Instance)*.

Вибір диска залежить від способу створення ВМ. Якщо ОС встановлюють з ISO-образа, то визначення обсягу диска є обов'язковим. У випадку розгортання ВМ із шаблона, який уже містить наперед налаштовану ОС, обраний диск, буде другим (не системним). У цьому випадку взагалі можна відмовитися від додавання диска.

Створюючи групи спорідненості та присвоюючи їх віртуальним комп'ютерам, користувач або адміністратор може впливати на виконання певної ВМ на певному хості. Тобто група спорідненості відображає бажану для користувача асоціацію між ВМ та хостом, який її виконує. У випадку поєднання гіпервізорів та серверів сховищ на одному фізичному сервері такий підхід дає змогу уникнути ситуації, коли віртуальну машину виконує один гіпервізор, а її віртуальний диск знаходиться на іншому. Якщо є необхідність у ви-

користанні груп спорідненості, то їх створення доцільно проводити до розгортання віртуальних машин.

Приналежність віртуального комп'ютера до певної мережі можна визначити лише у випадку використання розширеного режиму функціонування хмарної інфраструктури. Користувач має можливість «приєднати» ВМ до кількох віртуальних мереж (рис. 9.8), проте він мусить обрати мережу за замовчуванням – ту яка передаватиме публічний трафік в інтернет.

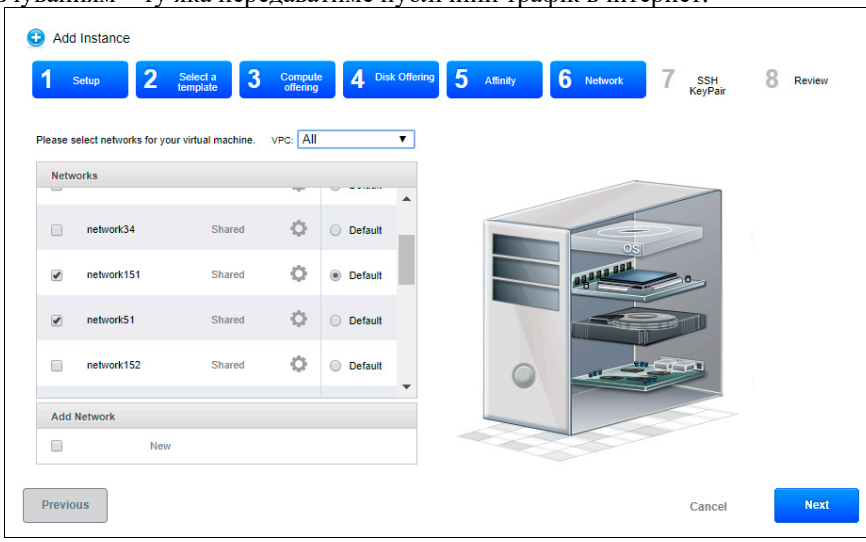

Рис. 9.8. Створення ВМ: вибір гостьових мереж

На останньому кроці віртуальній машині присвоюють назву. Після натискування на кнопку *Запуск ВМ (Lanch VM)*, потрібно зачекати, поки буде розгорнута віртуальна машина (час залежить від багатьох факторів, зокрема завантаженості гіпервізорів, доступності системних ВМ). Створений віртуальний комп'ютер буде відображатися на сторінці *Машини (Instances)*. Зелений колір поля *«Стан»* свідчить про те, що віртуальний комп'ютер завантажено. Перейшовши за гіперпосиланням, яке відповідає назві віртуального комп'ютера, можна побачити 3 вкладки (рис. 9.9), перша з яких – *Деталі (Details)* містить відомості про віртуальний комп'ютер, друга – NIS – дані про мережні з'єднання, третя – статистику функціонування ВМ.

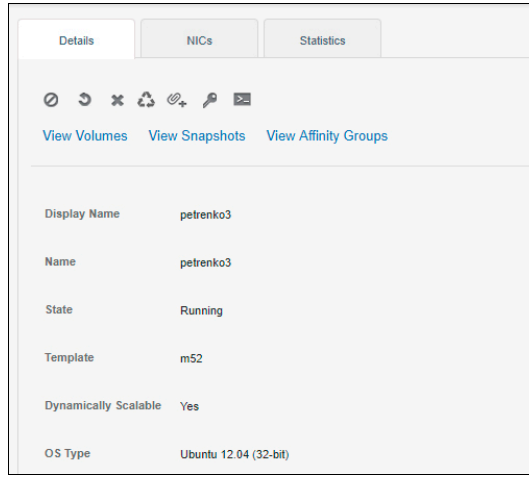

Рис. 9.9. Сторінка віртуальної машини

На рис. 9.8 доступні такі відомості про ВМ: назва (name) – petrenko3, стан (state) – завантажена, шаблон (template) – m52, можливість динамічної зміни обсяга диска (dynamically scalable), тип ОС (OS Type) – Ubuntu 12.04 тощо.

У верхній частині сторінки ВМ відображено панель її інструментів (рис. 9.10).

Рис. 9.10. Панель інструментів віртуальної машини

За її допомогою користувач може виконувати такі дії:

- вимкнути машину;
- перезавантажити машину:
- видалити її;
- відновити початковий стан (reinstall) – не варто використовувати;
- приєднати ISO-образ;
- переглянути консоль (графічний інтерфейс) віртуальної машини.

Останнє гіперпосилання відкриває нове вікно браузера, у якому відображається інтерфейс ОС (рис. 9.11)

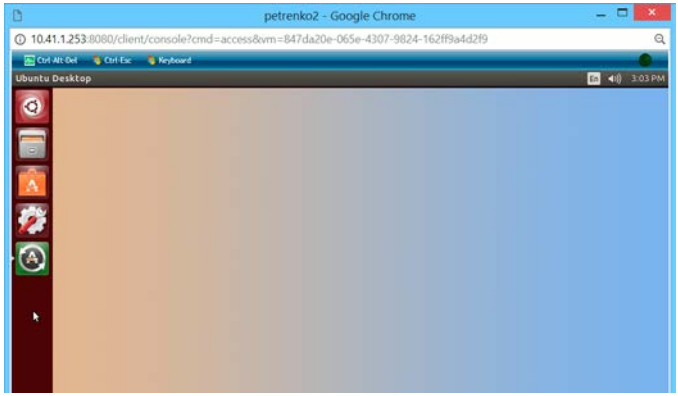

Рис. 9.11. Графічний інтерфейс ОС у консолі віртуальної машини

Вгорі вікна, яке містить консоль присутнє меню, яке дозволяє скористатися системними комбінаціями клавіш Ctrl+Alt+Delete, Ctrl+Esc, а також обрати мову введення віртуальної клавіатури.

Використовуючи вкладку NICS, користувач має змогу:

- переглянути мережні з'єднання ВМ;
- додати або видалити ВМ з гостьової мережі;
- створити запит на виділення додаткових IP-адрес.

За умови правильного налаштування мережних з'єднань хмарної інфраструктури та віртуального комп'ютера до нього можливий віддалений доступ засобами загальноприйнятих протоколів: SSH, RDP, VNC тощо. Варто зауважити, що за відображення інтерфейсу ОС у консолі ВМ відповідає системна ВМ Console Proxy. Отож, користувач може використовувати інтерфейс ОС віртуального комп'ютера, не залежно від того, чи присутні у ній мережні адаптери або правильно налаштовані мережні з'єднання.

На вкладці *Статистика (Statistic)* користувачеві доступна така інформація:

- кількість та частота ядер центрального процесора (ЦП);
- відсоток використання ЦП віртуального комп'ютера;
- обсяг переданих та отриманих даних з мережі;
- кількість операцій зчитування та запису диска, а також відповідні обсяги даних.

За допомогою кнопки *Метрика (Metrics)*, яка присутня у правому верхньому куті сторінки *Машини (Instanses)*, користувач має змогу переглянути статистику по усіх машинах (рис. 9.12)

Resources				CPU Usage «			Mem Usage «	Network Usage «		Disk Usage		«
Name	State	IP Address	Zone	Cores	Total	Used	Allocated	Read	Write	Read	Write	IOPS
petrenko4			zone1	1	1.0 Ghz	2.19%	1.00 GB	0.00 MB	0.06 MB	7063.53 MB	3936.53 MB	391022
petrenko3			zone1	1	0.5 Ghz	0.04%	0.50 GB	545.03 MB	15.48 MB	2167.62 MB	6608.89 MB	527198

Рис. 9.12. Зведена статистика за усіма віртуальними машинами користувача

9.2.7 Розгортання хмарної інфраструктури на основі платформи Apache CloudStack

Використовуючи веб-інтерфейс, адміністратор має можливість створювати та керувати об'єктами хмарної інфраструктури мережами, доменами, проектами, віртуальними машинами, обліковими записами користувачів тощо. Також у веб-інтерфейсі можна змінювати загальні параметри конфігурації платформи. Адміністратор може виконувати з віртуальними машинами ті ж дії, що й користувач.

При першому вході адміністратора після встановлення платформи, йому буде запропоновано провести початкове конфігурування хмарної інфраструктури за допомогою майстра. За його допомогою можна розгорнути найпростішу конфігурацію хмари, яка містить одну зону, стійку, кластер, хост. На хості може виконуватися один з двох гіпервізорів – KVM або XenServer. Для забезпечення функціонування сховищ можна використати лише NFS-сервер. Оскільки майстер допомагає розгорнути хмарну інфраструктуру у базовому режимі, то вона міститиме лише одну фізичну мережу.

Якщо адміністратор має досвід управління хмарою на основі Apache CloudStack, то він може відмовитися від її конфігурування за допомогою майстра та перейти до створення інфраструктури в ручному режимі за допомогою інтерфейсу адміністратора (рис. 9.13).

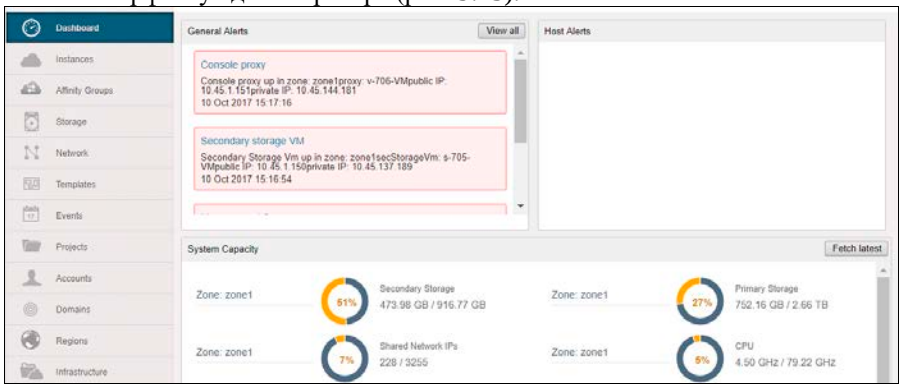

Рис. 9.13. Інтерфейс адміністратора платформи Apache CloudStack

Розглянемо процес розгортання хмарної інфраструктури на основі зони, яка працює розширеному режимі. Для її створення слід за допомогою меню перейти на сторінку *Інфраструктура (Infrastructure)*, яка відображатиме відомості про основні компоненти хмари та їх кількість. У правому верхньому куті сторінки *Зони (Zone)* У правому верхньому куті сторінки потрібно обрати кнопку *Додати зону (Add zone)* та вказати режим її роботи – *розширена зона (advanced zone)*. Додатково на сторінці вибору типу зони можна встановити використання груп безпеки, які забезпечують ізоляцію віртуальних машин. У цьому випадку кожен користувач платформи матиме змогу визначати правила фільтрування трафіку, який передається до його ВМ. На сторінці налаштування зони адміністратор хмари повинен вказати:

- назву зони;
- IP-адресу сервера DNS, який обслуговуватиме віртуальні комп'ютери у загальнодоступній мережі;
- IP-адресу сервера DNS, який обслуговуватиме віртуальні комп'ютери у приватній мережі;
- тип гіпервізора;
- використання зони для певного домена користувачів (не обов'язково);
- адресу та маску підмережі для гостьової мережі (не обов'язково);
- необхідність використання локальних сховищ для системних або користувацьких ВМ.

На наступному кроці виконують конфігурування мережі зони. Адміністратор хмари повинен вказати типи трафіку та інтерфейси, через які вони передаються. Розглянемо на прикладі як відбувається конфігурування мережі зони, яка функціонує у розширеному режимі. Нехай адміністратор планує розгорнути інфраструктуру, у якій для користувачів можна виділити кілька гостьових мереж (рис. 9.14).

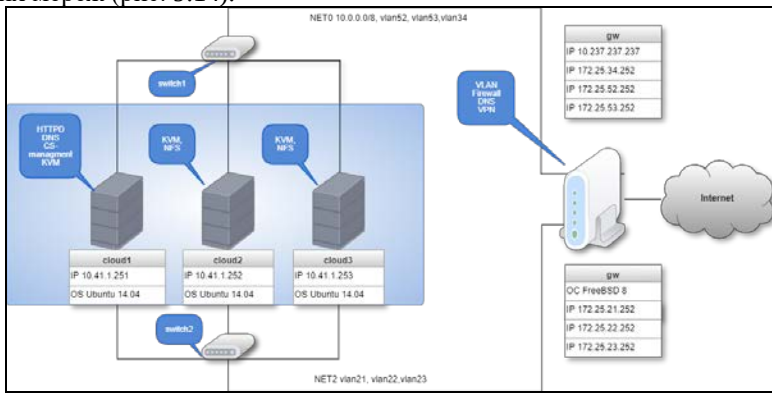

Рис. 9.14. Схема мережі розширеної зони.

З наведеного рисунку видно, що у хмарній інфраструктурі використовується 2 фізичні мережі. Мережа *NET0* з адресою 10.0.0.0/8, що призначена для передавання усіх видів трафіку (управління, загальнодоступного, гостьового, трафіку сховищ). Фізичні та віртуальні комп'ютери цієї мережі з'єднує комутатор другого рівня *switch1*. Крім того, у мережі *NET0* передається гостьовий трафік, який розподіляється у 3-ох віртуальних локальних мережах (VLAN) – *vlan52, vlan52, vlan34*. Аналогічно у мережі *NET2*, пристрої якої з'єднує комутатор *swith2*, гостьовий трафік розподіляється у мережах *vlan21, vlan22,vlan23*. Маркування трафіку віртуальних мереж виконує маршрутизатор *gw*. Функціонування хмарної інфраструктури забезпечують 3 сервери: *cloud1, cloud2, cloud3*. Незважаючи на застереження, які були наведені у попередніх параграфах, адміністратор хмари, з метою заощадження коштів, налаштував сервер *cloud1* для виконання функцій сервера керування, хоста, сервера первинного та вторинного сховищ. Сервери *cloud2, cloud3* виконуватимуть функції хостів, а також серверів первинних сховищ. На думку адміністратора така архітектура дозволить максимально ефективно використати обчислювальні потужності серверів, та мінімізувати трафік, що передається між гіпервізорами та сховищами. Зауважимо, що на кожному з серверів встановлено мережні адаптери, для яких сконфігуровані мережні мости *cloudbr0* та *cloudbr2*, які відповідають мережам *NET0* та *NET2*.

Отож, для реалізації зазначеної інфраструктури, у майстрі створення зони слід вказати (рис. 9.15):

Рис. 9.15. Конфігурування мережі розширеної зони.

- типи трафіку та відповідні фізичні мережні інтерфейси для їх передавання (виконують перетягуючи відповідні піктограми);
- метод ізоляції мереж (VLAN у нашому випадку);

- маркування трафіку.

Позначення кожного з видів трафіку необхідне гіпервізору для правильної роботи з мережними інтерфейсами. Для маркування кожного виду трафіку відповідно до його типу та інтерфейсу потрібно під кожною піктограмою трафіку перейти за гіперпосиланням *Редагувати (Edit)*. У вікні, яке з'явиться слід ввести назву відповідного інтерфейсу, у нашому прикладі *cloudbr0* або *cloudbr1*.

На наступному кроці слід вказати такі параметри адресування загальнодоступного трафіку:

- адресу шлюзу;
- маску підмережі;
- ідентифікатор VLAN;
- початкова та кінцева IP-адреси у діапазоні публічних IP-адрес.

Оскільки за передавання загальнодоступного трафіку відповідатимуть системні ВМ, то зазначений діапазон можна визначати не надто великим. Для ізоляції публічного трафіку від інших видів можна використати ту ж технологію VLAN. Проте ця вимога є необов'язковою. Для вищенаведеного прикладу діапазони можуть бути такими (рис. 9.16):

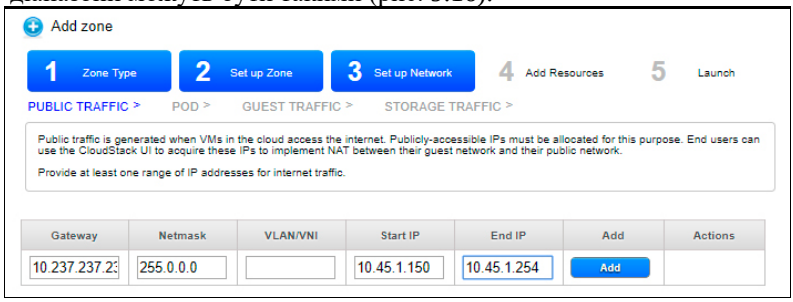

Рис. 9.16. Конфігурування діапазону загальнодоступної мережі розширеної зони.

У подальшому майстер створення зони запропонує створити стійку, що вимагає введення її назви, діапазону IP-адрес, маски підмережі та адреси шлюзу. Зауважимо, що зазначені діапазони зони та стійки не повинні перетинатися. Для опрацювання гостьового трафіку у процесі конфігурування стійки варто вказати діапазони, у межах яких будуть використовуватися ідентифікатори VLAN. Подібно загальнодоступного та гостьового налаштовують адресування трафіку сховищ.

У процесі додавання хоста слід ввести його IP-адресу, ім'я та пароль користувача, який має привілеї на створення та запуск віртуальних машин. Таким користувачем може бути *root* – адміністратор ОС. У цьому випадку на серверах, які виконуватимуть роль хостів, у конфігурації сервера SSH (Secure

SHell) слід дозволити віддалений вхід користувача root (змінити параметр *PermitRootLogin*). Якщо ж передбачено, що робота з віртуальними машинами буде здійснюватися від імені іншого облікового запису, то слід надати йому відповідні привілеї у файлі */etc/sudoers*.

Додавання до зони первинного сховища передбачає вказання:

- імені сховища;
- його доступності в межах зони або кластера;
- протоколу, за яким здійснюватиметься доступ;
- IP-адреси сервера;
- шляху до спільного ресурсу.

Якщо у зоні потрібно використовувати групи спорідненості (affinity groups), то на етапах додавання хостів та сховищ також вводять теги, які відповідають їх назвам (наприклад cloud1). Додавання вторинного сховища принципово не відрізняється від первинного.

Після введення даних усіх складових хмарної інфраструктури платформа Apache CloudStack протягом деякого часу виконуватиме розгортання хмари: створення зони, стійки, кластера, фізичних мереж, додавання хоста, сховищ, запуск системних віртуальних машин. У випадку успішного виконання усіх операцій, на сторінці інфраструктури буде відображено усі складові (рис. 9.17).

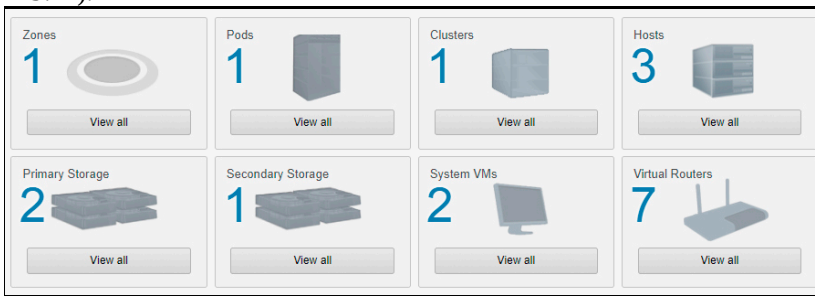

Рис. 9.17. Складові хмарної інфраструктури.

Натиснувши на потрібний об'єкт, можна перейти на сторінку його конфігурування. На сторінці *Зони (Zones)* можна переглянути:

- загальну інформацію про зону;
- структуру її об'єктів;
- мережні параметри;
- конфігурацію фізичних мереж та відповідних трафіків;
- статистику виділених ресурсів;
- стан системних ВМ;
- загальні параметри.

На рис. 9.18 наведено графічне подання фізичних мереж для розглянутого прикладу.

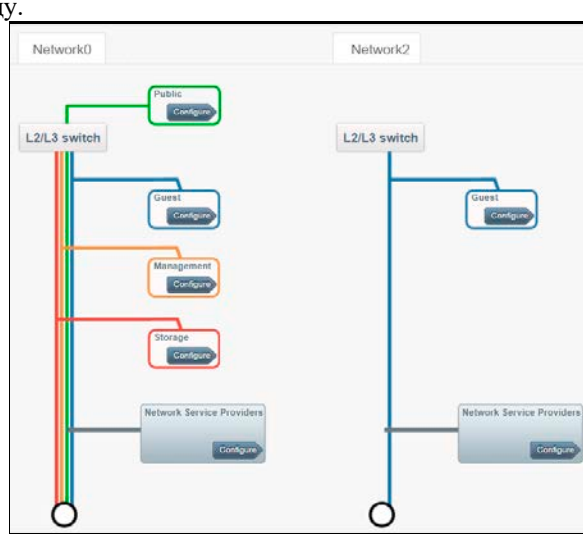

Рис. 9.18. Графічне подання фізичних мереж зони.

Використовуючи панель інструментів на сторінці зони, адміністратор має змогу:

- вимкнути зону;
- змінити її мережні налаштування (діапазон IP-адрес, маску, адресу шлюзу тощо);
- резервувати зону (dedicate zone);
- видалити зону.

Нагадаємо, що резервування об'єктів інфраструктури Apache CloudStack можливе для окремих користувачів або певного домену. Видалити зону можна лише у випадку відсутності у ній об'єктів (сховищ, хостів, кластерів, стійок, мереж, системних ВМ). Аналогічні дії можна виконувати для стійки, кластера, хотів, сховищ. Наприклад, перейшовши на сторінку хостів, можна додати, видалити, вимкнути або перевести хост у режим обслуговування. Видалення об'єктів хмарної інфраструктури Apache CloudStack здійснюється у порядку зворотному до їх створення.

У подальшому можна перейти до додавання гостьових мереж у хмарну інфраструктуру. У налаштуваннях зони потрібно по черзі обрати потрібні мережні інтерфейси, до яких додати теги. Нехай для запропонованого випадку такими мітками є *gnet0* – для моста *cloudbr0*, та *gnet2* – для *cloudbr2* (рис. 9.19).

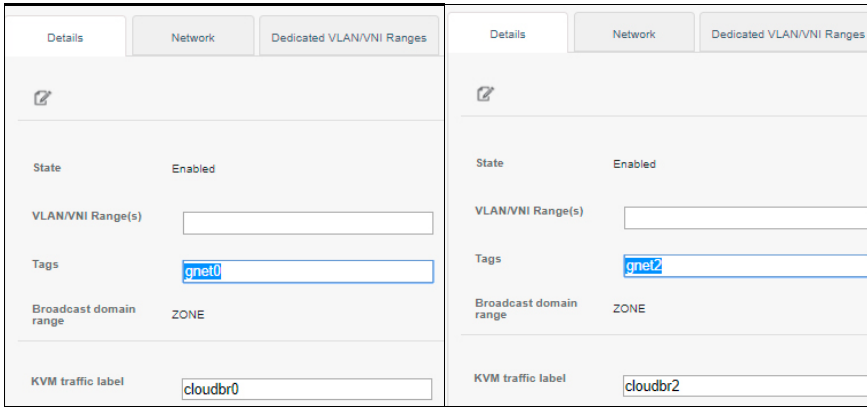

Рис. 9.19. Додавання тегів мережних інтерфейсів.

Далі за допомогою меню **Системні послуги (System offerings)** для кожної з фізичних мереж слід створити свій шаблон. У правому верхньому куті сторінки *Мережні послуги (Network offerings)* обираємо гіперпосилання *Додати мережні послуги (Add network offerings)*. У вікні, що завантажиться потрібно вказати:

- назву та опис шаблону;
- максимальну пропускну швидкість мережі (не обов'язково);
- тип гостьової мережі – спільна чи ізольована;
- сервіси, які доступні мережі;
- мітку фізичного інтерфейсу.

Для кожної гостьової мережі доступні сервіси: віртуальні приватні мережі (VPN), сервіс динамічного призначення IP-адрес (DHCP), сервер DNS, брандмауер (firewall), балансувальник навантаження, NAT-перетворювач (SNAT та DNAT), групи безпеки та інші. Пригадаємо, що у розгорнутій хмарній інфраструктурі адміністратору потрібно забезпечити функціонування 3-ох гостьових мереж *vlan52, vlan52, vlan34*, які асоційовані з мережею *NET0*, та 3-ох мереж *vlan21, vlan22,vlan23*, які асоційовані з мережею *NET2*. Нехай у мережах *vlan52, vlan52, vlan34* потрібно забезпечити автоматизоване призначення IP-адрес, а у мережах *vlan21, vlan22,vlan23* користувачі мають налаштовувати адресацію своїх віртуальних комп'ютерів вручну. У цьому випадку адміністратору слід створити 2 шаблони мережних послуг, які зображені на рис. 7.20.

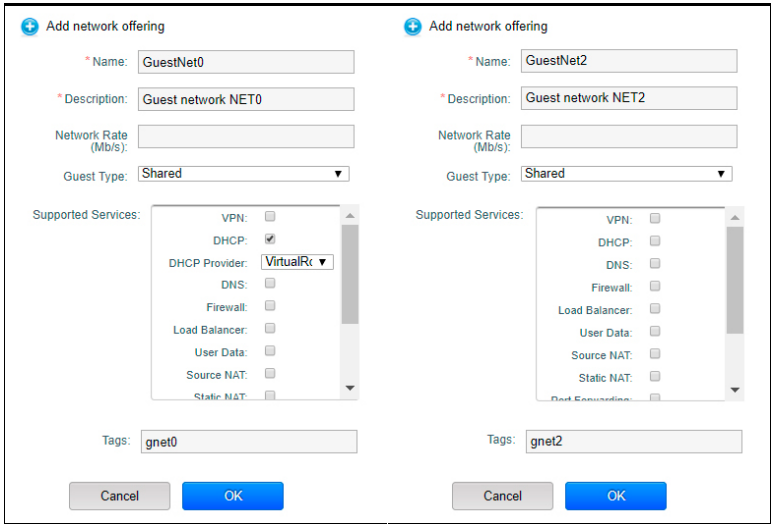

Рис. 9.20. Створення шаблонів мережних послуг.

На останньому етапі адміністратор може додати потрібну кількість гостьових мереж. Для цього на сторінці *Мережа (Network)* слід перейти за гіперпосиланням *Додати гостьову мережу (Add guest network)*. У вікні, що завантажиться вказуємо (рис. 9.21):

- назву та опис мережі;
- зону;
- фізичну мережу, у якій буде функціонувати гостьова мережа;
- ідентифікатор VLAN мережі;
- доступність мережі (доступна для усіх, для певного користувача або у межах домену);
- створений шаблон мережних послуг;
- початкову та кінцеву IP-адреси діапазону, з якого будуть адресуватися віртуальні комп'ютери користувачів;
- маску підмережі;
- шлюз, який буде виконувати маршрутизацію ВМ мережі.

Зауважимо, що платформа працює з обома версіями протоколу IP, отож у процесі створення хмарної інфраструктури, зокрема і при додаванні гостьової мережі можна вказувати й адреси IPv6.

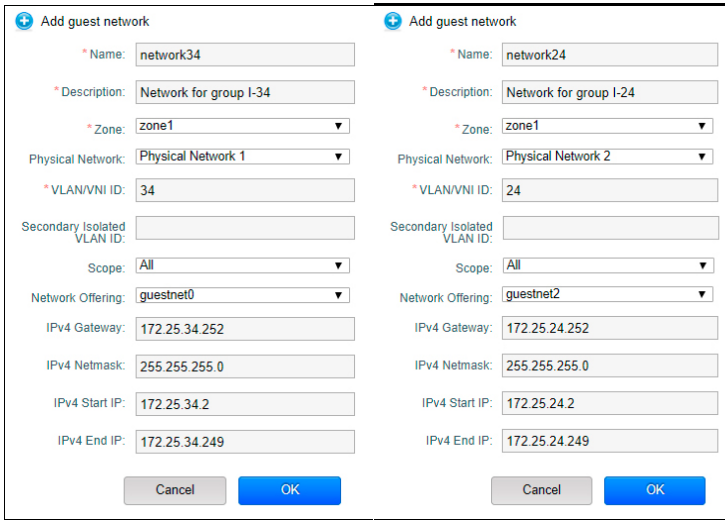

Рис. 9.21. Додавання гостьових мереж.

Для розширених зон платформа Apache CloudStack створює окрему системну ВМ –віртуальний роутер. Він використовується для маршрутизації гостьових мереж, для яких у шаблонах послуг призначено певні мережні сервіси (DHCP, VPN тощо). Зауважимо, що віртуальний роутер використовує IP-адресу, яка була вказана як адреса шлюзу при додаванні гостьової мережі. Цю особливість слів враховувати налаштовуючи фізичний маршрутизатор хмари. Стан та мережні параметри віртуального роутера можна переглядати на сторінці *Інфраструктура*, перейшовши до системних віртуальних машин.

Усі доступні гостьові мережі можна переглянути на сторінці зони, обравши певну фізичну мережу на вкладці *Мережі (Networks)* (рис. 9.22).

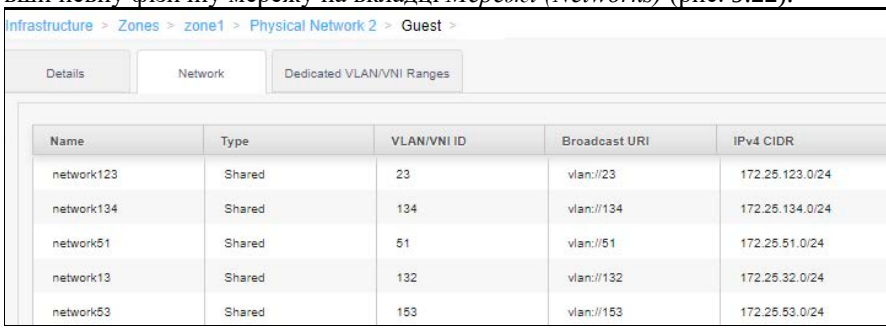

Рис. 9.22. Перегляд гостьових мереж

Після таких налаштувань у кожну із віртуальних машин можна додавати мережні адаптери, які працюватимуть в різних підмережах. Зазначена операцію виконують на сторінці ВМ, у вкладці *Мережні інтерфейси (NICS)*, перейшовши за гіперпосиланням *Додати мережу до ВМ (Add network to VM)***.** Після вибору мережі, вона з'явиться у переліку мереж віртуального комп'ютера, а у користувача, який створив ВМ, буде можливість змінювати її параметри.

9.2.8 Основи адміністрування платформи Apache CloudStack

Адміністрування хмарної платформи передбачає розгортання інфраструктури, управління її об'єктами, роботу з користувачами, розподіл обчислювальних ресурсів тощо. Подібно до облікових записів груп користувачів ОС, платформа Apache CloudStack підтримує надання користувачам ролей. Роль визначає допустимі функції користувача. Всі облікові записи CloudStack мають призначену певну роль, яка забезпечує дотримання правил доступу до об'єктів, а також повноваження на виконання запитів, які містять API-функції. Зазвичай існує чотири ролі за замовчуванням: адміністратор платформи, адміністратор ресурсу, адміністратор домену та користувач. Облікові записи користувачів у системі можна згрупувати за доменами або проектами.

У межах домену ім'я користувача має бути унікальним. Оскільки домени використовують ієрархічну структуру, то їх імена можуть повторюватися, але повний шлях до домену, починаючи з кореня (root), має бути унікальним. Наприклад, можна створити такі 2 домери */root/fm/i34*, а також */root/ipf/i34*.

Адміністратори – це облікові записи, які мають особливі привілеї. У системі можуть бути декілька адміністраторів. Адміністратори можуть створювати або видаляти інших адміністраторів та змінювати пароль для будь-якого користувача в системі. Адміністратори домену можуть виконувати адміністративні операції стосовно користувачів, які належать зазначеному домену. Адміністратори домену не можуть виконувати свої функції на фізичних серверах або інших доменах хмарної інфраструктури. Адміністратори кореневого домену мають повний доступ до системи, зокрема можуть керувати шаблонами, сервісними послугами, адміністраторами доменів тощо. Ресурси стосуються облікових записів. Користувач може використовувати будь-який ресурс, за умови, що він має повноваження на виконання певної операції. Наприклад, кореневий адміністратор може змінити власника будь-якої віртуальної машини інфраструктури і тим самим надати усі повноваження до роботи з нею іншому обліковому запису. Адміністратор домену або субдомену може зробити таку ж операцію стосовно віртуальних машин і користувачів у межах свого домену або його субдоменів.

Адміністратор виконує резервування ресурсів для певного домену чи облікового запису користувача. У такий спосіб можна забезпечити приват-

ність інфраструктури у контексті її продуктивності або гарантій безпеки. Зона, стійка, кластер або хост може бути зарезервований адміністратором кореневого домену для певного домену або облікового запису. Унаслідок цього лише користувачі цього домену або дочірніх доменів зможуть використовувати резервовану інфраструктуру.

Нині платформа Apache CloudStack надає такі типи резервування:

- явне – зона, стійка, кластер або хост резервуються лише для облікового запису або домену кореневим адміністратором під час початкового розгортання та конфігурації хмари;
- строге неявне, яке передбачає, що хост не буде доступний для кількох облікових записів; зазначене резервування буває корисним при розгортанні певних типів програм на віртуальному комп'ютерів, які, не порушуючи умови ліцензування, не можуть бути розподілені кількома обліковими записами;
- нестроге неявне – ВМ буде розгорнуто у спеціальній резервованій інфраструктурі, якщо це можливо, в іншому випадку вона може буде розгорнута у спільній інфраструктурі.

Явне резервування виконується під час розгортання нової зони, стійки, кластера чи хоста. Для цього адміністратору на сторінці конфігурування об'єкту слід обрати відповідну опцію та вказати домен або обліковий запис для резервування. Наприклад, щоб зарезервувати хост cloud3 для користувача petrenko_im із домену i34, слід на його сторінці у панелі інструментів обрати гіперпосилання, яке містить символ «+» та вказати потрібний домен (рис. 9.23).

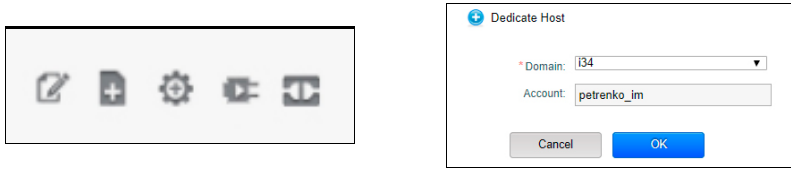

Рис. 9.23 Явне резервування хоста

Для забезпечення неявного резервування адміністратор, створюючи шаблон обчислювальних послуг, повинен у полі *Планування (Deployment planner)* вказати необхідність неявного планування *(ImplicitDedicationPlanner)*. Після цього у полі *Режим Планувальника (Planner mode)* буде доступний вибір режиму неявного резервування – строге або нестроге. Кожного разу, коли користувач створюватиме віртуальну машину на основі цього резервування, вона буде виконуватися на одному з виділених хостів.

Створення шаблонів обчислювальних послуг здійснюють за допомогою пункта меню *Service Offerings*. Перейшовши за гіперпосиланням *Додати обчислювальну послугу (Add compute offering),* визначають його основні характеристики (рис. 9.24):

- назву та опис шаблону;
- тип сховища – локальне або спільне мережне;
- кількість ядер процесора, які будуть виділені ВМ;
- обсяг оперативної пам'яті;
- максимальну швидкість передавання даних в мережі;
- теги хостів та сховищ;
- загальноступний чи резервований спосіб використання ресурсів.

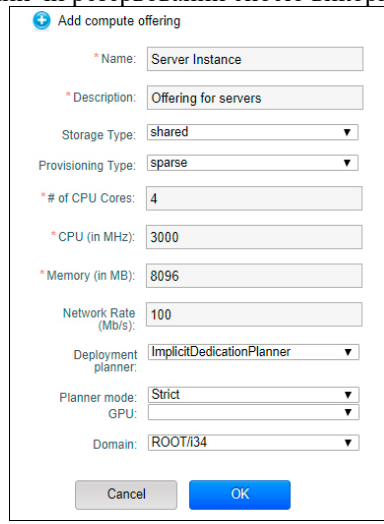

Рис. 9.24 Створення шаблона обчислювальних послуг

Для використання користувачем явного виділеного хосту, йому слід створити споріднену групу, яку вказати при розгортанні ВМ. Адміністратор може переміщувати віртуальні комп'ютери хостів чи сховищ на інші ресурси незалежно від способу їх резервування. У процесі такої операції платформа Apache CloudStack лише виведе застереження, проте виконає її. У випадку, якщо для хоста визначено строге резервування, але адміністратором не створено мітки, які використовує ВМ користувача, то вона не буде розгорнута.

Якщо адміністратор видалить обліковий запис або домен, усі складові інфраструктури, які були резервовані для нього, будуть звільнені. Тобто вони будуть доступні для спільного використання будь-яким обліковим записом

або доменом. У адміністратора існує можливість повторно резервувати їх для іншого облікового запису або домену.

Системні ВМ та віртуальні маршрутизатори впливають на можливість резервування хоста. Оскільки вони належать системному обліковому запису CloudStack, то можуть бути розгорнуті на будь-якому хості. Виконання системних ВМ та віртуальних маршрутизаторів на певному хості встановлює його недоступним для строгого резервування, проте не заперечує використання неявного, нестрогого виділення його обчислювальних ресурсів.

Робота адміністратора з користувачами передбачає створення, редагування, видалення їх облікових записів. Перейшовши на сторінку *Облікові записи (Accounts)*, можна переглянути перелік користувачів системи або окремого домену.

Створюючи новий обліковий запис користувача, слід вказати такі основні параметри(рис. 9.25):

- логін та пароль;
- адресу електронної пошти користувача;
- його ім'я та прізвище;
- домен, до якого буде належати обліковий запис;
- обліковий запис (не обов'язково);
- повноваження (адміністратор чи користувач).

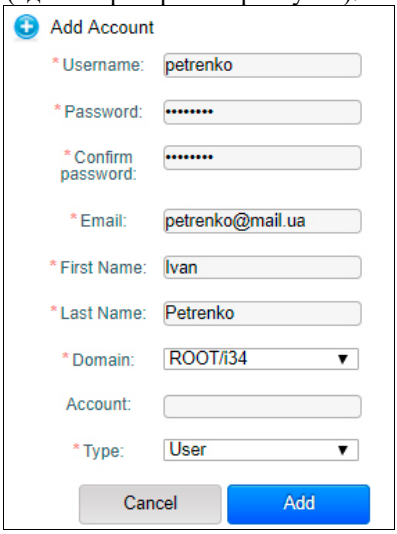

Рис. 9.25 Створення облікового запису користувача

Зауважимо, що параметр *Обліковий запис (Account)* забезпечує автентифікацію та роботу кількох користувачів у межах одного облікового запису.

Платформа Apache CloudStack може забезпечувати автентифікацію на основі даних зовнішньої бази, зокрема LDAP-каталогу. Він може міститися на LDAP-сервері такому як Microsoft Active Directory або Apache Directory Server. Для доступу до бази облікових записів користувачів Active Directory використовують протокол доступу до каталогів (LDAP – Lightweight Directory Access Protocol). Основне поняття – об'єкт каталогу можна уявити як таблицю бази даних. Вузли в ієрархії каталогу LDAP містять дані про об'єкт і є аналогічними записам реляційної бази. Характеристики об'єкта містять атрибути, які є аналогом полів. Рівні у ієрархічному дереві іменують за допомогою загально прийнятих позначень: країна – «C» (country), рівень організації – «OU», імена користувачів – «CN» (common name). Оскільки об'єкт у структурі LDAP має бути унікальним, то для його опису використовують унікальне ім'я (DN – Distinguished Name). Унікальне ім'я отримують послідовним визначенням значень атрибутів (C, OU, CN тощо). Наприклад, *CN=petrenko,OU=I34,OU=Students,OU=Domain Users,DC=w,DC=fizmat,DC=tnpu,DC=edu,DC=ua*.

У процесі автентифікації Apache CloudStack виконує пошук у зовнішньому дереві каталогів LDAP. Адміністратор може обмежити пошук певною частиною дерева (*BaseDN*), починаючи з вказаного базового каталогу, і отримати такі дані про користувача: логін, ім'я, прізвище, та електронна адресу. Для автентифікації традиційно використовуються логін та пароль, введені користувачем. Apache Cloudstack виконує пошук у власній базі користувача з уведеними даними. Якщо він існує, система виконує запит на зв'язування з DN і паролем.

Оскільки Active Directory є службою каталогів, яка не підтримує анонімні запити, то для пошуку даних необхідно створити окремий обліковий запис користувача, від імені якого здійснюватиметься зчитування даних.

Налаштування автентифікації на основі LDAP-каталогу здійснюють на торінці *Загальні налаштування (Global Settings).* Обравши вигляд *Конфігурація LDAP (LDAP Configuration),* вказують IP-адресу та порт сервера LDAP. Щоб увести інші параметри потрібно змінити вигляд на *Загальні налаштування (Global Settings)* (табл. 9.1) та у рядку пошуку праворуч ввести *ldap*.

Таблиця 9.2. Параметри з'єднання за протоколом LDAP з сервером Microsoft Active Directory

Атрибут	Можливе значення	Опис
ldap.basedn	OU=Users,DC=w,DC=fizmat, DC=tnpu,DC=edu,DC=ua	підкаталог, починаючи з якого здійснюють пошук даних
ldap.bind.principal	cn=ldapuser,ou=administrators, dc=fizmat,dc=tnpu,dc=edu,dc=	Шлях до об'єкта користувача, з привілеями якого

	ua	буде здійснено пошук
ldap.bind.password	**********	пароль користувача, вказаного у параметрі ldap.bind.principal
distinguishedName	CN=petrenko,OU=I34,OU=Students,OU=Users,DC=w,DC=fizmat,DC=tnpu,DC=edu,DC=ua	місцезнаходження об'єкта в дереві каталогів Active Directory
displayName	Петренко Іван	ім'я, яке буде виведено
ldap.username.attribute	sAMAccountName	логін
ldap.lastname.attribute	LastName	прізвище
ldap.firstname.attribute	FirstName	ім'я
mail	petrenko@fizmat.tnpu.edu.ua	електронна пошта
ldap.group.object	group	атрибут належності до групи
ldap.search.group.principle	CN=cloudstack,OU=Fizmat,OU=Students,OU=Users,DC=fizmat,DC=tnpu,DC=edu,DC=ua	шлях у каталозі до об'єкту групи, користувачі якої матимуть доступ до хмари
ldap.provider	microsoftad	тип LDAP-каталогу

Також існує можливість налаштувати платформу для роботи з кількома LDAP-серверами. У цьому випадку дані на них мають реплікувалися. Якщо система не зможе отримати дані з одного з них, то буде використовувати наступний. Якщо LDAP-сервер працює за захищеним протоколом SSL, слід налаштувати його підтримку. Спочатку потрібно отримати сертифікат, який використовує сервер LDAP, і додати його на диск сервера управління та вказати шлях та пароль до цього (атрибути ldap.truststore, ldap.truststore.password).

Поточна версія платформи автоматично не створює обліковий запис користувача у свій базі після першої його вдалої автентифікації. У зв'язку з цим після встановлення параметрів доступу до LDAP-каталогу, слід додати користувачів з нього у базу Apache CloudStack. Це здійснюють на сторінці *Облікові записи (Accounts),* використовуючи гіперпосилання *Додати обліковий запис LDAP (Add LDAP Account)*. У вікні, що завантажиться, обирають один або кілька облікових записів, вказують домен, повноваження та інші параметри (рис. 9.26).

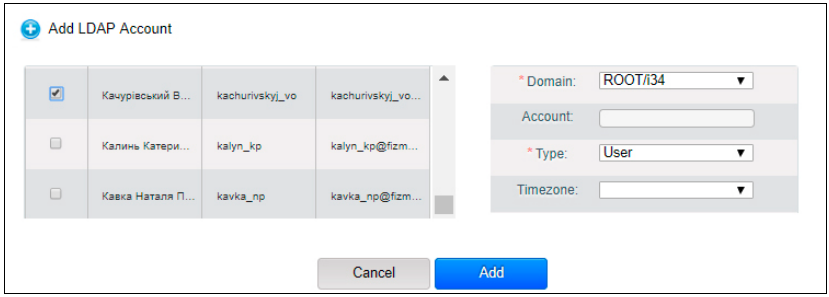

Рис. 9.26 Додавання облікового запису користувача з LDAP-каталогу

Зауважимо, що у випадку надання доступу лише для певної групи користувачів з LDAP-каталогу за допомогою параметра *ldap.search.group.principle*, пошук облікових записів буде швидшим. Якщо потрібно додавати користувачів у різні домени, то можна почергово долучати їх до зазначеної групи.

Як було зазначено вище, Apache CloudStack використовує домени для спрощення адміністрування облікових записів користувачів. Створення доменів здійснюють на однойменні сторінці. При цьому можна вказати так званий мережний домен – суфікс DNS, який буде стосуватися мережі, облікового запису, домену, зони у хмарній інфраструктурі. Існує можливість зв'язування домена з групою або підрозділом LDAP-каталогу. Для цього у панелі інструментів на сторінці доменів слід обрати *гіперпосилання Зв'язати домен із LDAP (Link domain to LDAP)*. У вікні, що завантажиться слід вказати (рис. 9.27):

- тип зв'язування – на основі групи чи підрозділу (group або OU);
- повний шлях до об'єкта (групи чи підрозділу);
- тип облікового запису – користувач чи адміністратор домену;
- адміністратор домену (не обов'язково).

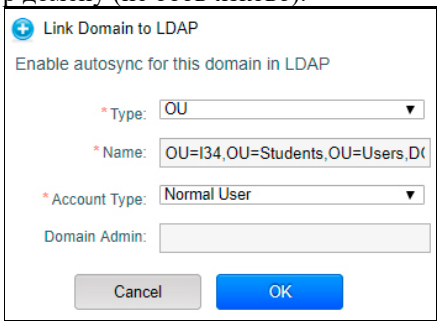

Рис. 9.27 Зв'язування домену з підрозділом у LDAP-каталозі

Для організації спільної роботи користувачів у платформі Apache CloudStack передбачено так звані *проекти (projects)*. Користувачі одного домену можуть об'єднуватися в команди проекту, що дає змогу їм співпрацювати та спільно використовувати віртуальні ресурси, зокрема ВМ, їх архіви (знімки), шаблони, диски даних, IP-адреси тощо. Система відслідковує використання ресурсів як для проекту вцілому, так і для кожного користувача зокрема. У зв'язку з цим існує можливість отримання статистичних даних, які стосуються облікового запису користувача та проекту. Наприклад, у корпоративній хмарі може бути створений проект для працівників відділу контролю якості. Адміністратор хмари матиме змогу відстежувати ресурси, що використовуються при тестуванні. Члени проекту можуть спростити ізоляцію своїх ресурсів від інших користувачів.

Перед тим, як користувачі хмарної інфраструктури зможуть використовувати проекти, адміністратор платформи Apache CloudStack повинен налаштувати різні системи їх підтримки, які передбачають запрошення до членства, виділення ресурсів проекту та обмеження кола користувачів, що зможуть створювати проекти.

Платформу можна налаштувати так, щоб адміністратори проекту могли додавати користувачів безпосередньо до нього або надсилали запрошення, яке повинен прийняти користувач. Запрошення можна надіслати електронною поштою або через обліковий запис користувача. Якщо потрібно, щоб адміністратори використовували запрошення, слід увімкнути та налаштувати функцію запрошень. Це здійснюються на сторінці *Глобальні налаштування (Global Settings)*, увівши до поля пошуку, яке знаходиться праворуч, рядок *project*. У таблиці 9.2 наведено відфільтровані параметри:

Таблиця 9.3. Параметри конфігурації запрошень до проектів у платформі Apache CloudStack

Атрибут	Опис
allow.user.create.projects	дозвіл користувачам створювати проекти
project.invite.required	використання запрошень до участі в проекті
project.email.sender	email відправника запрошення
project.invite.timeout	час очікування надсилання запрошення
project.smtp.host	SMTP-сервер, що відправлятиме запрошення
project.smtp.port	порт SMTP-сервера
project.smtp.useAuth	використання автентифікації SMTP-сервером
project.smtp.username	обліковий запис SMTP-сервера
project.smtp.password	пароль облікового запису SMTP-сервера

Після зміни глобальних параметрів платформи слід виконувати перезавантаження сервісу за допомогою команди: *service cloudstack-management restart.*

Адміністратор хмари має змогу контролювати ресурси, які можуть бути виділені для кожного проекту. Це здійснюється для запобігання неконтрольованого використання ресурсів хмари, зокрема екземплярів ВМ, їх знімків, IP-адрес. Адміністратори домену мають змогу переозначити такі обмеження ресурсів для окремих проектів з їх доменами. Власник проекту або адміністратор домену моє змогу змінити ці обмеження в сторону їх зменшення. Власник проекту може встановлювати обмеження на ресурси лише у випадку, якщо він є адміністратором домену. Якщо проект вже використовує більше ресурсів, ніж встановлений новий максимум, його ресурси не зазнають зміни, однак, у адміністратора не буде можливості додавати нових ресурсів певного типу, поки їх значення не опуститься нижче встановленої межі.

Для створення нового проекту адміністратору слід перейти на відповідну сторінку, обрати гіперпосилання *Додати проект (Add Project)* та вказати його назву. Проект буде створено у домені, який відповідає адміністратору. На сторінці домену його адміністратору будуть доступні 3 вкладки: *деталі (details), облікові записи (accounts), ресурси (resources)* (рис. 9.28).

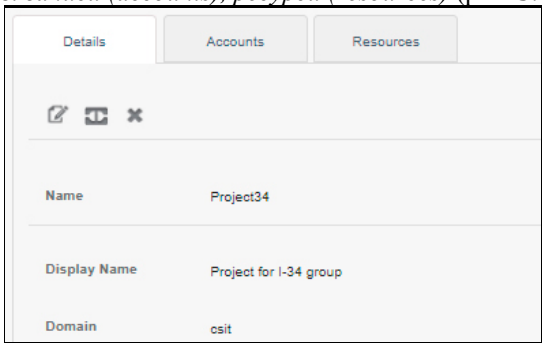

Рис. 9.28 Сторінка проекту

За допомогою першої вкладки можна переглянути та змінити основні відомості про домен. На цій вкладці можна вимкнути або видалити проект. Вимкнення домену робить його недоступним для користувачів, хоча й не змінює виділені для нього ресурси. Видалення проекту вивільняє резервовані для нього обчислювальні ресурси. Вкладка облікові записи (accounts) дає змогу переглядати, додавати та видаляти учасників проекту. За допомогою останньої вкладки *(resources)* адміністратор домену може встановити значення таких обчислювальних ресурсів, які будуть виділені для проекту:

- максимальну кількість ВМ користувача (max. user VMs);
- максимальну кількість публічних IP-адрес;
- максимальні кількості розділів, архівів, шаблонів, мереж;
- максимальну кількість ядер процесора;

- максимальний обсяг оперативної пам'яті;
- максимальні обсяги використовуваних первинного та вторинного сховищ.

Якщо у системі будуть активовані запрошення користувачів до проекту, то на його сторінці буде доступна відповідна вкладка – *Запрошення (Invitations)*. Прийняти запрошення користувач має змогу на сторінці проекту, змінивши відповідний вигляд, та обравши дію *Прийняти запрошення до проекту (Accept project invitation)* (рис. 9.29).

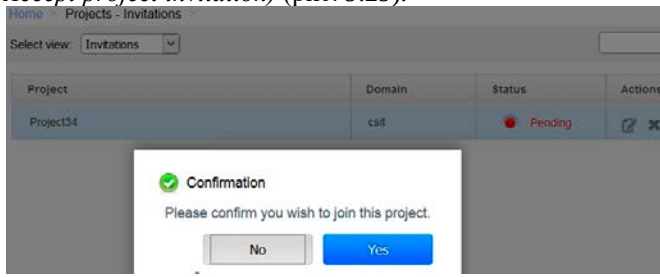

Рис. 9.29 Прийняття запиту на участь у проекті

Користувач може перейти до проекту на будь-якій сторінці платформи, обравши його у лівому верхньому куті. Після цього зміниться кольорова схема оформлення сайту. На інструментальній панелі користувача будуть доступними дані про проект (рис. 9.30):

- перелік його учасників;
- виділені обчислювальні ресурси;
- параметри мереж та безпеки проекту;
- події, що відбуваються з об'єктами проекту.

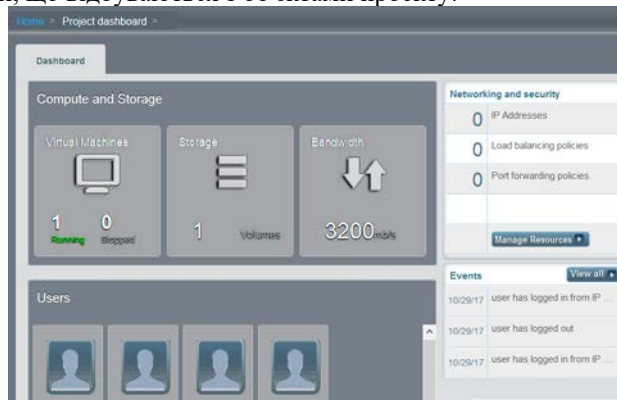

Рис. 9.30 Інструментальна панель проекту

Усі учасники проекту матимуть можливість одночасно працювати з віртуальними комп'ютерами, які створені в його межах. Говорячи про спільну діяльність учасників проекту, варто зауважити, що одночасно використовувати інтерфейс ВМ через консоль платформи зможе лише один користувач.

Шаблон є багаторазовою конфігурацією віртуальних машин. Створення віртуальних машин у платформі Apache CloudStack можливе на основі шаблонів або ISO-образів. Шаблоном є образ віртуального диска, який містить операційну систему, програмне забезпечення, системні та мережні параметри. Адміністратор має змогу визначити, хто може використовувати шаблон. Кожен шаблон асоціюється з певним типом гіпервізора, який вказується у процесі його створення.

За замовчуванням у платформі додано шаблон ОС Linux CentOS. Створювати та додавати шаблони до хмарної інфраструктури можуть не лише адміністратори, а й користувачі. Перед створенням шаблона слід встановити потрібне програмне забезпечення та виконати налаштування ОС. Потім варто вимкнути віртуальну машину. На сторінці машини, під панеллю її інструментів, можна помітити три гіперпосилання, за допомогою яких можна переглянути розділи, архіви та групи спорідненості ВМ. Перейшовши на сторінку розділів ВМ та обравши потрібний з них, можна побачити панель інструментів, яка стосується розділів (рис. 9.31):

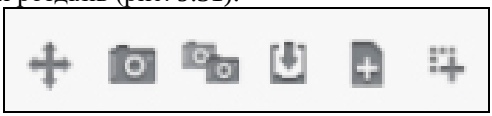

Рис. 9.32 Панель інструментів сторінки розділи

За її допомогою можна виконати такі дії:

- перенести розділ на інше первинне сховище (доступне лише для кореневого адміністратора);
- створити архів (знімок) розділу ВМ;
- запланувати повторюване створення архівів;
- завантажити образ розділу;
- створити шаблон, на основі обраного диска;
- змінити обсяг розділу (доступне лише для кореневого адміністратора).

Іншим способом є реєстрації шаблонів у хмарній інфраструктурі є використання сторінки *Шаблони (Templates)*. Використовуючи гіперпосилання *Upload from Local* у користувача є можливість завантажити шаблон з диска власного комп'ютера. Також існує можливість завантажити шаблон з певної URL-адреси. У останньому випадку користувач має змогу визначити такі параметри шаблона (рис. 9.33):

- адресу для завантаження файла шаблона;

- назву шаблона;
- його опис;
- зона, у якій буде доступний шаблон;
- тип гіпервізора;
- формат файла шаблона;
- тип операційної системи;
- доступність шаблона розгортання;
- захист паролем;
- можливість динамічної зміни обсягу розділу;
- загальнодоступність шаблона;
- необхідність застосування для ВМ, які будуть створені з шаблона, технології повної апаратної віртуалірації (HVM – hardware-assisted virtualization).

На сьогоднішній день платформа Apache CloudStack підтримує роботу з різними шаблонами, зокрема QCOW2 – формат емулятора QEMU, внутрішній для системи, VHD – формат віртуальних дисків системи віртуалізації Hyper-V від компанії Microsoft , VDMK – формат дисків віртуальних машин, створених за допомогою VmWare.

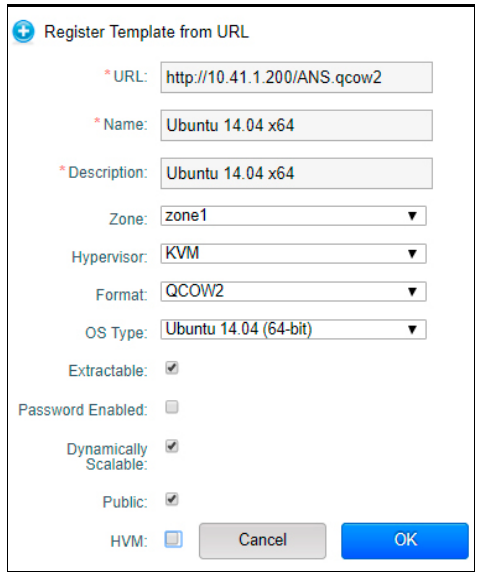

Рис. 9.33 Реєстрація шаблона за URL-адресою

Слід враховувати, що знімки та шаблони дисків є файлами значного обсягу. Як наслідок операції з ними можуть вимагати чималого часу та пропус-

кної здатності мережі. У зв'язку з цим розробники платформи Apache CloudStack рекомендують для шаблонів обсягом понад 100 Гб використовувати мережі з швидкістю 1-10 Гбіт/с.

У схожий спосіб можна зареєструвати ISO-образ CD- або DVD-диска. З його використанням можна створити ВМ та встановити на неї ОС. Для успішного завантаження файлів у обох випадках слід додати URL-адреси серверів до списку довірених. Це можна зробити, змінивши у глобальних налаштуваннях платформи значення параметра *secstorage.allowed.internal.sites*, в якому вказати IP-адресу мережі або окремого сервера, з якого завантажуватимуться файли.

У користувачів хмари існує можливість планувати створення знімків дисків ВМ. Для цього на сторінці ВМ потрібно перейти до відображення розділів (гіперпосилання *View Volumes*) та на панелі інструментів обрати гіперпосилання *Налаштувати повторюване створення шаблонів (Set up recurring shapshots)*.

У вікні, що завантажиться вказуємо (рис. 9.34):

- періодичність створення знімків – щогодинна, щоденна, щотижнева, щомісячна;
- дату та час створення знімка;
- часу зону;
- кількість знімків для зберігання.

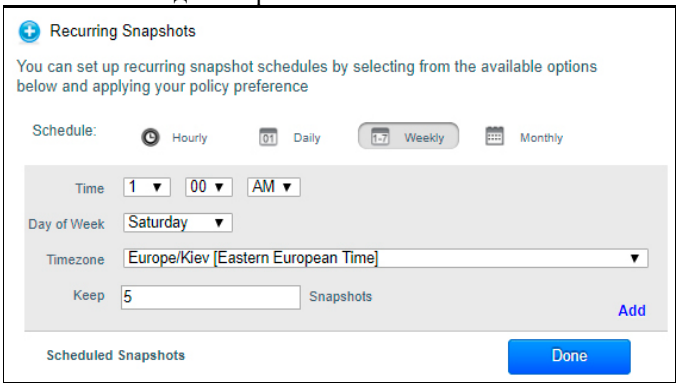

Рис. 9.34 Планування автоматичного створення знімків

Варто зауважити, що пропонований засіб дозволяє запланувати кілька схем створення знімків ВМ.

9.2.9 Використання API-функцій платформи Apache CloudStack

Платформа Apache CloudStack містить чимало API-функцій. Вони можуть бути використані програмістами та адміністраторами для розробки та тестування її нових модулів, а також для інтеграції платформи з іншими системами. Використання API-функцій дає змогу отримати доступ до даних про об'єкти хмарної інфраструктури та їх використання у процесі функціонування платформи.

Для формування запиту, який містить API-функції, слід вказати:

- URL-адресу до сервера управління, наприклад http://10.41.1.253:8080/client/;
- службову конструкцію «api?», яка містить шлях до певної API-функції, та вказує на початок параметрів, які передаються за допомогою способу GET;
- command – назву команди;
- apiKey –API-ключ, який генерується при створенні або зміні облікового запису користувача;
- додаткові параметри уточнення запиту – розділяється подібно до GET-запитів за допомогою символу «&»;
- формат відповіді – JSON або XML;
- signature – підпис запиту.

Незалежно від протоколу (HTTP або HTTPS), за допомогою якого здійснюється доступ до API-функцій Apache CloudStack, запит повинен бути підписаний. Це дає змогу платформі підтвердити, що запит надіслано від довіреного облікового запиту, який має повноваження виконувати відповідну команду. Для підписування запиту слід мати API-ключ та секретний ключ облікового запису, які можна одержати в адміністратора платформи.

Наприклад, нехай потрібно отримати дані про ВМ домену з ідентифікатором «6ac60985-6e33-4240». Відповідний API-запит буде мати вигляд:

http://10.41.1.253:8080/client/api?command=listVirtualMachines&
domainId=6ac60985-6e33-4240&apiKey=yyy

Для генерування підпису запиту слід виконати такі дії:

1. Одержати дані запиту, які передаватимуться, наприклад «*command=listVirtualMachines&domainId=5&apiKey=yyy*»;
2. Відсортувати параметри «змінна-значення» у алфавітному порядку;
3. Замінити символи «+», якими у запиті було замінено пробіл на «%20»;
4. Перетворити одержаний рядок у нижній регістр, наприклад, «*apikey=yyy&command=listvirtualmachines&domainId=6ac60985-6e33-4240*»;
5. Зашифрувати отримані дані алгоритмом SHA-1 за допомогою секретного ключа облікового запису;
6. Закодувати одержаний рядок у формат BASE64.

Одержаний у пункті 6 рядок і буде значенням параметра підпис (singnature). Виконавши такий запит, розробник отримує відповідь у форматі JSON або XML, яка буде мітити такі дані (рис. 9.35):

Рис. 9.35 Формат виводу відповіді на API-запит

- ідентифікатор та ім'я віртуальної машини;
- ідентифікатор та ім'я облікового запису її власника;
- ідентифікатор та назву домену, до якого належить ВМ;
- дату та час її створення;
- ідентифікатор та назву зони, до якої належить ВМ;
- стан ВМ (працює, зупинена, видалена);
- ідентифікатор та назву шаблона, з якого було створено ВМ;
- ідентифікатор та назву шаблону продуктивності;
- характеристики апаратного забезпечення ВМ (кількість ядер та частота процесора, обсяг оперативної пам'яті);
- ідентифікатор та назва мережі, до якої належить ВМ;
- параметри мережі (IP- та MAC-адреси, маска підмережі, адреса основного шлюзу та сервера DNS, номер VLAN);
- тип мережі (гостьова, приватна);
- тип гіпервізора;
- тип операційної системи, яка встановлена на ВМ.

Викликаючи API-функцію, можна встановити час її дії. Це дає змогу запобігти повторним запитам через незахищені протоколи, такі як HTTP. У

цьому випадку сервер управління буде перевіряти чи не закінчився вказаний час та відхилятися усі наступні API-запити. Щоб увімкнути зазначену функцію, слід додати до запиту параметр expires, присвоївши йому значення у форматі YYYY-MM-DDThh:mm:ssZ згідно стандарту ISO 8601. Після завершення визначеного проміжку часу підпис запиту стане не дійсним. Також існує можливість обмежити кількість API-запитів кожного облікового запису. Такий механізм використовують, щоб уникнути атак на сервер керування та для запобігання зниженню його продуктивності. Якщо кількість API-запитів перевищує порогове значення, то у відповідь на будь-які додаткові запити буде повернуто повідомлення про помилку. У загальній конфігурації платформи доступні такі параметри обмеження виконання API-запитів:

- api.throttling.enabled – задіює затримку при виконанні API-запитів;
- api.throttling.interval – інтервал в секундах, протягом якого обчислюється кількість API-запитів; після завершення цього часу кількість обнулюється;
- api.throttling.max – максимальна кількість API-запитів за визначений період;
- api.throttling.cachesize – обсяг кеш-пам'яті для зберігання лічильників API-запитів (зазвичай має перевищувати кількість облікових записів користувачі).

У кожній хмарній інфраструктурі визначена кількість результатів, які може повернути команда API. Таке обмеження дозволяє запобігти перевантаженню серверів та атакам DDOS. За його встановлення відповідає глобальний параметр default.page.size. Його значення залежить від кількості ВМ та користувачів у хмарі. Існує можливість зменшення обсягу сторінки відповіді для окремого API-запиту. Зменшення обсягу сторінки відповіді можливе за допомогою параметрів запиту listCapabilities та listDiskOfferings.

Якщо під час обробки запиту API виникає помилка, користувачеві буде згенеровано відповідь у вказаному форматі. Кожна відповідь з помилкою містить її код та текст, що описує можливу причину її виникнення.

У платформі Apache CloudStack реалізовано окремий вид API-запитів – асинхронні команди, виконання яких вимагає тривалого часу. Наприклад такими є команди створення знімка (архіву) диска або його перенесення на інше сховище. На відміну від синхронних команд вони негайно повертають ідентифікатор завдання, яке відповідає обробці API-запиту. Наприклад, якщо виконується команда створення ВМ *createVM*, то буде повернено ідентифікатор ресурсу, а також ідентифікатор завдання. Розробник може перевіряти стан виконавши команди, ввівши API-запит, *queryAsyncJobResult* та вказавши ідентифікатор завдання.

Наприклад, за допомогою такого API-запиту виконати команду увімкнення ВМ з ідентифікатором e7ee73cc:

http://10.41.1.253:8080/client/api?command=startVirtualMachine&id=e7ee73cc&apiKey=yyy&signature=sign2

У відповідь на зазначений API-запит сервер керування поверне сторінку з ідентифікатором завдання, який у свою чергу можна використати для відстеження стану виконання команди. У розглянутому прикладі можна скористатися таким запитом:

http://10.41.1.253:8080/client/api?command=queryAsyncJobResult&jobid=1b266114&signature= sign2

Якщо віртуальний комп'ютер було завантажено успішно, то у відповідь на запит, сервер поверне сторінку, яка міститиме детальні дані про завдання та стан ВМ (поля *jobstatus* та *jobresult*).

9.3.1 Огляд можливостей системи Proxmox VE

Proxmox Virtual Environment (VE) система віртуалізації, яку можна вважати платформою для розгортання корпоративних хмар. На відміну від Apache Cloudstack платформа поставляється у вигляді вільнопоширюваного Linux-дистрибутива на базі Debian GNU/Linux. У хмарній інфраструктурі Proxmox VE можна виконувати віртуальні машини з використанням гіпервізора KVM та контейнери на основі технології LXC (LinuX Container), що є системою віртуалізації на рівні операційної системи для запуску декількох ізольованих примірників ОС Linux на одному комп'ютері. LXC створює віртуальне оточення з власним простором процесів і мережевим стеком. Контейнери виконуються у ядрі основної ОС, що дає можливість виконувати більшу їх кількість у хмарній інфраструктурі. Проте контейнери зазвичай не дозволяють виконувати ОС відмінні від ОС сервера.

Серед інших можливостей платформи виділимо:

- управління об’єктами через веб-інтерфейс, зокрема через захищену VNC-консоль;
- підтримку віртуальних мереж у хмарній інфраструктурі;
- можливість об’єднання хостів у кластери;
- реплікація даних сховищ на різні вузли, а також наявність спеціалізованої файлової системи для реплікації конфігурації у межах кластера;
- наявність вбудованих інструментів для організації резервного копіювання, як окремих ВМ так і усієї платформи;
- управління доступом до всіх доступних об'єктів (VM, сховищ, вузли тощо) на основі ролей;
- підтримка різних механізмів автентифікації на основі Microsoft Active Directory, каталогу LDAP, Linux PAM, Proxmox VE authentication).
- чималий набір команд та API-функцій для розширеного управління платформою.

9.3.2 Встановлення платформи Proxmox VE

Перед встановленням платформи варто з'ясувати відповідність апаратного забезпечення її вимогам. Аналіз офіційної документації свідчить про незначні вимоги що стосуються самої системи (процесор з 64-ти бітною архітектурою, 1 Гб оперативної пам'яті, мережний адаптер). Проте слід резервувати обчислювальну потужність серверів залежно від кількості віртуальних машин та контейнерів, що будуть завантажуватися на виконання.

Для виконання процедури встановлення слід завантажити з офіційного сайту інсталяційний образ та записати його на носій. Це можна виконати в різних операційних системах з використанням командного інтерфейсу (ОС Linux) або спеціалізованих утиліт (наприклад Rufus ОС Windows). У ОС Linux слід скористатися командою:

dd bs=1M conv=fdatasync if=<файл-образ> of=/dev/<USB_пристрій>

Визначити правильну назву пристрою можна за допомогою команд *dmesg* та *lsblk*.

Після завантаження програми встановлення з носія слід обрати пункт «Інсталяція Proxmox VE» та прийняти умови ліцензійної угоди. Наступним кроком є вказання носія для встановлення платформи. Типовою файловою системою для Proxmox VE є ext4. Proxmox VE можна встановити із файловою системою ZFS, яка пропонує кілька рівнів програмних RAID-масивів. Зазначена файлова система доцільно використовувати для серверів, які не мають апаратного контролера RAID. Цільові диски потрібно вибрати в діалоговому вікні «Параметри» (рис. 9.36).

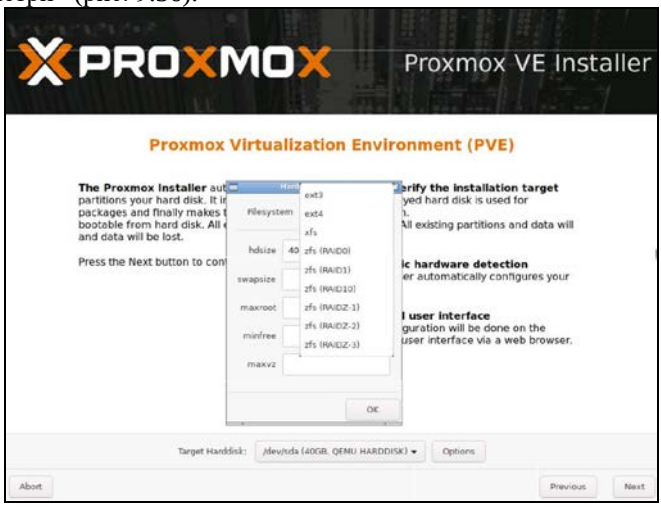

Рис. 9.36 Розподіл диска для встановлення платформи Proxmox VE

На наступному кроці користувачеві пропонується ввести основні параметри конфігурації платформи, зокрема місцезнаходження, часовий пояс та мову введення. Надалі потрібно вказати пароль суперкористувача (root) та відповідну адресу електронної пошти. Пароль повинен складатися не менше ніж з 5 символів. Загалом слід використовувати пароль, що відповідає загальноприйнятим безпековим вимогам.

Останнім кроком встановлення параметрів майбутньої системи є налаштування мережі. У процесі інсталяції вказують адреси протоколів IPv4 або IPv6. Проте одночасно використовувати обидва стеки протоколів на етапі встановлення неможливо. Відповідні налаштування можна зробити після встановлення.

Після виведення остаточних параметрів системи відбудеться безпосередньо встановлення, зокрема форматування дисків і копіювання пакетів. По завершенню процесу встановлення слід вилучити інсталяційний носій та перезавантажити систему.

9.3.4 Інтерфейс платформи Proxmox VE

Управління об’єктами хмарної інфраструктури Proxmox VE здійснюється через веб-браузер. Для доступу командного інтерфейсу хоста (гостьової консолі) використовується вбудована консоль

Веб-інтерфейс доступний за покликанням https://<IP-адреса_хоста>:8006 (логін за замовчуванням: root, а пароль вказується під час встановлення). Оскільки платформа використовує власну файлову систему кластера Proxmox (pmxcfs), користувач може приєднатися до будь-якого хоста, щоб керувати всім кластером (рис. 9.37).

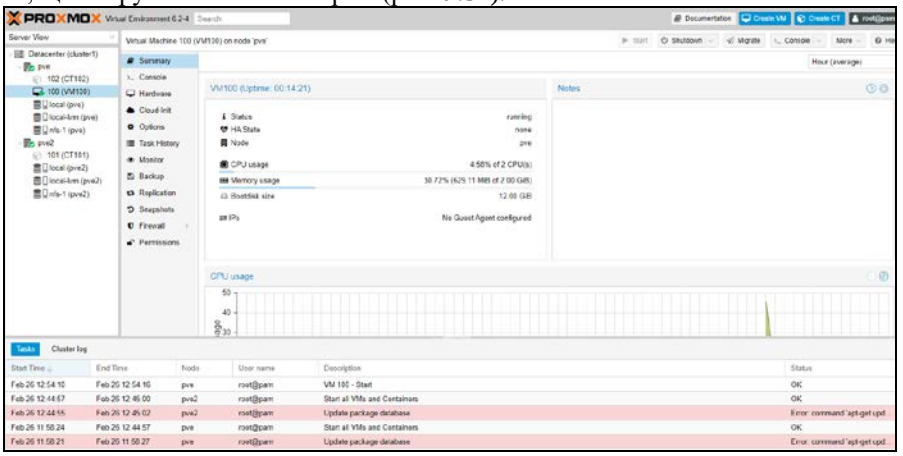

Рис. 9.37 Веб-інтерфейс платформи Proxmox VE

Зауважимо, що потрібні операції можна виконувати, увійшовши на будь-який вузол (на рис. 9.37 вузли (хости) pve та pve2 відображаються у вікні ліворуч). На відміну від платформи Apache Cloudstack Proxmox VE не використовує окремий сервер управління. Платформа має спрощений веб-інтерфейс, що автоматично завантажується у випадку звертання з мобільного пристрою (рис. 9.38).

Рис. 9.38 Веб-інтерфейс платформи Proxmox VE для мобільних клієнтів

Інтерфейс користувача Proxmox VE складається з таких складників (рис. 9.38).

- Верхній блок, що містить логотип платформи. У ньому відображається інформація про стан системи та присутні кнопки-покликання для виконання операцій.
- Дерево ресурсів, знаходиться ліворуч. У ньому обирають певні об'єкти (хости, ВМ, контейнери, сховища).
- У центральні панелі відображається основний вміст системи. Обрані у дереві об'єкти відображаються у цій області разом із параметрами конфігурації та статусом.
- Панель журналу (розташована внизу). Вона відображає записи журналу для останніх завдань.

У верхньому блоці інтерфейсу поряд з логотипом можна віднайти поточну версію платформи. Праворуч знаходиться рядок пошуку, який можна використати для швидкої навігації між об'єктами. У випадку складної інфраструктури цей спосіб може бути ефективнішим, ніж вибір об'єкта в дереві ресурсів.

Праворуч від рядка пошуку міститься логін поточного користувача. Традиційна кнопка із символом у вигляді шестерні призначена для роботи з вікном «Мої налаштування», у якому можна налаштувати деякі параметри інтерфейсу користувача. Крайня права частина заголовка містить кнопки для

отримання довідки, створення віртуальної машини та контейнера та виходу із системи.

Дерево навігації надає інструменти для управління основними об'єктами інфраструктури:

- Датацентр – містить параметри для всього кластера, які стосуються всіх вузлів).
- Вузол – містить хости кластера, на яких виконуються гостьові віртуальні машини, контейнери, а також створені відповідні шаблони.
- Сховища для зберігання даних. За замовчуванням створюються два сховища, що за своїм призначенням подібні до платформи Apache Cloudstack.
- Пули – об'єкти, що сформовані за певною ознакою ресурсів.

Вгорі дерева навігації є список вибору, за допомогою якого можна змінювати вигляд інтерфейсу. Існують такі подання сервера:

- Сервер, що відображає всі види об'єктів, згруповані за вузлами.
- Папка – виводить всі об'єкти, що згруповані за типом (рис. 9.39).
- Сховище – містить об'єкти зберігання, згруповані за вузлами.
- Пул – відображає віртуальні машини та контейнери, що згруповані за певною ознакою.

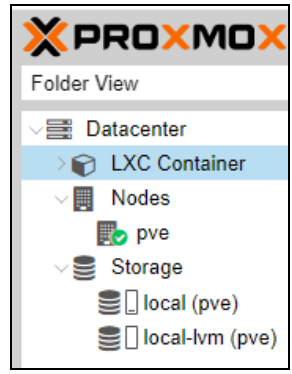

Рис. 9.38 Подання у вигляді папки

Внизу веб-інтерфейсу платформи Proxmox VE розміщена панель журналу. Вона призначена для відображення подій, що зараз відбуваються у кластері. До прикладу, вона містить відомості про створення нової або увімкнення існуючої віртуальної машини.

Традиційно в ОС Linux результати усіх подій системи зберігаються в окремих файлах (log-файлах). Існує можливість перегляду цього журналу у веб-інтерфейсі за допомогою подвійного клацання на відповідному записі. Там також можна перервати виконуване завдання.

Зауважимо, що панель відображає завдання з усіх вузлів кластера. Тобто користувач в режимі реального часу може бачити, коли хтось інший працює на іншому вузлі кластера.

Система видаляє старіші та завершені завдання з панелі журналу, щоб їх список був коротким. Проте користувач може знайти їх в історії завдань панелі вузлів.

При виборі елемента із дерева ресурсів у панелі вмісту відображається інформація та конфігурація відповідного об’єкта. На рівні датацентру обробки даних системний адміністратор може отримати доступ до налаштувань та інформації всього кластера. У цьому випадку основними для роботи системного адміністратора є такі розділи:

- Пошук – дозволяє знаходити вузли, віртуальні машини, контейнери, сховища та пули у всьому кластері.
- Підсумок – дає короткий огляд справності та використання ресурсів кластера.
- Кластер – надає функціональні можливості та інформацію, необхідну для створення або приєднання до кластера (рис. 9.40).

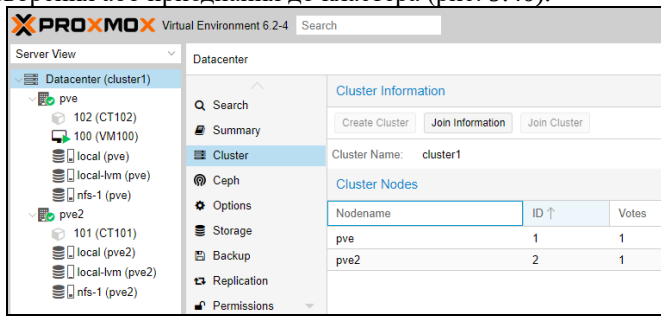

Рис. 9.40 Інформація про кластер Proxmox VE

- Параметри – дозволяє виконати перегляд або редагування параметрів за замовчування, що стосуються усього кластера.
- Зберігання – надає інтерфейс для управління сховищами кластера.
- Резервне копіювання дає можливість планувати завдання резервного копіювання в межах усього кластера. Тобто під час створення задач планування не має значення, на якому вузлі чи сховищі знаходяться об’єкти резервування.
- Реплікація – дає можливість налаштувати синхронізацію (дублювання) ВМ чи контейнерів на різних хостах кластера.
- Дозволи – містить інструменти для управління дозволами користувачів, груп, API-токенів, а також до налаштувань автентифікації.
- НА – забезпечує підвищену доступність об’єктів Proxmox VE.

- ACME – пропонує засоби для налаштування чинних сертифікатів за допомогою сервісу Let's Encrypt.
- Брандмауер – дозволяє створити шаблони фільтрації трафіку для кластера Proxmox.

Якщо у дереві об'єктів обрати певний вузол (node), то у панелі вмісту буде відображено інформацію, яка за структурою є аналогічною до датацентру. Розглянемо деякі об'єкти виводу, які є специфічними саме для хоста. До найважливіших розділів належить статистика, яка дає можливість оцінити завантаження фізичного сервера (рис. 9.41).

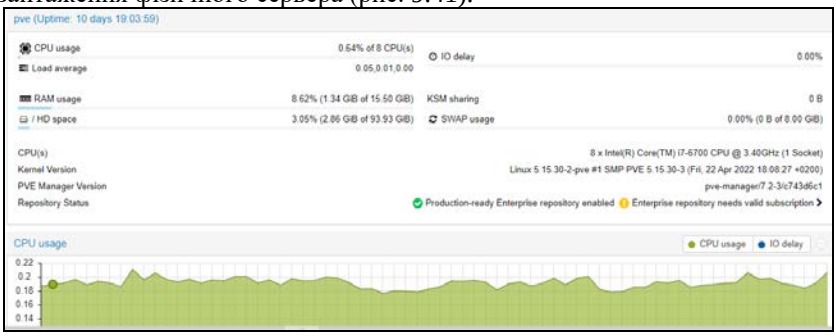

Рис. 9.41 Статистика використання ресурсів хоста Proxmox VE

За допомогою посилання Оболонка (Shell) адміністратор отримує доступ до командного інтерфейсу ОС фізичного сервера. У розділі Система доступні послуги для конфігурування мережі, SSL-сертифікатів, адрес DNS-серверів, зміни системного часу та перегляду подій ОС хоста.

9.3.5 Сховища платформи Proxmox VE

В основному платформа пропонує два підходи до збереження даних – на основі файлів та блоків даних.

Зберігання на рівні файлів. Технології зберігання на основі файлового рівня дозволяють отримати доступ до повнофункціональної файлової системи (POSIX). Щодо практики використання, то файлові сховища більш гнучкі, ніж блочні сховища, і дозволяють зберігати вміст будь-якого типу. Нині ZFS обґрунтовано вважають досконалою файловою системою, що повністю підтримує знімки та клони. Як і платформа Apache CloudStack Proxmox VE

Зберігання на рівні блоків даних. Технологія дозволяє зберігати великі необроблені обсяги даних. Зазвичай неможливо зберігати інші файли (ISO, резервні копії, образи дисків) на таких типах сховищ. Більшість сучасних реалізацій зберігання на блочному рівні підтримують знімки (shapshot) та клони дисків ВМ. До прикладу RADOS і GlusterFS є це розподіленими системами,

що тиражують дані на різні сховища. Основні доступні типи сховищ, що використовуються платформою Proxmox VE наведено у таблиці 9.4.

Таблиця 9.4. Основні типи сховищ, які підтримує платформа Proxmox VE (на основі даних офіційного сайту)

Тип	**Підхід**	**Спільне (мережне) сховище**	**Знімки**
NFS	файлове	так	ні
CIFS	файлове	так	ні
Proxmox Backup	обидва	так	–
GlusterFS	файлове	так	ні
CephFS	файлове	так	так
LVM	блокове	ні	ні
LVM-thin	блокове	ні	так
iSCSI/kernel	блокове	так	ні
iSCSI/libiscsi	блокове	так	ні
Ceph/RBD	блокове	так	так
ZFS over iSCSI	блокове	так	так

Кілька з наведених сховищ Proxmox VE працюють із форматом віртуальних дисків Qemu qcow2, що підримує «тонке забезпечення». Технологія передбачає, що лише ті блоки, які фактично використовує гостьова система, будуть записані в сховище. Ці файли не резервують увесь визначений при створенні ВМ обсяг даних, а використовують реально використаний обсяг. Такий підхід називають тонким забезпеченням (thin provisioning). Він дозволяє створювати образи дисків, які перевищують обсяг наявних на даний момент блоків зберігання. Усі типи сховищ, які підтримують функцію «миттєвих знімків», також підтримують тонке забезпечення.

Уся конфігурація сховища Proxmox VE зберігається в текстовому файлі /etc/pve/storage.cfg. Параметри, вказані у ньому, розповсюджується на всі вузли кластера. Наприклад, конфігурація локального сховища за замовчуванням має такий вигляд:

dir: local
path /var/lib/vz
content iso,vztmpl,backup

Запис визначає шлях для зберігання об’єктів, та їх типи (образи ISO, шаблони та резервні копії). Основними значеннями властивостей сховищ є такі:

- Nodes (вузли) – є списком імен вузлів кластера, для яких можна використовувати сховище. Цю властивість можна використовувати для обмеження доступу до сховища певним набором вузлів.
- Content (вміст). Сховище може підтримувати кілька типів вмісту, наприклад образи віртуальних дисків, ISO-образи cdrom, шаблони контейнерів або кореневі каталоги контейнерів.
- Images (образи). Підтримується формат ВМ KVM-Qemu.
- Rootdir – кореневий каталог для зберігання даних контейнерів.
- Shared (спільний доступ) – дозволяє Позначити сховище як спільне.
- Disable (вимкнути) – можна використовувати, щоб повністю вимкнути сховище.
- Format – формат диска за замовчуванням (raw|qcow2|vmdk)
- Snippets (фрагменти) – є файлами скриптів, що виконуються на ВМ за певних умов.

9.3.6 Мережі в інфраструктурі Proxmox VE

Платформа Proxmox VE використовує мережний стек ОС Linux. Конфігурацію мережі можна виконати через веб-інтерфейс або відредагувавши файл */etc/network/interfaces*. Проте система не записує зміни безпосередньо до файла */etc/network/interfaces*. Замість цього використовується тимчасовий файл */etc/network/interfaces.new*. Це дає можливість переконатися у коректності змін перед їх застосуванням. Використання у версії Proxmox VE 7.0 пакета ifupdown2 зміни конфігурації мережі застосовуються без перезавантаження фізичних серверів.

Для приєднання ВМ до фізичної мережі платформа використовує інтерфейс vmbr. Подібно до Apache Cloudstack він є мостом ОС Linux, який можна розглядати як віртуальний комутатор, до якого приєднано ВМ та фізичні інтерфейси. Нині платформа використовує такі правила для іменування мережних пристроїв:

- ethernet-адаптери отримують імена, що починаються з символів en, які використовуються systemd – підсистемою управління службами ОС Linux. Зазначене правило іменування використовується у сучасних версіях, для версії Proxmox VE 5.0 застосовуються старі імена, що починаються з eth;
- мости отримують імена vmbr[N], де N – номер моста може набувати значень від нуля до 4094;
- зв’язки іменуються подібно до мостів: bond[N];
- віртуальні локальні мережі (VLAN) отримують частину імені від відповідного мережного пристрою, до якої через крапку додається номер (ідентифікатор) VLAN, наприклад eno1.50, bond1.30.

Залежно від поточної організації мережі та обчислювальних ресурсів існує можливість спроєктувати мережу відповідно до мостової та моделі з маршрутизатором.

Якщо сервер Proxmox VE у приватній локальній мережі використовує зовнішній шлюз для доступу до інтернету, то найбільш доцільною є мостова модель. У цьому випадку кожна ВМ матиме віртуальний інтерфейс, підключений до мосту Proxmox VE (рис. 9.4.2). Кожен хост (node) використовуватиме окремий міст. Зазначена схема передбачає обмін трафіком між хостами (наприклад, node1 та node2). Для цього використовується комутатор SW.

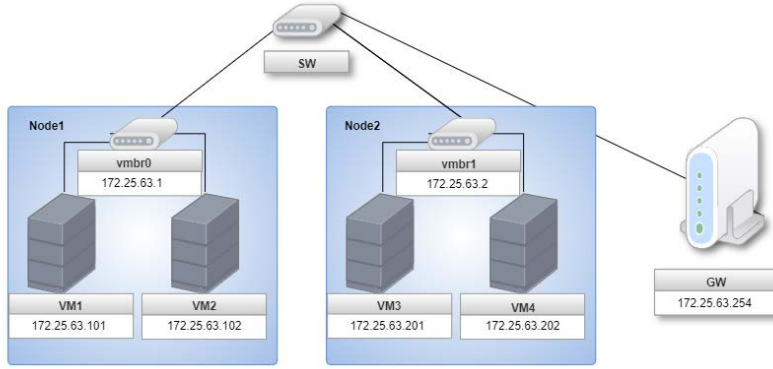

Рис. 9.42 Мостова модель мережі в інфраструктурі Proxmox VE

Якщо сервер Proxmox VE розміщено у хостинг-провайдера, що надає загальнодоступні IP-адреси для гостьових ВМ, то доцільним є налаштування мережі відповідно до моделі, яка передбачає використання маршрутизатора (рис. 9.43). Ним може бути сервер Proxmox VE. У цьому випадку слід налаштувати щонайменше дві IP-адреси – одна у зовнішній мережі (інтернеті), а інша – у мережі Proxmox VE.

Як видно з рисунка 9.43 маршрутизатором є пристрій «gw». У випадку якщо єдиною публічною адресою є IP-адреса сервера Proxmox VE, то слід налаштувати на ньому маршрутизацію з маскуванням адрес (SNAT – Source Network Address Translation). Для доступу до ВМ із мережі інтернет потрібно налаштувати переадресацію портів (DNAT – Source Network Address Translation). Для налаштування маршрутизації з NAT-перетворенням слід до файла конфігурації мережі додати такі рядки:

post-up echo 1 > /proc/sys/net/ipv4/ip_forward
post-up iptables -t nat -A POSTROUTING -s ’172.25.63.0/24’ -o eno1 -j MASQUERADE
post-down iptables -t nat -D POSTROUTING -s 172.25.63.0/24’ -o eno1 -j MASQUERADE

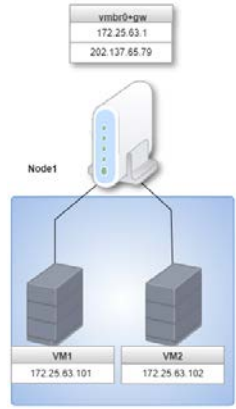

Рис. 9.43 Модель з маршуризатором мережі в інфраструктурі Proxmox VE

Перша команда вмикає у ядрі ОС режим маршрутизації. Друга задіюється після ініціалізації мережі та дозволяє NAT-перетворення IP-адрес відправників (172.25.63.0/24) на вихідному інтерфейсі (*eno1*). Остання команда призначення для видалення правила NAT-перетворень після вимкнення інтерфейсу.

Для забезпечення відмовостійкості або підвищення пропускної здатності мереж платформа Proxmox VE використовує зв'язування (агрегацію з'єднань – bonding). Загалом це технологія зв'язування кількох мережевих адаптерів у один мережевий пристрій.

Основними режимами об'єднання інтерфейсів є такі:

- Round-robin (balance-rr), що передбачає почергове передавання мережевих пакетів, починаючи з першого доступного інтерфейса (NIC) та закінчуючи останнім.
- Активне резервне копіювання (active-backup), при якому використовується лише один підлеглий мережевий адаптер. Інший інтерфейс задіюється у випадку, коли перший адаптер виходить з ладу.
- XOR (balance-xor), що забезпечує передавання даних на основі відповідності «вихідна MAC-адреса XOR MAC-адреса призначення»
- Broadcast (широкомовлення), за якого здійснюється передавання даних на всі доступні мережні інтерфейси. Цей режим забезпечує відмовостійкість.
- Агрегація динамічних посилань за протоколом IEEE 802.3ad (LACP – Link Aggregation Control Protocol). Протокол створює групи агрегації, які спільно використовують однакові швидкісні параметри та налаштування дуплексу. Використання режиму вимагає використання у

хмарній інфраструктурі Proxmox VE комутаторів, що підтримують стандарт IEEE 802.3ad.

Наступний фрагмент файла */etc/network/interfaces* призначений для створення агрегування інтерфейсів засобами протоколу LACP.

```
auto bond0
iface bond0 inet static
bond-slaves eno1 eno2
address 172.25.63.2/24
bond-miimon 100
bond-mode 802.3ad
bond-xmit-hash-policy layer2+3
```

Нині однією з найпопулярніших технологій сегментування мереж є віртуальні локальні мережі (VLAN). Платформа Proxmox VE підтримує зазначену технологію у базовій конфігурації. У хмарній інфраструктурі можливі кілька режимів використання віртуальних локальних мереж. Коротко розглянемо їх.

«Традиційна» VLAN, як дочірній інтерфейс мосту Linux. Режим передбачає створення окремого пристрою для кожної VLAN, що пов'язаним відповідним мостом. Наприклад, при додаванні до мережної конфігурації хоста VLAN з ідентифікатором 155 у його ОС буде створено два інтерфейс vmbr0.155. Наступний фрагмент файла */etc/network/interfaces* описує зазначену конфігурацію:

```
auto vmbr0.155
iface vmbr0.155 inet static
    address 172.25.155.253/24
    gateway 172.25.155.254
    bridge-ports enp2s0
    bridge-stp off
    bridge-fd 0
auto vmbr0
    iface vmbr0 inet manual
    bridge-ports enp2s0
    bridge-stp off
    bridge-fd 0
```

Зауважимо, що при цьому основний мостовий інтерфейс залишається, проте IP-адреса призначається інтерфейсу у віртуальній локальній мережі.

Прозорий режим, який передбачає обізнаність (awareness) мостового інтерфейсу про передавання через нього трафіку, що має тег (ідентифікатор) VLAN. Конфігурування з веб-інтерфейсу платформи має вигляд як на рис. 9.44.

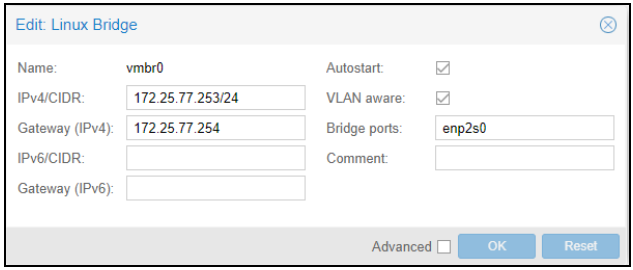

Рис. 9.44 Конфігурування «прозорого» моста для роботи з VLAN

У цьому випадку слід налаштувати відповідний VLAN на мережному комутаторі чи маршрутизаторі та вказати його у кожній ВМ, яка маєш працювати у цій мережі (рис. 9.45)

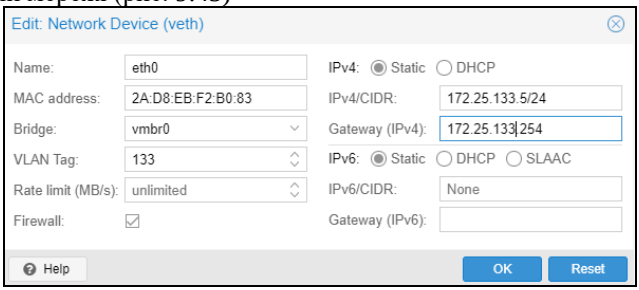

Рис. 9.45 Вказання тега VLAN у параметрах мережі ВМ

Режим OVS VLAN – віртуальна мережа вимагає використання програмного комутатора Open vSwitch.

Режим «Гостьова VLAN» − віртуальна мережа конфігурується всередині ОС, яка завантажена на ВМ. Як наслідок її конфігурування не можливе з інтерфейсу Proxmox VE.

9.3.7 Робота з віртуальними машинами у хмарній інфраструктурі Proxmox VE

Платформа використовує гіпервізор з відкритим кодом Qemu (скорочена форма від Quick Emulator). Qemu працює з підтримкою розширень процесора віртуалізації через модуль Linux KVM (Kernel Virtual Machine). У офіційній документації Proxmox VE Qemu та KVM вживаються як синоніми. З точки зору ОС хоста, екземпляр ВМ є процесом Qemu, який має доступ до локальних ресурсів сервера. Qemu дозволяє емулювати материнську плату, мережні адаптери, контролери SCSI, IDE та SATA, послідовні порти тощо. Це дає можливість Qemu виконувати немодифіковані операційні системи.

Проте такий підхід має наслідком зниження продуктивності. Для того, щоб зменшити цей ефект використовується модифіковані (паравіртуалізовані) драйвери пристроїв Virtio. У цьому випадку гостьова ОС розпізнає, що вона працює всередині гіпервізора Qemu.

Процес створення ВМ у хмарній інфраструктурі Proxmox VE відбувається аналогічно до платформи Apache Cloudstack та передбачає проходження користувачем таких кроків:

- визначення загальних налаштувань ВМ, до яких належать хоста, на якому буде виконуватися ВМ, її числовий ідентифікатор та ім'я;
- налаштування ОС, зокрема, тип та версія ОС, а також ISO-образ або фізичний носій, з якого буде виконуватися встановлення;
- системні налаштування, що визначають характеристики пристроїв ВМ (графічного адаптера, дискових контролерів, тип системи BIOS);
- конфігурація жорсткого диска – інтерфейс контролера (IDE, SATA, SCSI, virtio), тип кеш-пам'яті, обсяг та формат диска, сховище для його зберігання, швидкісні характеристики тощо (рис. 9.46);

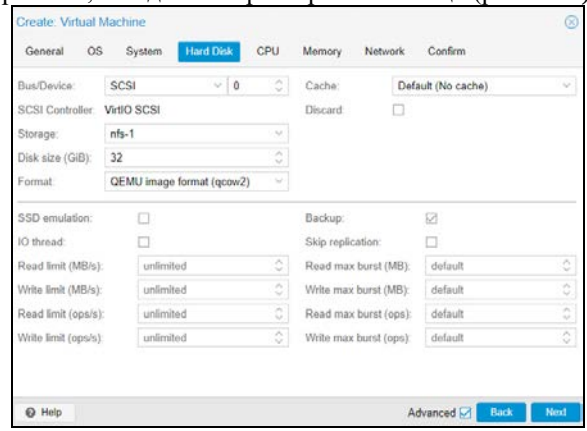

Рис. 9.46 Характеристики жорсткого диска

- характеристики центрального процесора (модель, кількість процесорів, ядер) та обсяг оперативної пам'яті;
- налаштування мережі, зокрема міст хоста, який забезпечуватиме доступ ВМ до мережі, тег VLAN (опціонально), модель та MAC-адреса адаптера, наявність фільтра трафіку (брандмауера) та параметри обмеження пропускної здатності мережі (рис. 9.47).

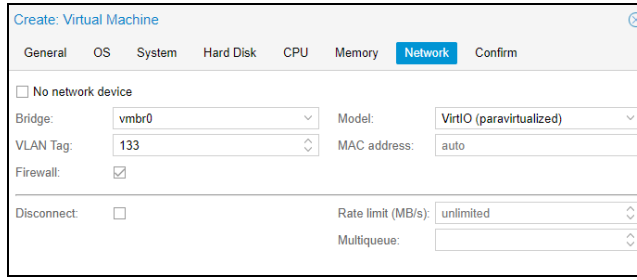

Рис. 9.47 Визначення параметрів мережного пристрою ВМ

Незважаючи на значну кількість налаштувань, Proxmox VE пропонує доцільні параметри за замовчуванням для віртуальних машин (VM). Після увімкнення створеної ВМ відбудеться завантаження з віртуального DVD-приводу, у який приєднано ISO-образ (рис. 9.48).

Рис. 9.48 Встановлення ОС Linux на віртуальну машину

Виділимо кілька параметрів конфігурації платформи Proxmox VE, які можуть бути важливими у процесі створення ВМ:

1. Якщо в інфраструктурі доступні кілька хостів (nodes), то слід потурбуватися про спільне сховище, для розміщення ISO-образів. Ним може бути загальнодоступна папка, створена за допомогою сервера NFS.
2. Формат віртуальних дисків залежить від сховища. Наприклад, при використанні локального сховища, платформа пропонує лише формат RAW, для NFS-сховища доступними будуть формати гіпервізорів QEMU та VMware.
3. Конфігурування параметрів протоколів TCP/IP відбувається в ОС.

Процес створення контейнерів є подібним до віртуальних машин, проте він відповідає їх специфіці, як наперед налаштованих ОС. Це дає можливість не виконувати встановлення ОС (натомість на етапі створення контейнера вказується пароль адміністратора). Необхідним є шаблон контейнера, який можна завантажити із загальнодоступних репозитаріїв. Конфігурування параметрів TCP/IP також виконують на етапі створення контейнера (рис. 9.49).

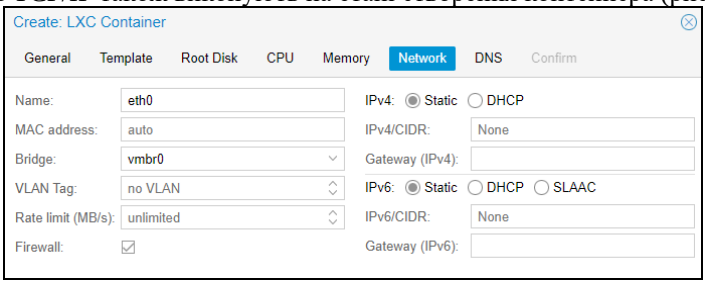

Рис. 9.49 Визначення параметрів мережного пристрою контейнера

Якщо існує потреба у створенні великої кількості однотипних ВМ або контейнерів, то слід копіювати (клонувати) обраний екземпляр. Також можна підготувати один екземпляр та конвертувати його у шаблон. Це виконують за допомогою контексного меню ВМ у дереві об'єктів. При цьому можливе створення зв'язаних (linked) або повних копій. У першому випадку результатом є незалежна ВМ. Нова віртуальна машина не використовує жодних ресурсів зберігання оригіналу. Існує можливість вибору іншого сховища та зміни формату образу диска. Сучасні драйвери дисків підтримують створення швидких зв'язаних клонів. Такий клон є копією для запису початковий вміст якого збігається з вихідними даними. Створення пов'язаного клону відбувається майже миттєво, і спочатку не займає додаткового місця. Їх називають зв'язаними, оскільки новий шаблон все ще використовує оригінал. Немодифіковані блоки даних зчитаються з оригінального образу, але модифікації записуються, а потім і зчитуються з нового файла.

9.3.8 Основи адміністрування облікових записів платформи Proxmox VE

Платформа Proxmox VE підтримує автентифікацію користувачів з локальної бази ОС (Linux PAM), з каталогів LDAP, Microsoft Active Directory. Також можливим є використання інтегрованого сервера автентифікації ProxmoxVE. За допомогою облікових записів користувачів, груп та механізму ролей адміністратор має можливість налаштувати гнучкий доступ всіх об'єктів

хмарної інфраструктури (ВМ, сховищ, хостів тощо) можна налаштувати детальний доступ.

Proxmox VE зберігає атрибути облікових записів користувачів у файлі */etc/pve/user.cfg*. У ньому не містяться паролі, натомість для кожного запису вказується метод (realm) автентифікації. Обліковий запис ідентифікується у формі <логін>@<realm>. Кожен обліковий запис містить додаткову інформацію про користувача, зокрема ім'я, прізвище, адресу електронної пошти, членство у групах, ключ двофакторної автентифікації. Обліковий запис root, що використовує метод автентифікації Linux PAM є системним адміністратором платформи та має до неї необмежений доступ. Кожен користувач може входити до кількох груп. Офіційна документація платформи радить використовувати групи для організації та обмеження прав доступу користувачів.

У випадку, коли існує необхідність надати доступ користувачам до певного набору ресурсів використовують пули. Під ними розуміють набір віртуальних машин, контейнерів та пристроїв зберігання. Такий підхід дає можливість застосувати одне правило до набору елементів.

Основним методом автентифікації користувачів платформи є використання Linux PAM. Він забезпечує авторизацію користувачів ОС хоста. У випадку використання у інфраструктурі двох хостів (nodes), обліковий запис користувач повинен існувати на кожному з них.

Для забезпечення роботи багатьох користувачів доцільно налаштувати автентифікацію користувачів на основі каталогу LDAP або його реалізації Active Directory. Для автентифікації потрібно, щоб хост Proxmox VE міг виконувати запити до сервера каталогів. До основних параметрів, які слід вказати, для автентифікації за протоколом LDAP належать:

- IP-адреса та порт LDAP-сервера (контролера домену Active Directory);
- облікові дані користувача з повноваженнями читання даних з каталогу (операція Bind User);
- атрибути користувача, що слід отримати з каталогу (пошта, належність до групи);
- фільтри для обмеження доступу до певних організаційних підрозділів каталогу;
- додаткові параметри (об'єкти синхронізації, операції з новими обліковими записами, видалення існуючих);

Для входу в систему адміністратор може додати вручну один обліковий запис (рис. 9.50) або виконати синхронізацію усього каталогу. Вкалазі операції виконують за допомогою командного або веб-інтерфейсу.

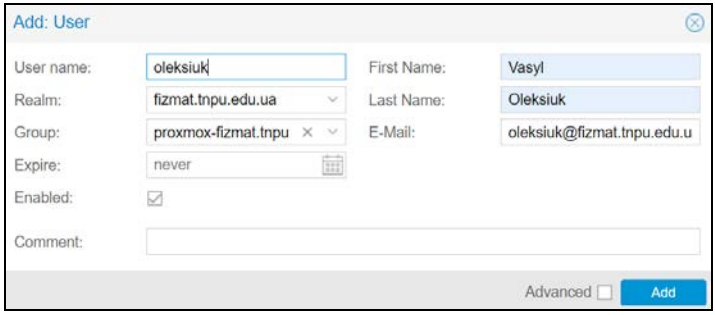

Рис. 9.50 Додавання облікового запису користувача платформи Proxmox VE

Для того, щоб користувач міг виконати певну дію (наприклад, перегляд, зміна або видалення частини конфігурації віртуальної машини), йому слід надати відповідні дозволи. Платформа Proxmox VE використовує систему керування дозволами на основі ролей і шляхів. Запис у таблиці дозволів дозволяє користувачеві, групі одержати певну роль під час доступу до об'єкта або шляху. Це означає, що таке правило доступу можна подати у вигляді трійки (шлях, користувач, роль), (шлях, група, роль) або (шлях, тег, роль), де роль містить набір дозволених дій, а шляхом є певний об’єкт інфраструктури, до якого застосовується правило.

Роль можна уявити як список дозволів. Платформа Proxmox VE містить перелік наперед визначених ролей, базовими серед яких є:

- Administrator – має усі повноваження;
- NoAccess – відсутні дозволи (використовується для заборони доступу);
- PVEAdmin – має більшість повноважень, але не може змінювати системні налаштування;
- PVEAuditor – має доступ лише для читання;
- PVEDatastoreAdmin – має повноваження для створення та виділення дискового простору для створення резервних копій та шаблонів;
- PVEDatastoreUser – має права для виділення місця для резервного копіювання та перегляду сховищ;
- PVEPoolAdmin – має права для виділення пулів;
- PVESysAdmin – має повноваження для створення списків керування доступом користувачів, аудиту, доступ до системної консолі та журналів;
- PVETemplateUse – передбачає права для перегляну та клонування шаблонів;
- PVEUserAdmin – має повноваження для управління обліковими записами користувачів;

- PVEVMAdmin – має усі права для адміністрування ВМ;
- PVEVMUser – користувач ВМ, володіє повноваженнями для перегляду, резервного копіювання, конфігурування пристроїв консолі, управління живленням ВМ.

Привілей можна уявити як право виконувати певну дію. Для спрощення управління списки привілеїв згруповані у ролі, які можна використовувати в таблиці дозволів. Привілеї не можна призначити безпосередньо стосовно користувачів чи шляхів. Повний перелік привілеїв можна знайти у офіційній документації платформи.

Права доступу призначаються об'єктам, зокрема віртуальним машинам, сховищам або пулам ресурсів. Для звернення до цих об'єктів платформа використовує шляхи, які подібні до файлової системи. Наведемо деякі приклади шляхів:

- /nodes/{node} – шлях до певного хоста Proxmox VE;
- /vms – шлях містить усі ВМ;
- /vms/{vmid} – шлях до певної ВМ;
- /storage/{storeid} – шлях до певного сховища.

9.3.8 Управління платформою Proxmox VE за допомогою інтерфейсу командного рядка та API-функцій

Як було зазначено вище, Proxmox VE надає доступ через веб-інтерфейс до консолі кожного хоста, що входить до кластера. Виконуючи команди у консолі адміністратор безпосередньо керує складниками інфраструктури. Наведемо кілька прикладів таких команд:

pvesh get /nodes – виводить список хотів у кластері;

pvesh set cluster/options -console html5 – задіює інтерфейс на основі HTML, як основну консоль ВМ;

Для управління віртуальними машинами Proxmox VE існує команду qm, за допомогою якої виконують такі операції:

- qm start <vmid> − запуск ВМ з вказаним ідентифікатором vmid;
- qm stop <vmid> − зупинення ВМ з вказаним ідентифікатором vmid;
- qm suspend <vmid> − призупинення ВМ;
- qm resume <vmid> − відновлення роботи ВМ;
- qm reboot <vmid> − перезавантаження;
- qm list − виведення списку ВМ, що створені на хості;
- qm clone <vmid> <newid> − створення повного або зв'язаного дубліката (клона) ВМ;
- qm migrate <vmid> <target> − міграція ВМ на інший хост;
- qm snapshot <vmid> <snapname> − створення знімка ВМ;
- qm delsnapshot <vmid> <snapname> − видалення знімка ВМ;

- qm config <vmid> − отримання конфігурації ВМ;
- qm create <vmid> [опції] – створення ВМ з вказаними опціями;
- qm destroy <vmid> − видалення ВМ;
- qm guest cmd <vmid> <command> − виконання вказаної команди на ВМ;
- qm guest exec-status <vmid> <pid> − отримання статусу виконання команди з ідентифікатором процесу pid;
- qm guest passwd <vmid> <username> − встановлення пароля для користувача username віртуальної машини;
- qm importdisk <vmid> <source> <storage> − імпортування диска з файла на вказане сховище;

Для прикладу, результатом виконання команди *qm config 180* є такі дані про конфігурацію ВМ з ідентифікатором 180:

- boot: order=scsi0;ide2;net0 – порядок використання пристроїв для завентаження ОС;
- cores: 1 – кількість ядер процесора ВМ;
- ide2: local:iso/ubuntu-22.04.2-live-server-amd64.iso,media=cdrom,size=1929660K – приєднаний образ диска у пристрій ide2;
- memory: 2048 – обсяг оперативної пам’яті;
- meta: creation-qemu=6.2.0,ctime=1677751941 – відомості про версію QEMU та час створення ВМ;
- name: vm2 – назва ВМ;
- net0: virtio=AA:3B:0E:40:A6:09,bridge=vmbr0,firewall=1 – відомості про тип мережного адаптера, його MAC-адресу, мостовий пристрій для приєднання та стан мережного фільтра (увімкнено);
- numa: 0 – стан використання технології нерівномірного доступу до пам’яті (вимкнено);
- ostype: l26 – тип ОС;
- scsi0: local-lvm:vm-180-disk-0,size=14G – параметри диска;
- scsihw: virtio-scsi-pci – дані про тип шини PCI;
- smbios1: uuid=6bd2d7e5-5c96-4042-8854-f9b278b043e4 – відомості про BIOS ВМ;
- sockets: 1 – кількість процесорів.

Для роботи з контейнерами існує аналогічна до qm команда pct. До команд для роботи з інфраструктурою Proxmox VE також належать:

- pvesm – утиліта для роботи зі сховищами;
- pvesubscription – «менеджер» підписок (використовуються для підтримки);
- pveperf – скрипт для вимірювання продуктивності хостів платформи;
- pveceph – засіб для роботи з сервісом сховищ CEPH;

- pvenode – утиліта для роботи з хостами;
- pvesh – інтерфейс для роботи з API;
- pveam – утиліта для роботи з шаблонами;
- pvecm – засіб для управління кластером;
- pvesr – утиліта для конфігурування реплікаціями сховищ;
- pveum – утиліта для роботи з обліковими записами користувачів;
- vzdump – утиліта для резервного копіювання ВМ та контейнерів;
- ha-manager – «менеджер» для конфігурування параметрів високої продуктивності платформи.

Proxmox VE використовує API-інтерфейс, що відповідає архітектурному стилю REST. Для того, щоб API вважався RESTful, він повинен відповідати таким критеріям:

- використання архітектури «клієнт-сервер», яку утворюють клієнти, сервери та ресурси, які керуються за допомогою HTTP(S)-запитів;
- тип зв'язку між клієнтом та сервером без збереження стану, тобто дані про клієнта не зберігається між запитами і кожен з них є окремим звертанням;
- використання кешування, що спрощує взаємодію між клієнтом та сервером.
- стандартизована форма подання даних, наприклад у форматі JSON, який є простим та придатним до аналізу з веб-браузера.

З детальною документацією щодо API можна ознайомитися за на офіційному сайті платформи Proxmox VE.

Подібно до процедури встановлення платформи API використовує протокол HTTPS та прослуховує порт з номером 8006. Отож, базова URL-адреса для цього запиту API є такою: https://<URL-адреса_сервера>:8006/api2/json/

Параметри API-запиту можна передати за допомогою стандартних методів:

- через URL-адресу;
- використовуючи тип вмісту 'x-www-form-urlencoded' для запитів, що надсилають дані методами PUT та POST.

У URL-адресі можна вказати формат повернення даних запиту. У наведеному вище прикладі використовується 'json', але можна використовувати будь-яке з таких значень: json, extjs, html, text.

Proxmox VE використовує автентифікацію на основі квитка або токена, усі запити до API повинні включати квиток у файлі cookie або надсилати токен API через заголовок авторизації. Квиток — це підписане випадкове текстове значення, який містить ім'я користувача та часову мітку. Квитки підписуються ключем автентифікації для всього кластера, та змінюють один раз на добу. Крім того, будь-який запит на запис (POST/PUT/DELETE) повинен містити токен запобігання CSRF всередині заголовка HTTP.

Наведемо приклад. Використовуючи утиліту Postman, отримаємо ключ та токен запобігання. Для цього створюємо новий запит, з використанням методу POST, вказуємо URL https://<URL-адреса_сервера:8006/api2/json/access/ticket, створюємо дві змінні логін і пароль та присвоїти їм відповідні значення (рис. 9.51).

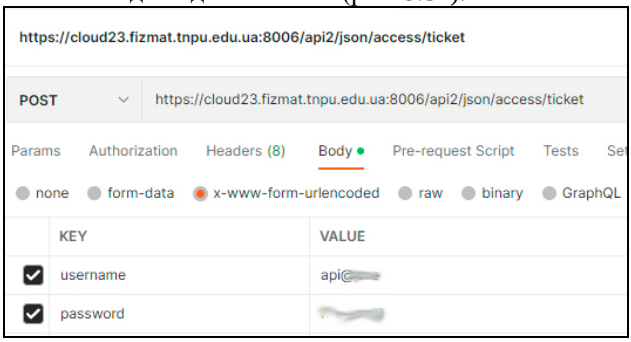

Рис. 9.51 Отримання ключа та токена запобігання в утиліті Postman

Токени можна створювати для окремих користувачів, і їм можна надавати окремі дозволи та дати закінчення, щоб обмежити обсяг і тривалість доступу. Для створення API слід у дереві об'єктів обрати Datacenter (рис. 9.52), та скористатися пунктом API. Після цього платформа згенерує секретний код для введеного токена. Якщо Токен API буде скомпрометований, його можна відкликати, не вимикаючи обліковий запис користувача.

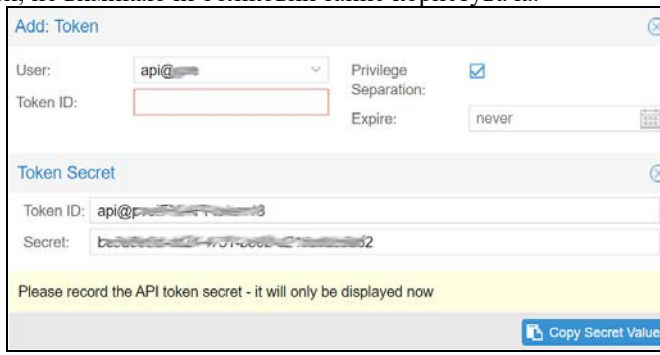

Рис. 9.52 Створення токена у веб-інтерфейсі Proxmox VE

Для того, щоб сформувати запит виклику API слід створити файл cookie, який буде містити отриманий із запиту ключ (рис. 9.51). У згаданій утиліті Postman створення файла cookie має такий вигляд (рис. 9.53). Отри-

маний з попереднього кроку ключ, присвоюють як значення змінної PVEAuthCookie.

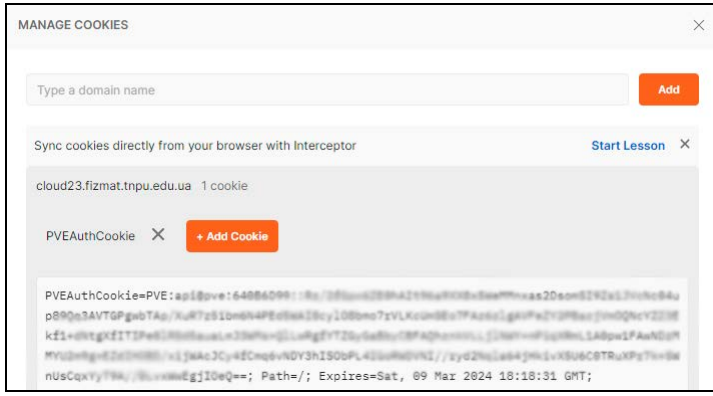

Рис. 9.53 Отримання ключа та токена запобігання в утиліті Postman

Використовуючи цей файл, можна надсилати API-запити до сервера Proxmox VE. Наприклад, через надсилання запиту методом GET за адресою https://<URL-адреса_сервера:8006/api2/json/nodes/ можна отримати список хостів кластера (рис. 9.54) або відомості про конкретний з них https://<URL-адреса_сервера:8006/api2/json/nodes/<назва_хоста>/status.

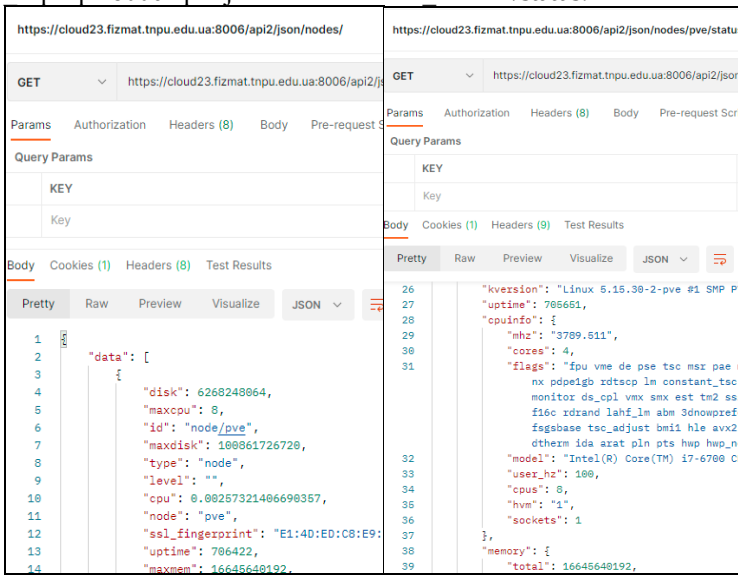

Рис. 9.54 Отримання даних про хост за допомогою запиту до API Proxmox VE

10. ЛАБОРАТОРНИЙ ПРАКТИКУМ

Лабораторна робота №1

Тема: Розгортання хмарного пакету Google Workspace

Мета роботи: *формування умінь реєстрації та початкового конфігурування пакету хмарних сервісів Google Workspace для освіти.*

1. У викладача отримати інформацію про дані організації та назву інтернет-домену, використовуючи які зареєструвати корпоративний обліковий запис Google Workspace для освіти. Заповнити таблицю.

№з/п	Дія	Екранна копія

2. Підтвердити власність інтернет-домену, створивши у ньому запис типу TXT. Заповнити таблицю:

№з/п	Дія	Екранна копія

3. Перевірити статус ліцензії хмарного пакету. Створити новий запит на отримання академічної підписки для сервісів Google Workspace. Заповнити таблицю:

№з/п	Дія	Екранна копія

4. Провести конфігурування інтернет-домену організації, додавши MX-записи, які забезпечують маршрутизацію електронної пошти. Використовуючи утиліти ОС або інтернет-сервіси перевірити коректність налаштувань. Заповнити таблицю:

№з/п	Дія	Екранна копія

5. Спроектувати структуру організаційних підрозділів освітнього закладу:
   - *учні* – підрозділ найвищого рівня;
   - *учителі* –підрозділ найвищого рівня;
   - *адміністрація* –підрозділ найвищого рівня.
6. У підрозділі «*учні*» створити структуру відповідно до розподілу дітей за класами. Заповнити таблицю:

№з/п	Дія	Екранна копія

7. На сторінці «*Користувачі*» панелі адміністрування завантажити шаблон електронної таблиці для додавання облікових записів. Заповнити їх окремо для кожного підрозділу, ввівши дані у такі поля:
   - ім'я (First Name);
   - прізвище (Last Name);
   - адреса електронної пошти (Email);
   - пароль (Password).
8. Виконати імпорт із створених таблиць. Перевірити коректність атрибутів створених облікових записів. Заповнити таблицю:

№з/п	Дія	Екранна копія

9. Перевірте коректність імпорту, зареєструвавшись з використанням даних кількох облікових записів.
10. Послідовно виконайте завдання 7-8 для усіх підрозділів освітнього закладу.
11. Створити такі облікові записи груп для таких категорій користувачів:
    - *teachers* – учителі;
    - *staff* – персонал школи;
    - *pupils* – усі учні;
    - *групи*, які відповідають класам школи.

    Додайти до них відповідні облікові записи користувачів. Заповнити таблицю:

№з/п	Дія	Екранна копія

12. Встановити такі рівні доступу до створених груп:
    - *teachers, staff* –загальнодоступний;
    - групи окремих класів (*7a, 7b*…) – командний;
    - *усі учні* – «лише повідомлення».

    Заповнити таблицю:

№з/п	Дія	Екранна копія

13. Перевірити коректність створення та надання доступу до облікових записів, надіславши електронні листи на зазначені у завдання групові адреси. Заповнити таблицю:

№з/п	Відправник	Одержувач	Результат надсилання

14. Встановити правила, що забороняють доступ учням 5-6 класів до сервісу відеоконференцій та надсилання миттєвих повідомлень Meet. Перевірити коректність налаштувань та заповнити таблицю

№з/п	Дія	Екранна копія

15. Створити роль «*класний керівник*», для якої передбачити можливість виконання таких дій:
    - рівень підрозділу – перегляд (читання) та оновлення даних;
    - рівень облікових записів користувачів – створення, перегляд (читання), оновлення (перейменування, зміна паролів, робота з псевдонімами) даних.

    Заповнити таблицю

№з/п	Дія	Екранна копія

16. Обліковим записам класних керівників делегувати визначені у попередньому завданні повноваження. Перевірити коректність налаштувань та заповнити таблицю

№з/п	Дія	Екранна копія

Лабораторна робота №2

Тема: Адміністрування поштового сервісу Gmail

Мета роботи: *формування умінь конфігурування хмарного сервісу Gmail.*

1. Використовуючи інтерфейс адміністратора, а також утиліти командного рядка ОС, перевірити налаштування маршрутизації пошти для зареєстрованого домену Google Workspace. За необхідності створити потрібні записи сервісу DNS. Заповнити таблицю:

№з/п	Дія	Екранна копія

2. Перевірити коректність налаштувань поштового сервісу, надіславши листи з адресами отримувача, які належать домену. Використати користувацький інтерфейс сервісу Gmail, а також проаналізувавши статистику журналу надсилання й отримання повідомлень у розділі *«Звіти»*. Заповнити таблицю:

№з/п	Дія	Екранна копія

3. Активувати використання у домені спільної адресної книги. Дозволити виведення усіх адрес електронної пошти та відображення лише профілів користувачів, які належать домену.
4. Дозволити користувачам змінювати фото у власному профілі.
5. Перевірити коректність налаштувань, виконаних у завданнях 4-5 та заповнити таблицю:

№з/п	Дія	Екранна копія

6. За вказівкою викладача додати кілька IP- та доменних адрес до списку дозволених відправників, до яких не застосовувати фільтри спаму.
7. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

8. За вказівкою викладача додати кілька IP- та доменних адрес до списку заборонених відправників.
9. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

10. У користувацьких налаштуваннях сервісу Gmail додати фільтр, для автоматичного перенесення листів певного відправника до папки *Спам*. Перевірити як перекриваються ці налаштування з параметрами, які були встановленні у завданнях 6 та 8. Заповнити таблицю та пояснити результат.

№з/п	Дія	Екранна копія

11. Налаштувати маршрутизацію усіх повідомлень на інший поштовий сервер (за вказівкою викладача). Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

12. Створити обліковий запис користувача *nonexistent*. У межах домену переспрямувати усі електронні повідомлення з неправильними адресами призначення на адресу *nonexistent@<назва_домену>*. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

13. Дозволити користувачам змінювати теми оформлення інтерфейсу Gmail. Перевірити коректність налаштувань.
14. Користувачам з підрозділів *teachers* та *staff* дозволити отримання повідомлень за протоколом POP3. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

15. Користувачам з підрозділу *pupils* дозволити автоматичне надсилання сповіщень про прочитання листа у межах домену. Користувачам з підрозділів *teachers* та *staff* дозволити надсилання зазначених сповіщень на будь-яку адресу, попередньо отримавши їх згоду. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

16. Для користувачів підрозділу *staff* дозволити делегувати доступ до їх скриньок. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

17. Дозволити користувачам з підрозділів *teachers* та *staff* автоматично пересилати вхідні листи на іншу адресу. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

18. Для облікового запису користувача *dir* переадресувати усю вхідну кореспонденцію на вказану викладачем поштову адресу. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

19. Для підрозділу *pupils* налаштувати перевірку вхідних повідомлень на відповідність певному вмісту. Повідомлення можуть бути надіслані як у межах домену, так і зовнішніми відправниками. Створити фільтр, який перевірятиме повідомлення на наявність слід ненормативної лексики. Виявлені повідомлення слід видаляти. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

20. Створити карантин *advertising*. Для усього домену створити фільтр, який перевірятиме заголовок та тіло повідомлення на наявність рекламного вмісту. Виявлені повідомлення слід поміщати до карантину.
21. Перевірити коректність налаштувань та заповнити таблицю:

№з/п	Дія	Екранна копія

22. Використовуючи розділ *«Звіти»*, переглянути результати виконаних налаштувань у завданнях 15-25. Заповнити таблицю:

№з/п	Дія	Екранна копія

23. Отримати статистику у графічному або табличному поданні:
    - використання користувачами сервісу Gmail;
    - надсилання та одержання повідомлень у межах домену.
    - перелік користувачів, які здійснювали автентифікацію протягом певної дати.

    Заповнити таблицю:

№з/п	Дія	Екранна копія

Лабораторна робота №3

Тема: Робота з хмарним сервісом Google Диск

Мета роботи: *формування умінь використання та конфігурування хмарного сервісу Google Диск.*

1. У інтерфейсі адміністратора для організації *teachers* дозволити використання спільних дисків. Заповнити таблицю.

№з/п	Дія	Екранна копія

2. Створити спільний диск *«Документація»*, до якого надати такі параметри доступу:
   - доступ для перегляду і коментування групі *teachers*, яка містить облікові записи учителів школи;
   - доступ для редагування групі *staff*, яка містить облікові записи адміністрації школи;

   Заповнити таблицю.

№з/п	Дія	Екранна копія

3. Створити на ньому папку Classes, у якій створити дерево папок, яка відповідає структурі класів.
4. До папки класу надати такі правила доступу:
   - доступ для перегляду і коментування групі, яка містить облікові записи учнів класу (наприклад, *7a, 7b*);
   - доступ для перегляду і коментування групі, яка містить облікові записи учителів школи (*teachers*);
   - доступ для редагування групі *staff*, яка містить облікові адміністрації школи;

   Заповнити таблицю.

№з/п	Дія	Екранна копія

На спільному диску створити шаблон журналу успішності, для певного класу. Наприклад, *шаблон_журнал_7а_2017-18.* На перший аркуш таблиці *Учні* додати список учнів та назви тем (рис. 5.10).

Прізвище	Ім'я	Дата1	Дата2	Дата3
		Тема1	Тема2	Тема3
Прізвище1	Ім'я1			
Прізвище2	Ім'я2			

Рис. 5.10 Шаблон таблиці-журналу

5. Використовуючи шаблон *шаблон_журнал_7а_2017-18,* створити таблицю *журнал_7а_2017-18.* У ньому скопіювати лист *«Учні»*, який назвати «*математика»*. Захистити аркуш «математика», надавши права на його редагування обліковому запису вчителя математики. Заповнити таблицю.

№з/п	Дія	Екранна копія

6. На спільному диску створити папку «*Архів»*, до якої надати доступ для редагування групам *teachers* та *staff*. Заповнити таблицю.

№з/п	Дія	Екранна копія

7. У межах домену заборонити обліковим записам надавати доступ користувачам, які не належать організації. Заповнити таблицю.

№з/п	Дія	Екранна копія

Для підрозділів *teachers* та *staff* дозволити надавати доступ користувачам, що не належать організації. Заповнити таблицю.

№з/п	Дія	Екранна копія

8. У межах домену заборонити обліковим записам надавати доступ за посиланням користувачам, які не належать організації. Перевірити коректність встановлених параметрів. Заповнити таблицю.

№з/п	Дія	Екранна копія

9. Для підрозділів *teachers* та *staff* дозволити надавати доступ за посиланням користувачам, що не належать організації. Перевірити коректність встановлених параметрів. Заповнити таблицю.

№з/п	Дія	Екранна копія

10. Для підрозділів *teachers* та *staff* дозволити користувачам переносити свої файли на спільні Диски. Перевірити коректність встановлених параметрів. Заповнити таблицю.

№з/п	Дія	Екранна копія

11. У межах домену дозволити користувачам вмикати до диска офлайн-доступ та використовувати клієнта Google Диска. Заповнити таблицю.

№з/п	Дія	Екранна копія

Лабораторна робота №4

Тема: Робота з хмарним сервісом Google Calendar

Мета роботи: *формування умінь використання та конфігурування хмарного сервісу Google Calendar.*

1. Використовуючи інтерфейс адміністратора сервісу Google Calendar, для підрозділу *staff* ввести дані про ресурси школи:
   - будівля школи – має перший та другий поверхи;
   - функції ресурсів – дошка, комп'ютер викладача, комп'ютери учнів, доступ до інтернету, проектор.

   Заповнити таблицю:

№з/п	Дія	Екранна копія

2. Створити такі ресурси – кабінети (класні кімнати) школи;
   - української мови – знаходиться на 1-му поверсі, місткість 30 учнів, наявність дошки;
   - історії – знаходиться на 1-му поверсі, місткість 30 учнів, наявність дошки та проектора;
   - математики – знаходиться на 1-му поверсі, місткість 30 учнів, наявність дошки, комп'ютера вчителя та проектора;
   - фізики – знаходиться на 2-му поверсі, місткість 30 учнів, наявність дошки, комп'ютера вчителя, проектора та доступу до інтернету;
   - інформатики – знаходиться на 2-му поверсі, місткість 15 учнів, наявність учительського та учнівських комп'ютерів, проектора та доступу до інтернету.

   Заповнити таблицю:

№з/п	Дія	Екранна копія

3. Створити Новий календар з такими параметрами:
   - назва – *«Розклад 7-а»*;
   - опис – *«Розклад 7-а класу 2017-18 навчального року»;*
   - заборона автоматичного прийняття запрошень;
   - відсутність доступу до календаря для усіх користувачів організації;
   - доступ для перегляду подій календаря користувачам груп *teachers* та *7а*;
   - доступ для редагування подій, а також керування спільним доступом календаря користувачам групи *staff*;

- відсутність сповіщень про нові події та заходи, які тривають цілий день;
- надсилання сповіщень електронною поштою та SMS про змінені або скасовані події;

Заповнити таблицю:

№з/п	Дія	Екранна копія

4. Зареєструватися у сервісі Google Calendar під обліковим записом підрозділу *teachers*. Створити календар «*Мій розклад*» з такими параметрами:
   - опис – «*Власний розклад уроків 2017-18 навчального року*»;
   - дозвіл автоматичного прийняття неконфліктних запрошень;
   - відсутність доступу до календаря для усіх користувачів організації;
   - наявність сповіщень електронною поштою та SMS про нові, змінені та скасовані події;

   Заповнити таблицю:

№з/п	Дія	Екранна копія

5. Зареєструватися у сервісі Google Calendar під обліковим записом підрозділу *staff*. Додати до календаря «*Розклад 7-а*» події згідно даних таблиці:

Назва уроку	День тижня	Час уроку	Учитель	Кабінет
українська мова	понеділок	8:30-9:15	teacher1	укр. мови
українська мова	вівторок	10:20-11:05	teacher1	укр. мови
українська мова	четвер	8:30-9:15	teacher1	фізики
алгебра	понеділок	11:15-12:00	teacher2	математики
алгебра	середа	11:15-12:00	teacher2	фізики
фізика	понеділок	9:20-10:10	teacher3	фізики
фізика	четвер	12:20-13:05	teacher3	фізики
інформатика	середа	10:20-11:05	teacher4	інформатики

   Встановити такі параметри подій:
   - назва події – відповідає назві уроку;
   - щотижнева повторюваність;
   - розташування (кімнати) – відповідно таблиці;
   - відсутність відеодзвінків;
   - надсилання запрошення відповідному учителю, дозвіл йому надсилати запрошення іншим користувачам;

   Заповнити таблицю:

№з/п	Дія	Екранна копія

6. Зареєструватися у сервісі Google Calendar під обліковим записом підрозділу *teachers*. Перевірити наявність подій у календарі *«Мій розклад»*. Заповнити таблицю:

№з/п	Дія	Екранна копія

7. Зареєструватися у сервісі Google Calendar під обліковим записом підрозділу *7а*. Перевірити доступність календаря *«Розклад 7-а»*. У випадку необхідності, додати його. Визначити, які дії з подіями доступні зареєстрованому користувачеві. Заповнити таблицю:

№з/п	Дія	Екранна копія

8. Для підрозділів *pupils* заборонити обліковим записам надавати доступ до подій користувачам, які не належать організації. Перевірити коректність встановлених параметрів. Заповнити таблицю.

№з/п	Дія	Екранна копія

9. Для підрозділів *teachers* та *staff* дозволити надавати доступ до подій користувачам, що не належать організації. Перевірити коректність встановлених параметрів. Заповнити таблицю.
10. Зареєструватися у сервісі Google Calendar під обліковим записом підрозділу *staff*. Створити календар «*Виробничі події*» з такими параметрами:
    - заборона автоматичного прийняття запрошень;
    - відсутність доступу до календаря для усіх користувачів організації;
    - доступ для перегляду подій календаря користувачам групи *teachers*;
    - доступ для редагування подій, а також керування спільним доступом календаря користувачам групи *staff*;
    - надсилання сповіщень електронною поштою та SMS про нові, змінені або скасовані події

    Заповнити таблицю.

№з/п	Дія	Екранна копія

Лабораторна робота №5

Тема: Робота з хмарним сервісом Google Classroom

Мета роботи: *формування умінь організації навчального процесу засобами хмарного сервісу Google Classroom.*

1. Зареєструватися у сервісі Google Classroom під обліковим записом адміністратора хмари. Створити курс *«Інформатика – 7а»*. Надіслати запрошення стати викладачем у курсі обліковому запису вчителя інформатики. Заповнити таблицю.

№з/п	Дія	Екранна копія

2. Зареєструватися у сервісі Google Classroom під обліковим записом учителя інформатики. Перевірити доступність курсу *«Інформатика – 7а»* та наявність повноважень викладача. Заповнити таблицю.

№з/п	Дія	Екранна копія

3. Надіслати запрошення стати учнями у курсі обліковим записам користувачів, що належать до групи *7а*. Заповнити таблицю. Вимкнути доступ до курсу *«Інформатика – 7а»* за кодом. Заповнити таблицю.

№з/п	Дія	Екранна копія

4. Зареєструватися у сервісі Google Classroom під обліковим записом учня відповідного класу. Перевірити доступність курсу *«Інформатика – 7а»*.
5. Зареєструватися у сервісі Google Classroom під обліковим записом адміністратора хмари. Встановити такі параметри сервісу:
   - дозволити підтвердженим викладачам на створювати курси;
   - дозволити кураторам переглядати інформацію у курсі;
   - дозволити викладачам керувати налаштуваннями доступу кураторів.

   Заповнити таблицю.

№з/п	Дія	Екранна копія

6. Зареєструватися у сервісі Google Classroom під обліковим записом учителя. Додати кураторів для одного-двох учнів, вказавши адресу електронної пошти, яка не належить домену школи. Прийняти запрошення. Заповнити таблицю.

№з/п	Дія	Екранна копія

7. Зареєструватися у сервісі Google Classroom під обліковим записом учителя інформатики. Додати до курсу тему *«Електронні таблиці»*.
8. У темі *«Електронні таблиці»* створити ресурс типу оголошення, який містить параграфи *«Уведення, редагування та форматування даних»*, збережені у форматі pdf. Заповнити таблицю.

№з/п	Дія	Екранна копія

9. У темі *«Електронні таблиці»* створити завдання *«Практична робота №1.»* з такими параметрами:
   - назва – «*Уведення, редагування та форматування даних в середовищі табличного процесора*»;
   - опис – «*Створіть на окремому аркуші електронну таблицю за наведеним зразком»;*
   - термін виконання – один тиждень;
   - долучити як файл електронну таблицю, яка містить зображення-взірець;
   - вказати необхідність скопіювати завантажений файл окремо для кожного учня.

   Заповнити таблицю.

№з/п	Дія	Екранна копія

10. Зареєструватися у сервісі Google Classroom під обліковим записом учня. Виконати завдання *«Практична робота №1»*.
11. Зареєструватися у сервісі Google Classroom під обліковим записом учителя. Створити форму *«Тест №1»* для проведення тестування з такими параметрами:
    - увімкнути оцінки, які показувати пізніше, після перевірки тесту вручну;
    - обов'язкове введення та збирання електронних адрес учнів;
    - сповіщення викладача про завершення тестування кожним учнем;
    - одна спроба виконання тесту;
    - заборона учням редагувати відповіді пісня надсилання тесту;
    - заборона перегляду учнями правильних відповідей, а також підсумкових даних, які стосуються усього класу;
    - виведення кількості балів за кожне запитання.

    Заповнити таблицю.

№з/п	Дія	Екранна копія

12. Додати до форми *«Тест №1»* 3 запитання з однією правильною відповіддю, 2 запитання з кількома правильними відповідями та одне запитання на введення правильної відповіді.

13. У темі «*Електронні таблиці*» створити завдання «*Тест №1*» з такими параметрами:
    - опис – «*Уведення, редагування та форматування даних в середовищі табличного процесора*»;
    - термін виконання – один день – найближча середа з 10:20 до 11:05;
    - долучити до завдання форму «*Тест №1*».

    Заповнити таблицю:
14. Зареєструватися у сервісі Google Classroom під обліковим записом учня. Виконати завдання «*Тест №1*».
15. Зареєструватися у сервісі Google Classroom під обліковим записом учителя. Виставити оцінки за виконання завдань «*Практична робота №1*» та «*Тест №1*». Переглянути діяльність учня на цього сторінці у курсі. Заповнити таблицю:

№з/п	Дія	Екранна копія

16. Увійти до електронної скриньки, яка була вказана при запрошенні куратора. Перевірити наявність сповіщень.
17. Зареєструватися у сервісах Google Диск та Календар під обліковим записом учителя. Які ресурси, пов'язані зі створеним курсом, там з'явилися?
18. Запропонуйте, як у сервісі Classroom можна організувати подання, нагадування та перевірку домашніх завдань.

Лабораторна робота №6

Тема: Робота з сервісом відеотрансляцій Google Meet

Мета роботи: *формування умінь створення та управління відеозустрічами засобами хмарного сервісу Google Meet.*

1. Зареєструватися як користувач сервісу Google Meet. Створити відеовиклик, вказавши електронну адресу співрозмовника. Не закриваючи вікна трансляції, перейти до сервісів Gmail та Google Calendar. Чи відображаються у них дані про відеодзвінок? Заповнити таблицю:

№з/п	Дія	Екранна копія

2. У трансляції увімкнути режим відображення певного вікна (наприклад, презентації або таблиці). Чи обов'язково співрозмовник буде їх бачити?
3. Із сеансу колеги запросити ще одного співрозмовника? Чи матимуть змогу усі учасники спілкуватися і бачити один одного одночасно?
4. Організатору відеодзвінка спробувати заблокувати третього учасника. Чи вплине таке блокування на його відображення у всіх користувачів? Заповнити таблицю:

№з/п	Дія	Екранна копія

5. Зареєструватися у сервісі Google Meet під обліковим записом адміністратора домену. Створити текстовий чат, запросивши до нього користувачів групи *7а*. Перевірити правильність виконання завдання та заповнити таблицю:

№з/п	Дія	Екранна копія

6. У інтерфейсі адміністратора заборонити користувачам підрозділу *pupils* спілкуватися у чаті з користувачами, які знаходяться за межами організації. Перевірити правильність виконання завдання та заповнити таблицю:

№з/п	Дія	Екранна копія

7. Перейти до сервісу YouTube. Створити нову трансляцію за допомогою додатку з такими параметрами:
   - назва – «*Семінар. Хмарні сервіси Google Workspace для освіти*»;
   - опис – «*Вебінар про можливості використання хмарного пакету Google Workspace у навчальному процесі*»;
   - дата та час початку – негайно;

- доступ для усіх користувачів;
- дозвіл використання текстових повідомлень під час трансляції;
- категорія відео – освіта;
- наявний доступ до відеозапису після завершення трансляції;
- дозвіл залишати коментарі після завершення відеозустрічі.

Заповнити таблицю:

№з/п	Дія	Екранна копія

8. Отримати посилання на трансляцію та надіслати його кільком користувачам.
9. Зареєструватися як учасник відеотрансляції. Перевірити можливості стати доповідачем, надсилати коментарі. Заповнити таблицю:

№з/п	Дія	Екранна копія

10. Зареєструватися як анонімний глядач трансляції. Які операції є доступними у цьому випадку?
11. Як модератор трансляції зробити доповідачем одного з учасників. Спробувати вимкнути веб-камеру або мікрофон доповідача.
12. Запросити ще одного користувача до відеозустрічі. Додати його як доповідача. Спробувати зробити доповідачем анонімного глядача. Перевірити коректність налаштувань. Заповнити таблицю:

№з/п	Дія	Екранна копія

13. Спробувати видалити одного з учасників трансляції та його коментарі. Пояснити результат. Заповнити таблицю:

№з/п	Дія	Екранна копія

Лабораторна робота №7

Тема: Встановлення хмарної платформи Apache CloudStack

Мета роботи: *формування умінь інсталювати платформу Apache CloudStack на ОС Ubuntu.*

1. Для виконання лабораторної роботи потрібно два комп'ютери, які працюють під управлянням ОС Ubuntu. Один з них буде виконувати функції сервера управління, та вторинного сховища, а інший – функції гіпервізора та первинного сховища.
2. Потрібно перевірити дані про ОС, визначивши назву наявного дистрибутиву ОС Linux та його версію.
3. На обох комп'ютерах додати репозитарій пакетів Apache CloudStack до списку сервер інсталяційних серверів ОС. Завантажити та додати відкритий ключ репозитарія до довірених ключів. Виконати поновлення індекс пакетів ОС. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

4. На першому комп'ютері виконати встановлення таких пакетів:
   - сервера управління – cloudstack-management;
   - сервер управління базами даних – mysql-server;
5. Встановити пароль користувача root на сервері MySQL. У файлі конфігурації *my.cnf* вказати такі параметри:
   - максимальна кількість з'єднань із сервером дорівнює 350;
   - двійковий (нестиснений – row) формат ведення журналу сервера.

   Перезавантажити сервер MySQL. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

6. Створити базу даних cloud, що необхідна для роботи сервера управління, вказавши такі параметри:
   - обліковий запис та пароль користувача cloud сервера MySQL;
   - розгортання бази даних з повноваженнями адміністратора (root) та його пароль;
   - шифрування бази даних з використанням файла;
   - пароль шифрування конфіденційних параметрів у файлі конфігурації Apache CloudStack;
   - пароль шифрування конфіденційних параметрів у базі даних;
   - IP-адресу сервера управління.

Завершити встановлення сервера управління та завантажити його сервіс. Перевірити наявність помилок у його журналі. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

7. На обох комп'ютерах встановити сервер мережної файлової системи (NFS). Створити папки, які будуть використані для розміщення спільних мережних ресурсів первинного та вторинного сховищ:
   - /export/secondary – на першому комп'ютері;
   - /export/primary – на другому комп'ютері.

   Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

8. На першому на другому комп'ютері створити спільні ресурси /export/primary та /export/secondary з такими параметрами:
   - доступ для читання та запису з комп'ютерів, які належать хмарі (сервер управління та гіпервізор);
   - асинхронний режим доступу;
   - інтерпретувати команди з привілеями адміністратора (root);
   - не виконувати додаткову перевірку дочірніх каталогів папки.

   Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

9. На сервері управління слід приєднати спільні ресурси первинного та вторинного сховищ у папку /mnt/primary та /mnt/secondary відповідно. Налаштувати автоматичне приєднання зазначених ресурсів до папок /mnt/primary та /mnt/secondary. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

10. Виконати команду завантаження до папки /mnt/secondary та встановлення системної віртуальної машини (ВМ) для роботи з гіпервізором KVM. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

11. Перейти до конфігурування хоста. На другому комп'ютері встановити пакет, необхідний для роботи хоста – cloudstack-agent. У файлі конфігурації вказати параметр автоматичного визначення моделі процесора хоста. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

12. Вказати такі параметри роботи бібіліотеки libvirt, що необхідна для роботи з віртуальними машинами:

- з'єднання за протоколм tcp та на порт з номером 16509;
- не використання автентифікації та протоколу TLS;
- повну підтримку протоколу TCP (файл */etc/default/libvirt-bin*).

Перезавантажити сервіс *libvirt-bin* та перевірити наявність помилок у його журналі. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

13. Вимкнути профіль AppArmor для бібліотеки libvirt. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

14. Встановити пакет bridge-utils. У файлі конфігурації мережі хоста описати такі мережні інтерфейси:
    - фізичний інтерфейс (наприклад eth0) слід увімкнути при завантаженні без присвоєння IP-адрес;
    - cloudbr0 – для передавання управляючого та гостьового трафіку. Параметри протоколів TCP/IP на вибір викладача або такі:
        - IP-адреса – 172.25.3.(100+N);
        - маска підмережі – 255.255.255.0;
        - шлюз за замовчуванням та DNS-сервера – 172.25.3.254;
    - cloudbr1 – для передавання приватного трафіку.

    Перезавантажити сервіс networking. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

15. Завантажити веб-інтерфейс сервера управління. Спробувати зареєструватися з використанням облікового запису користувача admin із стандартним паролем. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

Лабораторна робота №8

Тема: Робота з інтерфейсом платформи Apache CloudStack

Мета роботи: *формування умінь розгортати базову конфігурацію хмари та використовувати веб-інтерфейс платформи Apache CloudStack.*

1. Завантажити веб-інтерфейс сервера управління. Зареєструватися з використанням облікового запису користувача admin із стандартним паролем. Обрати базовий режим режим розгортання хмарної інфрастуктури.
2. Створити зону з назвою *zoneN*. Вказати адресу як внутрішнього, так зовнішнього DNS-сервера – 172.25.3.254. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

3. Створити стійку *PodN*, вказавши такі параметри:
   - адресу основного шлюзу – 172.25.3.254;
   - маску підмережі – 255.255.255.0;
   - діапазон IP-адрес для передавання загальнодоступного трафіку – 172.25.3.(130+4N-4)-172.25.3.(130+4N);
   - діапазон IP-адрес для передавання гостьового трафіку – 172.25.3.(30+4N-4)-172.25.3.(30+4N);

   Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

4. Додати кластер з назвою *ClusterN*. Вказати тип його гіпервізора – KVM.
5. Додати хост, вказавши його IP-адресу, логін та пароль користувача root. Вказати мітку хоста, яка відповідає імені комп'ютера, на якому виконується гіпервізор KVM. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

6. Додати первинне сховище *primary1*, вказавши його IP-адресу та шлях до спільної папки. Додати вторинне сховище *primary2*, вказавши його IP-адресу та шлях до спільної папки. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

7. Завантажити створення інфраструктури. Дочекатися завершення процесу. Переглянути системні журнали на сервері управління та хості. Пе-

ревірити наявність її складових – зони, стійки, кластера, хоста, сховищ, системних віртуальних машин. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

8. Створити віртуальну машину (ВМ) на основі наявного шаблона ОС CentOS з такими параметрами:
   - обчислювальну продуктивність віртуального комп'ютера – small instance;
   - відсутність диска (крім того, який містить шаблон);
   - відсутність групи спорідненості;
   - назву ВМ – CentOS1.
9. Дочекатися завантаження ВМ. Зареєструватися в ОС, вказавши стандартний логін та пароль. Перевірити мережні параметри ВМ та її доступність з мережі. Пояснити результат. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

10. Використовуючи групи безпеки, надати доступ до ВМ за протоколами TCP, UDP та ICMP з усіх IP-адрес. Перевірити правильність виконання завдання та заповнити таблицю:

№з/п	Дія	Команда або екранна копія

11. За допомогою панелі інструментів виконати такі основні операції з ВМ – вимкнути, перезавантажити, приєднати ISO-образ. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

12. Створити знімок ВМ. Внести зміни до ОС ВМ – створити папки, змінити конфігурацію системних файлів. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

13. Відновити стан ОС ВМ (до початкового стану або з використанням останнього знімка ВМ). Проаналізувати результат. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

14. Завантажити на сервер управління дистрибутив ОС Ubuntu. Додати його до зареєстрованих ISO образів хмари.

Вказівка: слід додати сервер, з якого буде виконуватися завантаження до довірених, змінивши серед глобальних налаштувань значення параметра *secstorage.allowed.internal.sites*.

Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

15. Використовуючи завантажений ISO-образ створити нову ВМ *Ubuntu1*. Налаштувати її мережні з'єднання та доступ за протоколом SSH. Перевірити коректність її функціонування.
16. На основі ВМ *Ubuntu1* створити шаблон *template-Ubuntu1* з такими параметрами:
    - тип ОС – Ubuntu відповідної версії та розрядності;
    - доступність для усіх користувачів;
    - динамічна зміна обсягу диска.

    Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

17. Використовуючи шаблон *template-Ubuntu1* створити ще одну ВМ *Ubuntu2.* Які існують відмінності між ВМ *Ubuntu1* та *Ubuntu1?*

Лабораторна робота №9

Тема: Розгортання розширеної хмарної інфраструктури на основі платформи Apache CloudStack

Мета роботи: *формування умінь розгортати складені мережі у хмарній інфраструктурі з використанням Apache CloudStack.*

1. На комп'ютері, що виконує функції сервера управління зупинити сервіс cloudstack-management. Видалити базу даних cloud. Очистити вміст папок /mnt/primary, /mnt/secondary.
2. Створити нову базу даних cloud, що необхідна для роботи сервера управління, вказавши такі параметри:
   - обліковий запис та пароль користувача cloud сервера MySQL;
   - розгортання бази даних з повноваженнями адміністратора (root) та його пароль;
   - шифрування бази даних з використанням файла;
   - пароль шифрування конфіденційних параметрів у файлі конфігурації Apache CloudStack;
   - пароль шифрування конфіденційних параметрів у базі даних;
   - IP-адресу сервера управління.

   Завершити встановлення сервера управління та завантажити його сервіс. Перевірити наявність помилок у його журналі.
3. Змінити мережні параметри на сервері управління та хості, додавши до нього віртуальні інтерфейси eth0.10 та eth0.20 з такими параметрами:
   - ідентифікатори віртуальної мережі 10 та 20 відповідно;
   - IP-адреса 192.168.10.N та 192.168.20.N відповідно;
   - маска підмережі – 255.255.255.0;

   Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

4. На сервері управління додати функції сервера первинного сховища, встановивши NFS-сервер.
5. На сервері управління додати функції хоста, встановивши пакет cloudstack-agent.
6. На сервері управління та хості налаштувати маршрутизацію у такий спосіб, щоб дозволити передавання даних у мережу 172.25.3.0/24 з мережі 192.168.10.0/24 та заборонити з 192.168.20.0/24. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

7. Створити розширену зону *AdvZone1*, вказавши такі параметри:
   - IP-адресу сервера DNS у загальнодоступній мережі – 172.25.3.254;
   - IP-адресу сервера DNS у приватній мережі – 172.25.3.253;
   - тип гіпервізора – KVM.

   Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

8. Виконати конфігурування мережі зони *AdvZone1*, вказавши такі параметри:
   - усі види трафіку передаються через інтерфейс *cloudbr0*;
   - метод ізоляції мереж – VLAN;
   - основний шлюз – 172.25.3.254;
   - маска підмережі – 255.255.255.0;
   - діапазон IP-адрес для передавання загальнодоступного трафіку – 172.25.3.(130+4N-4)-172.25.3.(130+4N);
9. Додати стійку *AdvPod1*, вказавши такі параметри:
   - основний шлюз – 172.25.3.254;
   - маска підмережі – 255.255.255.0;
   - діапазон IP-адрес для передавання гостьового трафіку – 172.25.3.(30+4N-4)-172.25.3.(30+4N);

   Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

10. Додати інші складові інфраструктури:
    - два хости, обов'язково вказавши для них теги;
    - два первинних сховища;
    - вторинне сховище.

    Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

11. Завантажити створення інфраструктури. Дочекатися завершення процесу. Переглянути системні журнали на сервері управління та хості. Перевірити наявність її складових – зони, стійти, кластера, хоста, сховищ, системних віртуальних машин. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

12. Додати 2 гостьові мережі до фізичних мереж зони, вказавши їх мітки – *gnet10* та *gnet20*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

13. Для доданих гостьових мереж створити шаблони мережних послуг *gnet10tmpl* та *gnet20tmpl*, з такими параметрами:
    - тип мережі – спільна;
    - використання VLAN;
    - сервіси, які доступні у мережі – DHCP-сервер.

    Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

14. У інфраструктурі додати гостьові мережі *network10 (network20)*, вказавши такі їх параметри:
    - назву та опис;
    - номер VLAN – 10(20);
    - шаблон мережних послуг – gnet10tmpl (gnet20tmpl);
    - основний шлюз – 192.168.10.N (192.168.20.N);
    - маска підмережі – 255.255.255.0;
    - діапазон IP-адрес, які виділяють ВМ: 192.168.10.102–192.168.10.199 (192.168.20.102–192.168.20.199).

    Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

15. Створити 2 віртуальні машини *vm1* та *vm2*, першу з яких додати до мережі *network10,* а другу – до *network20.* Визначити мережні параметри створених ВМ, використовуючи їх ОС та веб-інтерфейс Apache CloudStack. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

16. Перевірити чи передається трафік з мережі *network10* (*network20*) до зовнішніх мереж, а також між собою. Пояснити результат.
17. Додати ВМ *vm1* до мережі *network20*. Встановити мережні параметри відповідного інтерфейсу. Перевірити зв'язок між ВМ *vm1* та *vm2*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

18. Чи можна налаштувати передавання даних з ВМ *vm2* до зовнішніх мереж (інтернету) через *vm1*?

Лабораторна робота №10

Тема: Адміністрування платформи Apache CloudStack

Мета роботи: *формування умінь управління ресурсами хмарної інфраструктури Apache CloudStack.*

1. Зареєструватися як адміністратор хмарної інфраструктури. Створити домен *d1*. У домені *d1* створити два облікові записи *u1* та *u2*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

2. Зареєструватися під обліковим записом користувача *u1*. На основі шаблона *template-Ubuntu1* створити віртуальну машину (ВМ) *vm11* з шаблоном продуктивності *Small Instance.* Завантажити створену ВМ. Переглянути статистику використання нею обчислювальних ресурсів хмари. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

3. Зареєструватися як адміністратор хмарної інфраструктури. У домені *d1* створити обліковий запис *a1*, якому надати повноваження адміністратора домену.
4. Зареєструватися під обліковим записом користувача *a1*. Вимкнути ВМ *vm11*. Додати до ВМ *vm11* додаткову IP-адресу та налаштувати її використання ОС. Передати право власності на ВМ *vm11* користувачу *u2*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

5. Зареєструватися під обліковим записом користувача *u2*. Увімкнути ВМ *vm11*. Визначити на якому хості виконується ВМ. Перевірити коректність налаштування додаткової IP-адреси. Створити знімок ВМ *vm11*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

6. Зареєструватися під обліковим записом користувача *a1*. Спробувати створити шаблон продуктивності *d1instance*. Пояснити що спостерігається.
7. Зареєструватися під обліковим записом користувача адміністратора хмари. Створити шаблон продуктивності *d1instance* з такими параметрами:

- тип сховища – спільне;
- кількість ядер процесора, які будуть виділені ВМ – 2;
- обсяг оперативної пам'яті – 512 Мб;
- необмежену швидкість передавання даних в мережі;
- режим резервування ресурсів – нестрогий;
- приналежність шаблону домену *d1*.

Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

8. Зареєструватися під обліковим записом користувача *u2*. Змінити шаблон продуктивності ВМ *vm11* на *d1instance.* Увімкнути ВМ та перевірити виділення обчислювальних ресурсів для неї. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

9. Зареєструватися під обліковим записом користувача *a1*. Створити групи спорідненості, які відповідають тегам хостів. Вимкнути ВМ *vm11*. Змінити її параметри, вказавши створені групи спорідненості. Увімкнути ВМ. Які зміни спостерігається? На якому хості виконується ВМ? Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

10. Зареєструватися під обліковим записом користувача *u1*. Чи доступні для користувача *a2* групи спорідненості, що були створені адміністратором домену *a1*?
11. Створити власні групи спорідненості, які відповідають тегам хостів. На основі шаблону CentOS створити ВМ *vm12*, вказавши шаблон продуктивності *Small instance* та створені групи спорідненості.
12. Увімкнути ВМ, визначити на якому хості вона виконується. Перевірити виділення для неї обчислювальних ресурсів. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

13. Зареєструватися як адміністратор хмарної інфраструктури. У домені *d1* створити два облікові записи *u3* та *u4*.
14. Зареєструватися як адміністратор домену *a1*. У домені *d1* створити проект *pr1* з такими параметрами:
    - максимальна кількість ВМ користувача –1;
    - максимальна кількість публічних IP-адрес – 2;
    - максимальна кількість ядер процесора – 1;
    - максимальний обсяг оперативної пам'яті – 512 Мб;
    - необмежені обсяги використовуваних сховищ.

Надіслати запрошення до проекту користувачам *u3* та *u4*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

15. Зареєструватися під обліковим записом користувача *u3*. У проекті *pr1* на основі шаблона *template-Ubuntu1* створити ВМ *vm21* з шаблоном продуктивності *Small Instance*. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

16. Зареєструватися під обліковим записом користувача *u3*. У проекті *pr1* спробувати створити ще одну ВМ *vm22*. Що спостерігається?
17. Зареєструватися під обліковим записом користувача *u4*. Які ВМ є доступними для користувача. Визначити виділення обчислювальних ресурсів для кожної з них та порівняти з встановленими обмеженнями для проекту. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

18. У проекті *pr1* на основі шаблона *template-Ubuntu1* створити ВМ *vm22* з шаблоном продуктивності *d1instance*. Пояснити що спостерігається?

Лабораторна робота №11

Тема: Розгортання хмарної платформи Proxmox

Мета роботи: *формування умінь інсталювати віртуальне середовище Proxmox VE та розгортати хмарну інфраструктуру на його основі.*

1. Для виконання лабораторної роботи потрібен віртуальний комп'ютер. Створити у корпоративній хмарі ВМ з такими параметрами:
    a. ISO-образ – Proxmox;
    b. продуктивність – EVE-NG instance;
    c. диск обсягом 35 Гб;
    d. мережа – network13.
2. Встановити платформу Proxmox. Використати типові налаштування та увесь доступний дисковий обсяг. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

3. Відімкнути віртуальний ISO-диск та завантажити платформу Proxmox з основного носія. Перейти за посиланням, яке буде вказано на екрані терміналу.
4. Зареєструватися у з використанням облікового запису root. Переглянути хмарну інфраструктуру. Заповнити призначення та основні характеристики таких її складників:
- датацентр;
- PVE;
- local (PVE);
- local-LVM (PVE).

Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

5. До сховища local (PVE) додати ISO-образ диска, що вказаний викладачем. Вказівка: замість веб-інтерфейсу варто безпосередньо завантажити обраний образ за протоколом SFTP до папки /var/lib/vz/template/iso.
6. На основі завантаженого образу створити ВМ з такими параметрами:
- назва ВМ – w100;
- кількість ядер процесора – 2;
- тип центрального процесора– host;
- обсяг оперативної пам'яті – 2Гб;

- обсяг диска – 12 Гб;
- мережевий адаптер – e100.

Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

7. Встановити на ВМ w100 операційну систему із завантаженого ISO-образа (див. завданні №5)
8. Налаштувати мережні параметри та віддалений доступ до ВМ w100.
9. Вимкнути ВМ w100 та ОС PVE. До ВМ, яка виконує PVE додати мережний інтерфейс network12.
10. Увімкнути ВМ PVE. Додати мережний інтерфейс типу «Linux Bridge», який відповідає інтерфейсу network12.

Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

11. Додати 2-ий мережевий адаптер до ВМ w100. Увімкнути ВМ w100. Отримати мережні параметри за протоколом DHCP.
12. Завантажити шаблон Ubuntu-16.04-standart або Ubuntu-20.04-standart.
13. Використовуючи завантажений шаблон, створити контейнер з такими параметрами:
    - назва контейнера – cte101;
    - кількість ядер процесора – 1;
    - обсяг оперативної пам'яті – 512 Мб;
    - обсяг диска – 8 Гб;
    - 2 мережевих адаптери – e100 (для першого з них встановити статичну IP-адресу, а для іншого отримати за протоколом DHCP).

Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

14. Завантажити створений контейнер. Зробити висновок про його відмінності від віртуальної машини.
15. Об’єднати у кластер власний хост та хост колеги. Перевірити можливість управління обома хостами.
16. Налаштувати NFS-сервер на власному хості. Створити папку /export/nfs, до якої надати доступ для читання та запису.
17. Додати нове сховище типу NFS, вказавши шлях до спільної папки на NFS-сервері. Вказати призначенням сховища збереження дисків ВМ та контейнерів. Заповнити таблицю:

№з/п	Дія	Команда або екранна копія

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Биков В.Ю. Технології хмарних обчислень, ІКТ-аутсорсінг та нові функції ІКТ-підрозділів навчальних закладів і наукових установ / В.Ю. Биков // Інформаційні технології в освіті. – Випуск 10. – Херсон: ХДУ, 2011. – № 10. – С. 8-23.
2. Глазунова О.Г. Принципи формування «академічної хмари» сучасного університету на основі відкритих програмних платформ. // Інформаційні технології і засоби навчання. – 2014. – №5 (43). – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/1096
3. Литвинова С.Г. Хмарні сервіси Office 365 : навчальний посібник / С. Г. Литвинова, О. М. Спірін, Л. П. Анікіна. – Київ. : Компринт, 2015. – 170 с.
4. Олексюк В. П. Досвід інтеграції хмарних сервісів Google Apps у інформаційно-освітній простір вищого навчального закладу. [Електронний ресурс]/ В. П. Олексюк // Інформаційні технології і засоби навчання. — 2013. — №3. — Режим доступу до журн.: http://journal.iitta.gov.ua/index.php/itlt/article/view/824/631
5. Олексюк В. П. Проектування моделі хмарної інфраструктури ВНЗ на основі платформи Apache CloudStack. Електронний ресурс]/ В. П. Олексюк // Інформаційні технології і засоби навчання. – 2016. – №4. – Режим доступу до журн.: http://journal.iitta.gov.ua/index.php/itlt/article/view/1453/1074
6. Розгортання та адміністрування хмарної платформи Google Workspace for education у закладі вищої освіти / О. М. Спірін та ін. *Інформаційні технології і засоби навчання*. 2022. Т. 92, № 6. С. 172–197. DOI: https://doi.org/10.33407/itlt.v92i6.5078
7. Сейдаметова З. С. Облачные технологии и образование. / [З. С. Сейдаметова, Э. И. Аблялимова, Л. М. Меджитова и др.]. – Сімферополь : «ДИАЙПИ», 2012. – 204 с.
8. Фамілярська Л. Організація освітнього середовища післядипломної педагогічної освіти засобами хмарних сервісів Google / Л. Фамілярська // Інформатика та інформаційні технології в навчальних закладах. – 2015. – № 5/6. – С. 38–44.
9. Шишкіна М. П. Формування і розвиток хмаро орієнтованого освітньо-наукового середовища вищого навчального закладу : монографія / М. П. Шишкіна. – К. : УкрІНТЕІ, 2015. – 256 с.
10. Ярмахов Б., Рождественская Л. Google Apps для образования. – СПб.: Питер, 2015. – 224 с.

11. Antonopoulos N. Cloud Computing. Principles. Systems and Applications / N. Antonopoulos, L. Gillam. – London; New York: Springer-Verlag, 2010. – 379 p.
12. Balyk N., Vasylenko Ya., Oleksiuk V., Shmyger G. Designing of Virtual Cloud Labs for the Learning Cisco CyberSecurity Operations Course. *Proceedings of the 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*, Kherson, Ukraine, June 12-15, 2019. CEUR Workshop Proceedings. Volume 2393. P. 960-967. http://ceur-ws.org/Vol-2393/paper_338.pdf
13. Cloud computing. Principles and Paradigms. / Edited by Rajkumar Buyya, James Broberg, Andrzej Goscinski. – New Jersey: John Wiley & Sons, Inc., 2011. – 641 p.
14. Oleksiuk V., Oleksiuk O. The practice of developing the academic cloud using the Proxmox VE platform. *Educational Technology Quarterly*. 2021(4), pp.605–616. DOI: https://doi.org/10.55056/etq.36.
15. Oleksiuk V., Oleksiuk O., Spirin O., Balyk N., Vasylenko Ya. Some experience in maintenance of an academic cloud. Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020). Kryvyi Rih, Ukraine, December 18, 2020. CEUR Workshop Proceedings. 2019. URL: https://ceur-ws.org/Vol-2879/paper06.pdf
16. Oleksiuk V., Oleksiuk O. Methodology of teaching cloud technologies to future computer science teachers. Proceedings of the 7th Workshop on Cloud Technologies in Education (CTE 2019). Kryvyi Rih, Ukraine, December 20, 2019. CEUR Workshop Proceedings. 2019. URL: https://ceur-ws.org/Vol-2643/paper35.pdf
17. Spirin O.M, Oleksiuk V., Balyk N., Lytvynova S., Sydorenko S. The blended methodology of learning computer networks: cloud-based approach. *Proceedings of the 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*, Kherson, Ukraine, June 12-15, 2019. CEUR Workshop Proceedings. Volume 2393. P. 68-80. http://ceur-ws.org/Vol-2393/paper_231.pdf (Last accessed: 02.12.2022) ***(індексується у Scopus)***.

СЛОВНИК ТЕРМІНІВ

Active Directory – служба каталогів для організації доменів ОС Windows. З логічної токи зору домен Active Directory організовано у вигляді дерева об'єктів.

Apache CloudStack – проект компанії Apache Software Foundation, у межах якого розробляється програмне забезпечення з відкритим вихідним кодом, що може бути застосоване для розгортання загальнодоступних і корпоративних хмар згідно моделі «інфраструктура як сервіс» (IaaS).

DNS (Domain Name System) – служба перетворення рядкових адрес серверів інтернет у числові IP-адреси, що організовує групи комп'ютерів у мережі інтернет за допомогою ієрархії доменів.

Gmai – хмарний сервіс електронної пошти від компанії Google. Надає доступ до поштових скриньок через веб-інтерфейс і за протоколами POP3, SMTP та IMAP.

Google Workspace – це пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google, доступний за передплатою

Internet (від англ. *Interconnected Networks – об'єднані мережі*) – глобальна комп'ютерна мережа, яку утворюють з'єднані мережі провайдерів, організацій, осіб тощо.

IaaS (Infrastructure-as-a-Service) – модель, яка передбачає розгортання у «хмарі» інформаційної інфраструктури організації. Основою для реалізації моделі є технології віртуалізації.

IP (Internet Protocol) – мережний протокол, що відповідає за передавання і маршрутизацію повідомлень між вузлами інтернет.

IP-адреса – це послідовність чотирьох байт, які записують у вигляді десяткових чисел, розділених крапками; є унікальною адресою комп'ютера в мережі.

HTTP (від англ. *Hypertext Transfer Protocol* – протокол передавання гіпертексту) – один з найпоширеніших мережних протоколів інтернету, основа Web.

NFS – див. Мережна файлова система.

OpenStack – це комплекс проектів вільного програмного забезпечення для створення обчислювальних хмар. Основними програмними складовими OpenStack

Organization Unit – див. Підрозділ.

PaaS (Platform-as-a-Service) – модель, яка передбачає розгортання у хмарі певної програмної платформи, яку можуть використовувати не лише користувачі сервісу, а й програмісти та розробники.

RDP (Remote Desktop Protocol) – протокол віддаленого робочого столу – протокол ОС Windows, який описує правила передавання даних між клієнтом та сервером терміналів.

Router – див. маршрутизатор.

SaaS (Software as a Service) – модель надання програмного забезпечення, згідно якої для повнофункціонального його використання клієнту необхідний лише веб-браузер.

SMTP (від англ. *Simple Mail Transfer Protocol* – простий протокол передавання пошти) – це мережний протокол, призначений для передавання електронної пошти.

TCP (від англ. *Transmission Control Protocol*) – протокол керування передаванням) – мережний протокол, призначений для керування передаванням та передавання даних у мережах стеку протоколів TCP/IP.

TCP/IP – стек мережних протоколів, на яких базується інтернет. Назва утворена з абревіатур двох базових протоколів – TCP та IP.

URL (від англ. *Uniform Resource Locator*) – це стандартизований спосіб запису адреси ресурсу в мережі інтернет.

Авторизація – процес надання доступу до мережних ресурсів. Зазвичай відбувається після аутентифікації.

Акаунт (обліковий запис) Google – це єдиний обліковий запис для доступу до хмарних сервісів корпорації Google.

Автентифікація – процес перевірки достовірності користувача в операційній системі, який полягає у порівнянні його імені та пароля з даними, що зберігаються в базі даних операційної системи.

Браузер – програма для перегляду веб-сторінок. Існує чимало програм-браузерів: Internet Explorer, Netscape Navigator, Mozilla, Opera тощо.

Веб-вузол – див. Веб-сайт.

Веб-сайт – це сукупність веб-сторінок, об'єднаних змістовно, URL яких має спільне доменне ім'я (D N S -ім'я).

Веб-сервер – це набір програм, які забезпечують обмін даними засобами протоколу передавання гіпертексту HTTP.

Власник – обліковий запис користувача, який створив об'єкт файлової системи.

Гібридна хмара (англ. hybrid cloud) – це хмарна інфраструктура, що складається з двох або більше різних хмарних інфраструктур (приватних, громадських або публічних), які залишаються унікальними сутностями, але з'єднанні між собою стандартизованими або приватними технологіями, що уможливлюють переносимість даних та прикладних.

Гіпервізор (англ. hypervisor) – програма, що виконує віртуальні машини.

Група – сукупність облікових записів користувачів, яка має окремий ідентифікатор. Правила, які застосовуються до групи діють на кожен обліковий запис користувача, що входить до неї.

Диск Google (англ. Google Drive) – хмарне сховище даних, яке належить компанії Google Inc., що дозволяє користувачам зберігати свої дані на серверах у хмарах та ділитися ними з іншими користувачами хмар в інтернеті.

Домен – логічне об'єднання комп'ютерів, контролер якого містить спільну базу облікових записів користувачів.

інтернет – див. Internet.

Інтерфейс (від англ. Interface – поверхня розділу, перегородка) – сукупність засобів, методів і правил взаємодії (управління, контролю і т. д.) між елементами системи. У комп'ютерних науках під інтерфейсом розуміють не тільки пристрої, але й правила (протокол) їх взаємодії.

Клієнт-сервер – мережна архітектура, у якій усі пристрої є або клієнтами, або серверами. Клієнтом є машина (зазвичай ПК), що відправляє запит,

сервером – машина, що відповідає на запит. Обидва терміни (клієнт і сервер) можуть бути застосовані як до фізичних пристроїв, так і до програмного забезпечення.

Комутатор (switch) – пристрій, що визначає адресу кожного повідомлення і з'єднує комп'ютер-відправник та комп'ютер-адресат.

Контролер домену – комп'ютер, який містить базу даних об'єктів домену.

Логін – ім'я користувача, яке використовують у процесі аутентифікації.

Локальна комп'ютерна мережа – сукупність певного числа комп'ютерів, розміщених на відносно незначній території.

Маршрутизатор (router) – пристрій, що з'єднує в одну мережу окремі мережі, що можуть працювати за різними протоколами. Роль маршрутизатора може виконувати комп'ютер. Основними завданнями маршрутизатора є визначення раціонального маршруту передавання пакетів даних від одного вузла мережі до іншого та їх передавання.

Мережна плата (мережний адаптер) – це апаратний пристрій, що забезпечує фізичне підключення комп'ютера до мережі. Це або спеціальна плата розширення, що містить гніздо для підключення мережних кабелів, або окремий пристрій, який підключають через порт USB. У сучасних комп'ютерах мережна плата часто інтегрується в материнську плату. Для використання мережної плати необхідно встановити її драйвери.

Мережний протокол – набір правил, за якими відбувається обмін даними між комп'ютерами в мережі.

Мережна файлова система (NFS – Network Filesystem) – засіб для створення розподілених ресурсів у ОС типу Unix. Основою функціонування NFS є однойменний протокол (NFS).

Монтування – процес приєднання файлових систем у ОС Linux.

Он-ла́йн (англ. on-line) – зв'язок, який підтримується у режимі реального часу (безперервно).

Організаційна одиниця – див. Підрозділ.

Пароль – код доступу для одержання закритих даних (наприклад, для входу у домен).

Підрозділ – контейнер, в якому можуть зберігатися інші об'єкти Active Directory.

Поштовий клієнт – програма передавання клієнтові отриманих поштовим сервером повідомлень.

Поштовий сервер – програма пересилання, завданням якої є отримання повідомлень відправника та їхнє подальше передавання в мережі, а також передавання отриманих поштовим сервером повідомлень клієнтові.

Приватна хмара (англ. private cloud) – це хмарна інфраструктура, яка призначена для використання виключно однією організацією. Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Публічна (загальнодоступна) хмара (англ. public cloud) – це хмарна інфраструктура, яка призначена для вільного використання широким загалом. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи будь-якої їх комбінації). Публічна хмара перебуває в юрисдикції постачальника хмарних послуг**.**

Ретрансляція – функція SMTP-сервера, який передбачає обмеження передавання листів, що надсилаються різними клієнтами.

Розподілений мережний ресурс – каталог або пристрій, до якого організовано доступ через мережу і який має унікальне мережне ім'я.

Сайт – у доменах Active Directory частина мережі, де всі контролери домену зв'язані швидким, недорогим і надійним мережним підключенням.

Сервер – комп'ютер або програма, що надає свої ресурси іншим комп'ютерам у мережі.

Сесія [сеанс] (session) – активне з'єднання поміж користувачем, комп'ютером або поміж двома комп'ютерами. Сеанс роботи користувача (зв'язку з джерелом інформації). Період взаємодії абонентів, який складається з трьох фаз: установлення з'єднання, передавання інформації та завершення з'єднання.

Системний адміністратор – особа, яка виконує функції управління операційною системою. Системний адміністратор використовує відповідний обліковий запис операційної системи, наприклад, root або administrator.

Складена мережа – сукупність кількох мереж. Мережі, які належать до складеної мережі, називають підмережами.

Топологія – спосіб організації фізичних з'єднань, опис конфігурації мережі, схема розташування і з'єднання мережних пристроїв. Мережна топологія може бути: фізичною – опис реального розташування і зв'язків між вузлами мережі та логічною – опис переміщення сигналу в рамках фізичної топології.

Трафік – 1) потік даних у локальній або глобальній мережі; 2) обсяг даних, що надходить на комп'ютер з мережі й відправлений з нього в мережу.

Хмарні технології (англ. Cloud Technology) – модель забезпечення повсюдного і зручного мережного доступу на вимогу до деякої супупності налаштовуваних обчислювальних ресурсів.

Хост – будь-яка одиниця комп'ютерної техніки, підключена до комп'ютерної мережі, наприклад, комп'ютер, сервер, маршрутизатор тощо. Як правило, для позначення імені хоста, використовують його мережне ім'я (для локальної мережі), IP-адресу чи доменне ім'я (для інтернету). У хмарних технологіях під хостом (нодою) розуміють комп'ютер, що виконує програму гіпервізор.

Чат – (пер. з анг. бесіда) спілкування двох і більше користувачів інтернет в епістолярному стилі в режимі реального часу, тобто одночасно в тому самому «вікні». Учасники чата пишуть повідомлення й оперативно одержують відповідні послання на цьому ж екрані.

Шлюз – у комп'ютерних мережах проміжний вузол, що забезпечує зв'язок комп'ютерів з різних сегментів мережі.

ЗМІСТ

ДЛЯ НОТАТОК

Навчальне видання

Олексюк Василь Петрович
Спірін Олег Михайлович

ОСНОВИ ХМАРНИХ ТЕХНОЛОГІЙ

Навчально-методичний посібник

Інститут цифровізації освіти.
Національної академії педагогічних наук України
м. Київ, вул. Максима Берлінського, 9
Свідоцтво про державну реєстрацію:
серія ДК №7609 від 23.02.2022 р.
Електронна пошта (E-mail): iitzn_apn@ukr.net