КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.627
УДК 004.75

**Смірнова Тетяна Віталіївна**
к.т.н., доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-6896-0612
*sm.tetyana@gmail.com*

**Конопліцька-Слободенюк Оксана Костянтинівна**
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-9981-5194
*ksuha80@gmail.com*

**Буравченко Костянтин Олегович**
к.т.н., доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-6195-7533
*buravchenkok@gmail.com*

**Смірнов Сергій Анатолійович**
к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0002-7649-7442
*smirnov.ser.81@gmail.com*

**Кравчук Оксана Вікторівна**
інспектор відділу кадрів
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0009-0008-8453-0557
*vov-14@i.ua*

**Козірова Наталія Леонідівна**
асистент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0009-0005-8753-5132
*natalidonchenko23@gmail.com*

**Смірнов Олексій Анатолійович**
д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-9543-874X
*dr.smirnovoa@gmail.com*

# ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНИХ СЕРВІСІВ IAAS, PAAS ТА SAAS

**Анотація.** Загрози кібербезпеки постійно еволюціонують, і хмарні обчислення не є винятком. Зловмисники вдосконалюють техніки атак, спрямовані на виявлення вразливостей в IaaS, PaaS та SaaS. У роботі розглянуті наступні проблемні питання: недостатність аналітичних засобів; конфіденційність та безпека даних; іінансові та організаційні витрати для забезпечення

кібербезпеки хмарних технологій IaaS, PaaS та SaaS. Метою роботи є дослідження того, яким чином для поширених моделей хмарних обчислень: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) і програмне забезпечення як послуга (SaaS) необхідно належно впровадити адекватні і відповідні заходи захисту для забезпечення кібербезпеки. Для цього у роботі були досліджені моделі хмарних технологій, визначено, що хмарні сервіси включають різні моделі, які дозволяють користувачам отримувати доступ до різних видів ресурсів через Інтернет. Виявлено, що існує три загальноприйняті моделі хмарних сервісів: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS), а також два основних гравці: хмарний провайдер та абонент хмарних послуг. Набір рівнів, над якими кожен з цих гравців має контроль, залежить від моделі хмарного сервісу або середовища. Для кожного з цих хмарних сервісів було наведено його опис, надані рекомендації щодо контролю доступу, забезпечення конфіденційності, визначено умови використання, наведені переваги та недоліки, розглянуті тенденції ринки даних послуг. Запропоновані підходи до формування безпечного середовища розробки додатків у хмарних сервісах. Також узагальнено такі характеристики, як широкий доступ до мережі, об'єднання ресурсів, швидка еластичність, вимірювання сервісів та обмін даними. Запропоновано рекомендації щодо проектування контролю доступу для IaaS, PaaS і SaaS відповідно до їхніх різних характеристик. Крім того, узагальнені правила політики безпеки для кожної хмарної системи. Запропоновано технології захисту безпеки на кожному з трьох основних рівнів хмарних сервісів: рівні додатків, проміжного програмного забезпечення та віртуальних машин, через відмінності в організації, яка контролює кожен з цих рівнів. Виявлено, що для будь-якого рівня можливо забезпечити більш ефективний захист, якщо той самий суб'єкт контролює рівень, що знаходиться нижче. Оскільки мережевий, апаратний та рівень абстракції ресурсів у всіх моделях хмарних сервісів контролюються хмарним провайдером, він має в своєму розпорядженні більш ефективні засоби захисту.

**Ключові слова:** кібербезпека; контроль доступу; конфіденційність; комп'ютерні науки; хмарні сервіси; телекомунікаційна система; IaaS; PaaS; SaaS.

## ВСТУП

**Постановка завдання дослідження.** У зв'язку зі зростаючим впровадженням моделей хмарних обчислень — інфраструктури як послуги (IaaS), платформи як послуги (PaaS) і програмного забезпечення як послуги (SaaS) — реалізація адекватних і належних заходів захисту безпеки стала першочерговим завданням.

Загрози кібербезпеці постійно еволюціонують, і хмарні обчислення не є винятком. Зловмисники вдосконалюють техніки атак, спрямовані на виявлення вразливостей як назагал у хмарних сервісах, так й у хмарних сервісах, дослідженню кібербезпеки яких призначена дана робота: IaaS, PaaS та SaaS.

Захист конфіденційності даних є ключовим завданням для багатьох організацій, особливо в контексті обробки конфіденційної корпоративної та особистої інформації. Використання хмарних послуг покладає особливі вимоги до захисту цієї інформації. З урахуванням динаміки кількості та складності атак на інфраструктуру хмарних сервісів, важливо розробляти та впроваджувати ефективні та сучасні засоби захисту для попередження інцидентів безпеки. Успішне впровадження хмарних послуг вимагає високого рівня довіри користувачів. Забезпечення адекватного рівня захисту допомагає зберігати довіру користувачів та дотримуватися регуляторних вимог. Хмарні технології стають все більш поширеними, зокрема серед малих та середніх підприємств. З цієї причини, важливість адекватних заходів захисту виявляється для різних рівнів організацій.

В архітектурному стеку корпоративних обчислень компоненти на всіх рівнях належать або контролюються однією сутністю — підприємством. Однак у середовищах хмарних служб управління різними рівнями розділено між постачальником хмарних послуг і передплатником хмарних служб залежно від моделі хмарної служби. У даній

роботі досліджується вплив цієї різниці в контролі на набір фактичних заходів захисту, які можуть бути реалізовані на різних рівнях для різних моделей хмарних сервісів. Також вказується на цінність доступу до нижніх рівнів для реалізації заходів захисту компонентів на більш високому рівні.

Актуальність теми полягає у необхідності розробки та вдосконалення стратегій та технологій захисту в хмарному середовищі, щоб забезпечити безпеку, конфіденційність та доступність даних у сучасному інформаційному світі.

Завданням даного дослідження є систематичний аналіз можливостей та викликів використання IaaS, PaaS та SaaS щодо кібербезпеки з метою розробки рекомендацій для їх оптимального впровадження.

Таким чином, виходячи з усього вищенаведеного, актуальним завданням яке вирішується у даній роботі є дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS для оптимізації процесів виявлення та протидії кіберзагрозам.

**Постановка проблеми.** Розгляд підходів для забезпечення кібербезпеки хмарних технологій IaaS, PaaS та SaaS у кібербезпеці виявив наступні проблемні питання:

- Недостатність аналітичних засобів: Сучасні кіберзагрози стають все більш витонченими, вимагаючи від організацій вдосконалення своїх засобів виявлення. Питанням залишається, наскільки концепції IaaS, PaaS та SaaS можуть надати високотехнологічні аналітичні інструменти для вчасного виявлення та відповіді на нові кіберзагрози.
- Конфіденційність та безпека даних: Перед впровадженням IaaS, PaaS та SaaS важливо вирішити питання щодо збереження конфіденційності та безпеки оброблюваних даних в хмарному середовищі.
- Фінансові та організаційні витрати: Визначення ефективності та обгрунтованості витрат на впровадження IaaS, PaaS та SaaS вимагає ретельного оцінювання економічних та організаційних аспектів.

Таким чином, це дослідження прагне відповісти на зазначені питання та вирішити визначені проблеми, сприяючи розробці стратегій ефективного використання IaaS, PaaS та SaaS у сфері кібербезпеки.

**Аналіз останніх досліджень і публікацій.** Різні рівні в архітектурному стеку хмарних сервісів базуються на основі невеликих відмінностей від моделі, запропонованої альянсом з безпеки хмарних сервісів [1]. Незважаючи на те, що існує загальний консенсус щодо загроз і цілей безпеки для кожного рівня [2], незрозумілим залишається вплив різниці в контролі над різними рівнями в різних моделях хмарних сервісів (або середовищах) на набір заходів захисту безпеки, які можуть бути реалізовані. У даній роботі пропонуються підходи до побудови заходів захисту для кожного рівня в трьох моделях хмарних сервісів — IaaS, PaaS та SaaS.

**Мета статті.** Дослідити яким чином для поширенних моделей хмарних обчислень — інфраструктура як послуга (IaaS), платформа як послуга (PaaS) і програмне забезпечення як послуга (SaaS) необхідно належно впровадити адекватні і відповідні заходи захисту для забезпечення кібербезпеки. В архітектурному стеку обчислювальної системи підприємства компоненти на всіх рівнях належать або контролюються одним суб'єктом — підприємством. Однак в середовищах хмарних сервісів контроль над різними рівнями розділений між хмарним провайдером і хмарним абонентом на основі моделі хмарного сервісу. У даній роботі досліджується вплив цієї різниці у реалізації контролю на набір фактичних заходів захисту безпеки, які можуть бути реалізовані на різних рівнях для різних моделей хмарних сервісів. Також вказується на значення доступу до нижчих рівнів для реалізації заходів захисту для компонентів на вищому рівні.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

**Моделі хмарних технологій**

Завдяки підтримці різних сервісних моделей, хмарні системи можуть надавати широкий спектр послуг кінцевим користувачам, розробникам та системним адміністраторам. Хмарні системи розроблялися протягом часу і концептуалізуються через поєднання програмного забезпечення, апаратних компонентів і технологій віртуалізації [3].

Такі характеристики хмари, як об'єднання ресурсів, швидка еластичність та послуги, що оплачуються по мірі використання, прискорили її широке впровадження в промисловості. Зокрема, хмарні системи пропонують послуги для додатків, зберігання даних, управління даними, мережу та управління обчислювальними ресурсами для споживачів через мережу (та інтернет загалом). Прикладами популярних хмарних додатків є веб-сервіси електронної пошти (наприклад, Gmail від Google, Office 365 Outlook від Microsoft), сховища даних (наприклад, Google Drive, Microsoft OneDrive, Dropbox) для кінцевих користувачів, а також системи управління взаємовідносинами зі споживачами та бізнес системи (наприклад, Customer Relationship Management (CRM) Cloud, Workday) для управління бізнесом.

Незважаючи на значний прогрес хмарних систем, існує занепокоєння щодо запропонованих рівнів безпеки та конфіденційності. Важливість цих побоювань стає більш очевидною, якщо врахувати зростаючу кількість користувачів, які перейшли на хмарні сервіси.

Моделі розгортання хмарних технологій (наприклад, публічна хмара, приватна хмара, хмара спільноти, гібридна хмара тощо) конфігуруються залежно від обсягу користувачів, сервісів та ресурсів хмари на основі вимог до сервісів, вони можуть бути розгорнуті приватно, розміщені на території виділеної інфраструктури споживача хмарних послуг або провайдера, або розміщені публічно одним або декількома постачальниками хмарних послуг. Система може бути налаштована і використовуватися одним споживачем або групою довірених партнерів, або підтримувати багатокористувацьку оренду і бути загальнодоступною для різних кінцевими користувачами, які придбали послугу. Залежно від типу моделі розгортання хмари, хмара може мати обмежені приватні обчислювальні ресурси або доступ до великої кількості віддалених ресурсів з віддаленим доступом. Різні моделі розгортання передбачають ряд компромісів у тому, як споживачі можуть контролювати свої ресурси, а також масштаб, вартість і доступність цих ресурсів [4]. Архітектура хмарної системи складається, загалом, з наступних шарів функцій:

VM (Virtual Machine), в тому числі:

- Додатки;
- Інтерфейс прикладного програмування (API);
- Операційна система (ОС);
- Гіпервізор;
- Сховище;
- Мережа;
- Апаратне забезпечення.

Хмарний сервіс може надавати доступ до програмних додатків, таких як електронна пошта або офісні інструменти (тобто модель «Програмне забезпечення як послуга», або SaaS); середовище для споживачів, де вони можуть створювати та експлуатувати власне програмне забезпечення (тобто модель «Платформа як послуга», або PaaS), або мережевий доступ до віртуалізованих обчислювальних ресурсів, таких як обчислювальні потужності та сховища (тобто Інфраструктура як послуга, або IaaS). Різні

моделі обслуговування мають різні сильні сторони і підходять для різних споживачів і бізнес-цілей [5].

Хмарні сервіси включають різні моделі, які дозволяють користувачам отримувати доступ до різних видів ресурсів через Інтернет. Зараз існує три загальноприйняті моделі хмарних сервісів [1], [8] — Інфраструктура як послуга (IaaS), Платформа як послуга (PaaS) та Програмне забезпечення як послуга (SaaS), а також два основних гравці — хмарний провайдер та абонент хмарних послуг. Набір рівнів, над якими кожен з цих гравців має контроль, залежить від моделі хмарного сервісу або середовища.

**IaaS (Інфраструктура як послуга)**

Інфраструктура як послуга (IaaS). Можливість, що надається споживачеві, полягає в наданні обробки, зберіганні мереж та інших основних обчислювальних ресурсів, де споживач може розгортати і запускати довільне програмне забезпечення, яке може включати операційні системи та додатки. Споживач не керує і не контролює базову хмарну інфраструктуру, але має контроль над операційними системами, сховищами та розгорнутими додатками і, можливо, обмежений контроль над окремими мережевими компонентами (наприклад, брандмауерами хостів) [8].

Приклади: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

**Рекомендації щодо контролю доступу до IaaS**

Безпека хмарної системи IaaS значною мірою залежить від віртуалізації (гіпервізора). Одним з найбільш поширених рішень для їх захисту є система управління віртуалізацією [15], яка знаходиться між базовим обладнанням та гіпервізором. Система управління віртуалізацією забезпечує захист як гіпервізорів, так і віртуальних машин різними способами. Системи управління віртуалізацією забезпечують різні рівні доступу на різних користувачів. Деяким користувачам надається доступ до адміністративного інтерфейсу гостьової ОС лише для читання; деяким дозволяється керувати окремими гостьовими ОС, а деяким надається повний адміністративний контроль.

**Рекомендації щодо забезпечення конфіденційності Iaas**

Шифрування даних:

- Використовуйте шифрування для захисту даних під час їх транспорту та зберігання в хмарному середовищі.
- Розглядайте можливість використання шифрування на рівні файлової системи або віртуальних дисків.

Керування доступом:

- Використовуйте сильні механізми автентифікації та авторизації для обмеження доступу до інфраструктурних ресурсів.
- Встановлюйте політики «найменших привілеїв» для керування рівнями доступу користувачів.

Мережева безпека:

- Використовуйте файрволи для контролю мережевого трафіку та обмеження доступу до служб.
- Забезпечте безпеку мережевих з’єднань, використовуючи VPN або інші методи шифрування для захисту даних під час їх передачі.

Моніторинг та аудит:

- Регулярно проводьте моніторинг діяльність інфраструктури для виявлення ненормальних патернів та потенційних загроз безпеці.
- Встановлюйте системи аудиту для запису подій та аналізу активності користувачів.

Фізична та логічна ізоляція:

- Забезпечте фізичну і логічну ізоляцію між віртуальними машинами та іншими ресурсами.
- Використовуйте технології віртуалізації та контейнеризації для створення ізольованих середовищ.

Резервне копіювання та відновлення:

- Регулярно створюйте резервні копії важливих даних та конфігурацій для можливості відновлення в разі втрати чи пошкодження.
- Управління ідентифікацією та ключами:
- Ефективно управляйте ідентифікацією та ключами, використовуючи безпечні методи зберігання та обміну ключами.

Стандарти безпеки:

- Стежте за стандартами безпеки та використовуйте актуальне програмне забезпечення та протоколи.

Оновлення та патчі:

- Регулярно оновлюйте оперативні системи, програмне забезпечення та компоненти — інфраструктури для усунення вразливостей.

Планування для інцидентів:

- Розробляйте плани відновлення після інцидентів та здійснюйте тренування персоналу щодо їх використання.

Ці рекомендації слід взяти до уваги під час проектування та експлуатації інфраструктури в середовищі IaaS для максимального забезпечення конфіденційності даних.

**Умови використання IaaS**

Давайте обговоримо випадки, коли IaaS здається найкращим варіантом, якщо вам доводиться вибирати між IaaS, PaaS і SaaS [6]:

- Ви стартап, якому бракує коштів, необхідних для створення інфраструктури.
- Ви використовуєте великі дані. У цьому випадку вам потрібна інфраструктура як послуга. Відзначається здатністю справлятися з великими навантаженнями. Крім того, ця послуга хмарних обчислень сумісна з інструментами бізнес-аналітики. З їх допомогою можливо прогнозувати галузеві тенденції та створювати інноваційні продукти та послуги.
- Ваша компанія переживає стрімке зростання. За допомогою рішень IaaS ви можете легко змінювати конкретне апаратне чи програмне забезпечення відповідно до ваших потреб, що розвиваються.
- У вас немає точних вимог до вашої заявки. IaaS відомий своєю гнучкістю та масштабованістю.

**Переваги хмарної моделі IaaS**

**Масштабованість за вимогою.** Очевидною перевагою хмарної моделі IaaS є те, що її можливо швидко масштабувати відповідно до зростаючих бізнес-вимог вашої компанії. Постачальники IaaS пропонують найпотужнішу технологію зберігання даних і мереж, щоб задовольнити потреби своїх клієнтів [7].

**Велика надійність.** Припустимо, виходить з ладу певний апаратний компонент або ви втрачаєте підключення до Інтернету. Ці технічні проблеми не вплинуть на вашу інфраструктуру. Крім того, як правило, постачальники IaaS розподіляють навантаження системи на кілька центрів обробки даних і серверів. Таким чином, обчислювальні ресурси, апаратне забезпечення та хмарні програми завжди будуть доступні.

**Операційна гнучкість.** IaaS надає вашій команді доступ до апаратного забезпечення, обчислювальної потужності та програм, які регулярно використовуються. Завдяки цьому вони можуть будь-коли переглядати необхідні файли та дані на ходу.

**Аварійне відновлення (DR) і безперервність бізнесу (BC).** Більшість планів DR дорогі та громіздкі. Якщо компанія має кілька філій, їй необхідно встановити окремі плани DR і BC для кожної філії. Тим часом IaaS поєднує DR і BC у своїх планах обслуговування. Якщо трапиться катастрофа, компанія може покластися на них, зменшуючи витрати та зберігаючи керованість бізнесу.

**Недоліки інфраструктури як послуги**

Давайте розглянемо основні недоліки цієї хмарної моделі:

- **Проблеми із застарілими системами.** У хмарі можливо запускати застарілі програми. Однак може статися, що інфраструктура не розроблена для захисту таких програм. Цей факт змушує вас вдосконалювати свою програму, перш ніж перемістити її в хмару.
- **Внутрішнє навчання є обов'язковим.** З рішеннями IaaS ви матимете справу з безпекою даних, резервним копіюванням і безперервністю бізнесу. Це означає, що вашій команді доведеться навчитися керувати новою інфраструктурою. В іншому випадку процес моніторингу та управління ресурсами може стати занадто складним.
- **Відсутність гнучкості.** Постачальники IaaS обслуговують і оновлюють апаратне та хмарне програмне забезпечення. Якщо служби, з якими ви працюєте, не оновлюються регулярно, ефективність і продуктивність вашої команди можуть бути скомпрометовані.
- **Питання безпеки даних.** IaaS дозволяє керувати програмами, даними, проміжним програмним забезпеченням і ОС платформи. У той же час ви не можете контролювати безпеку зв'язку між інфраструктурою та віртуальними машинами. Таким чином, ви залежите від заходів безпеки, які пропонує ваш постачальник IaaS.

**Тенденції ринку IaaS**

За даними досліджень у 2021 році ринок IaaS зріс на 41,4%. Це зростання відбувається завдяки підтримці IaaS потреб бізнесу, таких як масштабованість і здатність швидко впроваджувати інновації. Крім того, постачальники IaaS прагнуть задовольнити потреби компаній у постійному розвитку та безпеці [8].

Ще один тренд, який буде присутній у найближчому майбутньому — регіональні хмарні екосистеми. Завдяки геополітичній різноманітності провайдери IaaS із сильною локальною присутністю мають чудові можливості.

**PaaS (Платформа як послуга)**

Можливість, що надається споживачеві, полягає в розгортанні в хмарі інфраструктуру створених споживачем або придбаних додатків, створених за допомогою мови програмування, бібліотеки, сервісів та інструментів, що підтримуються провайдером. Споживач не керує і не контролює базову хмарну інфраструктуру, включаючи мережу, сервери, операційні системи або сховища, але має контроль над розгорнутими додатками і, можливо, над налаштуваннями конфігурації середовища, в якому розміщені додатки [9].

Приклади: Heroku, Microsoft Azure App Service, Google App Engine.

**Рекомендації щодо контролю доступу до PaaS**

Необхідно розробити ефективний метод захисту даних пам'яті шляхом очищення кешу процесора під час перемикання контексту. Однак, щоб уникнути значного погіршення продуктивності, слід очищати лише високочутливі дані пам'яті.

Для управління доступом до декількох реплік даних слід запровадити метод управління централізованою політикою. Таким чином, як тільки дані в межах провайдера PaaS дублюються між провайдерами PaaS, будь-яка зміна в політиці, повинна призводити до відповідного оновлення центральної політики доступу до даних системи. Крім того, політика управління доступом, пов'язана з реплікованими даними в інших постачальників PaaS, повинна бути синхронізуватися відповідно політики контролю доступу в центральній системі.

**Рекомендації щодо забезпечення конфіденційності Paas**

Platform as a Service (PaaS) є однією з моделей хмарних послуг, і захист конфіденційності даних у цьому контексті вельми важливий. Ось декілька рекомендацій щодо забезпечення конфіденційності у PaaS:

1. Шифрування даних (Застосовуйте шифрування для даних, які зберігаються та передаються в середовищі PaaS. Використовуйте як можливо більше шифрувальних методів, таких як TLS для захисту передачі даних та шифрування на рівні бази даних).
2. Доступ та автентифікація (Використовуйте сильну автентифікацію для забезпечення, що лише вповноважені користувачі мають доступ до сервісів PaaS; керуйте правами доступу, використовуючи концепції найменувань (least privilege), щоб кожен користувач отримував лише ті права, які необхідні для виконання його завдань).
3. Моніторинг та аудит (Встановлюйте системи моніторингу для виявлення ненормальної активності, вразливостей та атак; проводьте регулярні аудити для перевірки налаштувань конфігурації, доступу та інших параметрів безпеки).
4. Фізична та логічна ізоляція (Забезпечте фізичну та логічну ізоляцію між різними користувачами на платформі; використовуйте віртуалізацію та контейнеризацію для забезпечення ізоляції середовищ).
5. Резервне копіювання та відновлення (Регулярно створюйте резервні копії даних та конфігураційних параметрів; тестуйте процедури відновлення, щоб переконатися в їх ефективності в разі виникнення проблем).
6. Ідентифікація та управління ризиками (Регулярно оцінюйте ризики безпеки та вживайте заходів для їх зменшення або усунення).

Забезпечення конфіденційності в середовищі PaaS вимагає комплексного підходу та постійного вдосконалення заходів безпеки.

**Умови використання**

Коли вам доводиться вибирати між IaaS, PaaS та SaaS, обирайте рішення платформи як послуги, якщо:

- Ви надаєте послуги з розробки програмного забезпечення на замовлення.
- Кілька розробників у вашій компанії працюють над одним проектом. У цьому випадку продукти «платформа як послуга» додають гнучкості та швидкості всьому процесу.
- Ваша компанія розробляє мобільні додатки. Завдяки гнучким рішенням PaaS ви можете створювати міжплатформні програми. Вони будуть адаптовані під будь-який пристрій і операційну систему.

**Доставка PaaS**

Доставка PaaS така ж, як і SaaS. Єдина відмінність полягає в тому, що PaaS не доставляє програмне забезпечення через Інтернет, а пропонує середовище. PaaS звільняє розробників від турбот про інфраструктуру, операційні системи або зберігання даних.

Використовуючи спеціальні компоненти, вбудовані в PaaS, розробники проектують і створюють програмне забезпечення. Ці компоненти включають операційні системи, засоби розробки та проміжне програмне забезпечення.

**Переваги PaaS**

- **Економічна ефективність.** З хмарними рішеннями PaaS вам більше не потрібно створювати програми з нуля. Отже, це хороший варіант, якщо у вас обмежені ресурси або ви хочете зменшити свої операційні витрати.
- **Швидкий запуск.** Попередньо створена серверна інфраструктура дозволяє швидко створювати прототипи та розробляти. У результаті ви можете миттєво випустити свою програму. Ранній запуск, у свою чергу, підвищує ваші шанси на успіх.
- **Скорочений час розробки.** Постачальники PaaS надають вам доступ до різноманітних бібліотек, фреймворків, шаблонів та інших інструментів. Усі ці інструменти прискорюють і спрощують весь процес розробки.
- **Швидке тестування та розгортання.** PaaS забезпечує гнучкість доступу до різних машин і різних конфігурацій для тестування вашого додатка. Це надає широкі можливості для тестування продуктивності та сумісності ваших програм. Таким чином, ви можете вносити зміни в додатки, створені в PaaS, за короткий час.
- **Легке обслуговування.** Платформа як послуга звільняє розробників від створення, оновлення та налаштування серверів. Провайдери PaaS відповідають за такі речі.
- **Швидкий обмін даними в командах.** Продукти PaaS зазвичай дозволяють обмінюватися даними між багатьма командами розробників. Таким чином, компанії не потрібно виділяти однакові ресурси для окремих команд розробників.
- **Інтеграція та агрегація даних.** Створення додатків зазвичай передбачає інтеграцію та агрегацію даних з часом. Системи PaaS включають необхідні компоненти, що прискорює роботу з розробки.

**Недоліки моделі «платформа як послуга»**

- **Проблеми з виконанням.** Іноді ви можете виявити, що моделі послуг PaaS не налаштовані для мов програмування та фреймворку, які ви хочете використовувати. Крім того, може статися, що певна версія фреймворку недоступна з хмарними службами PaaS.
- **Зміни від постачальника.** Зміни в поточній архітектурі, внесені постачальниками PaaS, можуть стати для вас серйозною проблемою. Давайте подивимося, як це працює. Припустимо, ви працюєте з мовою Ruby. Він сумісний із хмарним рішенням, яке ви використовуєте. Раптом постачальник розгортає оновлення, яке потребує Python для подальшої сумісності. У вас є два варіанти: змінити мову програмування або постачальника PaaS.
- **Відсутність налаштування для застарілих систем.** Якщо у вас є застарілі програми чи служби, ви можете помітити, що вони погано працюють із

продуктами PaaS. Щоб вирішити цю проблему, вам доведеться інвестувати значні кошти в налаштування та зміни конфігурації [10].

- **Межі експлуатаційної здатності.** Налаштовані хмарні операції мають автоматизоване керування робочими процесами. Це може не працювати добре з рішеннями PaaS. Таким чином, робочі параметри можуть бути обмежені для ваших кінцевих користувачів.
- **Питання безпеки даних.** Сервісні моделі PaaS дозволяють запускати власні рішення або служби. Але ви не контролюєте дані, розміщені на хмарних серверах, якими керують треті сторони. Тому безпека залежить від постачальника PaaS і третіх сторін. Якщо ваші клієнти мають певну політику хостингу, вони можуть не мати змоги розгорнути свої послуги.

**Тенденції ринку PaaS**

Попит на гнучкість, масштабованість і гнучкість визначає розвиток ринку PaaS. Компанії PaaS пропонують складні інфраструктури. Отже, незалежні постачальники програмного забезпечення можуть зосередитися на підвищенні бізнес-цінності своїх хмарних продуктів [11].

Ще одна тенденція полягає в тому, що PaaS пропонує модель самообслуговування. Це означає, що розробник може завантажити скомпільований код і миттєво запустити програму. Такий підхід підходить як для стандартних, так і для індивідуальних рішень. Цей метод допоможе зростати ринку PaaS у найближчому майбутньому.

У той же час різноманітність додатків, представлених на ринку, заважає ефективності бізнесу. Коли справа доходить до створення великомасштабних програм, розробникам потрібно використовувати різні рішення PaaS. Наприклад, це може включати поєднання PaaS для інтерфейсу користувача, обміну повідомленнями та безпеки. Тому ця тенденція заважає зростанню ринку PaaS.

**SaaS (Програмне забезпечення як послуга)**

Програмне забезпечення як послуга (SaaS). Можливість, що надається споживачеві, полягає у використанні додатків провайдера, що працюють на хмарній інфраструктурі. Доступ до додатків здійснюється з різних клієнтських пристроїв через інтерфейс тонкого клієнта, наприклад, веб-браузер (наприклад,веб-поштова програма), або через програмний інтерфейс. Споживач не керує і не контролює хмарною інфраструктурою, включаючи мережу, сервери, операційні системи, сховища або навіть окремими можливостями додатків, за можливим винятком обмежених налаштувань конфігурації додатків для конкретного користувача [12].

Приклади: Google Workspace, Microsoft 365, Salesforce.

**Рекомендації щодо контролю доступу до SaaS**

Що стосується багатоквартирних будинків, авторизація може здійснюватися за допомогою централізованої, децентралізованої або гібридна системи авторизації. У централізованій системі авторизації постачальник SaaS управляє централізованою базою даних авторизації для кожного кінцевого користувача та його облікових записів. У децентралізованій або гібридній системі авторизації окремі орендарі відповідають за весь або частину процесу авторизації. Зауважимо, що різним орендарям можуть знадобитися різні системи. Врахування атрибутів або ролей орендарів має вирішальне значення при виборі найбільш підходящої системи. Атрибути або ролі повинні бути добре розроблені та враховувати ієрархічні відносини при впровадженні політики управління активами для різних орендарів.

**Рекомендації щодо забезпечення конфіденційності**

У моделі розгортання додатків цілісність конфіденційних даних, що знаходяться в домені власника даних, повинна бути захищена. Механізми захисту даних додатків включають дані схеми шифрування, за допомогою яких дані можуть бути зашифровані за допомогою певних криптографічних примітивів, і ключі дешифрування будуть доступні лише авторизованим користувачам [13]. Для такого контролю можливо використовувати схеми контролю доступу на основі атрибутів (ABAC) та шифрування на основі атрибутів (ABE), які дозволяють контроль доступу до даних SaaS [14], оскільки ці схеми можуть використовувати ідентифікаційні дані користувачів через атрибути для управління, шифрування та розшифрування даних додатків. Однак, враховуючи великий обсяг даних у моделі SaaS, шифрування та дешифрування значно знижують продуктивність. Тому, коли використовується шифрування, слід звернути увагу на те, щоб забезпечити конфіденційність даних, пропонуючи при цьому хорошу продуктивність.

**Рекомендації щодо управління атрибутами та ролями**

У системі SaaS управління доступом на основі атрибутів і ролей використовує політики і заздалегідь визначені ролі для управління правами доступу до додатків і баз даних. Основна проблема розгортання управління доступом на основі атрибутів або ролей є досягнення згоди щодо того, які типи атрибутів або ролей слід використовувати і що слід враховувати при проектуванні систем управління доступом. Якщо набір розглянутих атрибутів або ролей занадто малий, гнучкість буде знижена. Однак якщо кількість атрибутів або ролей занадто велика, складність політик зросте.

**Умови використання**

Програмне забезпечення як послуга є найбільш прийнятним варіантом серед IaaS vs PaaS vs SaaS у таких випадках:

- Ви стартап, якому потрібно швидко запустити проект. У вас мало часу на вирішення проблем із сервером.
- Час від часу ви використовуватимете додаток, як програмне забезпечення для оподаткування.
- Ви працюєте над короткостроковим проектом, який вимагає швидкої співпраці.
- Вашому додатку потрібен доступ як для комп’ютера, так і для мобільного пристрою.

**Доставка SaaS**

Провайдери надають рішення SaaS кінцевим користувачам через Інтернет. Як правило, ви можете використовувати рішення SaaS як додаток або встановити його на своєму пристрої. Наприклад, ви можете використовувати Google Docs через Інтернет. Тим часом вам потрібно завантажити Adobe Creative Cloud на свій комп’ютер.

Що чудово в SaaS, так це те, що вам не потрібна допомога IT-спеціалістів для встановлення програми на кожному пристрої. Постачальники керують оновленнями програмного та апаратного забезпечення, заощаджуючи ваш час і ресурси.

**Основні переваги моделей програмного забезпечення як послуги**

- **Зниження витрат.** Що стосується технології SaaS, постачальники несуть відповідальність за вирішення потенційних технічних проблем. Вони мають справу з даними, серверами та мережами зберігання. Крім того, вони надають своїм користувачам послуг послуги з обслуговування, відповідності та безпеки. Таким чином ви зможете істотно скоротити свої витрати.

- **Економія часу.** Вам не потрібно завантажувати та встановлювати програмні продукти на окремі пристрої. В результаті технічний персонал звільняється від виснажливих завдань, пов'язаних із встановленням або оновленням програмного забезпечення.
- **Доступність.** Ви можете легко отримати доступ до програм SaaS. Все, що вам потрібно для використання такої програми, це комп'ютер або мобільний пристрій зі стабільним підключенням до Інтернету. Таким чином, продукти SaaS особливо корисні для команд, які працюють віддалено.
- **Готові рішення.** Постачальники програмного забезпечення як послуги пропонують готові продукти, які легко налаштувати та використовувати. Вам доступні як базові пакети, так і більш складні рішення.
- **Регулярне автоматичне оновлення.** Постачальники включають автоматичні оновлення в рішення SaaS. Таким чином, їхні клієнти не хвилюються щодо оновлення програмного забезпечення.
- **Резервне копіювання даних.** SaaS включає програмне забезпечення для резервного копіювання. Це спеціальна технологія, яка допомагає зберігати та захищати дані, створені за допомогою продукту SaaS [15]. Технологія включена в SaaS і доставляється через хмару. Таким чином, компанії економлять на резервному копіюванні та зберіганні своїх даних.
- **Стабільна доставка.** Постачальники SaaS дбають про найкращий досвід роботи своїх клієнтів із продуктами. Таким чином, вони максимально забезпечують стабільну роботу своїх SaaS-рішень. Це означає, що ваш бізнес працює з мінімальними простоями.
- **Сприятливий для планування бізнесу.** Провайдери SaaS піклуються про складні обчислювальні операції та щоденну діяльність своїх користувачів. Ви передаєте встановлення, оновлення та обслуговування програмного забезпечення постачальнику SaaS. Отже, ви зосереджені на веденні та розвитку свого бізнесу.
- **Проба перед покупкою.** Провайдери SaaS є широко поширеною практикою пропонувати клієнтам пробний період. Таким чином, ви можете перевірити, як додаток працює для вашої компанії, перш ніж інвестувати у впровадження системи.

**Недоліки моделі SaaS**

Ми обговорили основні переваги хмарного сервісу SaaS. Тепер давайте подивимося на недоліки цього варіанту:

- **Проблеми з продуктивністю.** Інтернет-залежні програми, що працюють у віддалених центрах обробки даних, іноді можуть демонструвати низьку продуктивність. У той же час програми, встановлені на комп'ютерах ваших співробітників, можуть працювати набагато краще. Щоб уникнути цієї проблеми, вам слід інвестувати в надійне та швидке підключення до Інтернету. Крім того, вам потрібна продуктивність програми.
- **Недостатній захист даних.** Це одна з головних причин, чому деякі компанії не хочуть переходити на хмару програмного забезпечення як послуги. Таким чином, управління доступом стає вашим пріоритетом. Подумайте про це, перш ніж довіряти свою конфіденційну інформацію сторонньому постачальнику послуг.

- **Відсутність підтримки інтеграції.** Деякі продукти SaaS потрібно інтегрувати з іншими інструментами та програмами, які використовує ваша компанія. Таким чином, ви автоматизуєте бізнес-процеси та підвищите продуктивність своїх співробітників. У зв'язку з цим постачальники програмного забезпечення як послуги можуть надати вам обмежену підтримку. У результаті вам доведеться інвестувати внутрішні ресурси для керування цими інтеграціями.
- **Проблеми під час переходу на SaaS.** Ця проблема називається блокуванням постачальника. Це означає, що користувач або компанія залежать від постачальника, щоб використовувати продукт [16]. Перехід до іншого постачальника передбачає значні витрати ресурсів і часу. Що стосується SaaS, це означає, що перехід на інше програмне хмарне рішення може бути складним. У разі переходу на інший SaaS кінцеві користувачі несуть значні витрати на зміну або потребують власної інженерної переробки.
- **Відсутність кастомізації.** Локальне програмне забезпечення постачається з різними комплектами розробки (SDK). Вони дозволяють налаштувати рішення відповідно до потреб вашого бізнесу. Тим часом SaaS має низькі можливості налаштування. Таке програмне забезпечення розроблено для задоволення найпоширеніших потреб. Таким чином, SaaS може не мати спеціальних функцій або не відповідатиме вимогам продуктивності.
- **Контроль SaaS залежить від провайдера.** Ви довіряєте контроль над рішенням SaaS провайдеру. По-перше, такий контроль передбачає оновлення функціоналу та інтерфейсу. Більш того, контроль за безпекою даних і моделями управління даними також лежить на провайдері. Така ситуація означає, що кінцевим користувачам потрібно буде адаптувати свої моделі безпеки та управління до функцій SaaS [17].
- **Періоди несправності.** Оскільки провайдер керує SaaS, ваші клієнти також залежать від його належної роботи. Технічне обслуговування та боротьба з кібератаками та збоями в мережі призводять до простою. Отже, вам і вашим клієнтам потрібно дочекатися, поки провайдер закінчить планові та позапланові роботи.

**Тенденції ринку SaaS**

З впровадженням 5G користувачі частіше використовують SaaS. Тому все більше компаній впроваджують SaaS для прискорення своїх операцій.

Багато компаній запровадили модель дистанційної роботи, щоб не відставати від ринку та підтримувати комфорт співробітників. Це спричинило попит на інструменти співпраці SaaS. Наприклад, кількість щоденних активних користувачів Microsoft Teams зросла зі 115 мільйонів у 2020 році до 145 мільйонів у 2021 році.

Аналітика є ще одним важливим компонентом ринку SaaS. Компанії цінують і використовують хмарні інструменти SaaS для аналізу своїх бізнес-процесів і даних [18]. Насправді такі рішення допомагають їм залишатися конкурентоспроможними.

Останні події на ринку SaaS пов'язані з Amazon. Спочатку компанія запустила Smart Commerce. Це рішення створює вітрини. Таким чином, це допомагає роздрібним торговцям надавати своїм покупцям досвід роботи в магазині. Крім того, Amazon Web Services співпрацює з IBM, щоб надати програмне забезпечення IBM як послугу на AWS. Програмне забезпечення включає автоматизацію, дані, ШІ та безпеку.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У середовищі SaaS проміжне програмне забезпечення розробляється (або закуповується), розгортається і використовується повністю хмарним провайдером.

У випадку з середовищем IaaS сценарій такий самий, за винятком того, що суб'єкт, який бере в ньому участь, є хмарним абонентом, а не хмарним провайдером. Заходи захисту проміжного програмного забезпечення в цих двох середовищах полягають у дотриманні найкращих практик, необхідних для будь-якого життєвого циклу розробки програмного забезпечення [19]. Однак, проміжне програмне забезпечення у випадку середовища PaaS, хоча і розробляється та розгортається хмарним провайдером, воно пропонується як додаток, що використовується абонентами. Звідси випливають наступні додаткові заходи захисту безпеки:

- всі елементи проміжного програмного забезпечення повинні бути сертифіковані незалежною третьою стороною на відсутність шкідливого програмного забезпечення.
- проміжне програмне забезпечення повинно бути розроблене таким чином, щоб воно могло приймати зв'язок тільки через зашифрований канал [20].
- архітектура рівня проміжного ПЗ повинна бути такою, щоб бути такою, щоб ймовірність уразливостей безпеки через неправильну конфігурацію компонентів проміжного програмного забезпечення була проміжного ПЗ, які надаються виключно для управління безпекою (на відміну від тих, що надаються для підтримки цілісності додатків).
- проміжне програмне забезпечення, яке надається виключно для управління безпекою (на відміну від тих, які надаються для підтримки цілісності/працездатності додатків — наприклад, проміжне програмне забезпечення, яке надає такі функції, як перевірка ідентичності, авторизація/контроль доступу, перевірка вхідних даних, реєстрація подій тощо) повинні мати максимальну довіру завдяки незалежним акредитованим перевіркам/сертифікаціям третьою стороною.

**Безпечне середовище розробки додатків**

У SaaS та IaaS інструменти, необхідні для розробки додатків, належать і використовуються однією і тією ж організацією. Тому застосовуються звичайні заходи захисту для безпечного розгортання цих інструментів. У випадку PaaS інструменти використовуються абонентом хмари. [21] Тому потрібні спеціальні заходи захисту.

Вони полягають у наступному:

- Переконатися, що інструменти розробки та бібліотечні коди (час компіляції та час виконання), які надаються провайдерами хмарних технологій PaaS, були сертифіковані як такі, що не містять шкідливого програмного забезпечення.
- Переконатися, що провайдер PaaS надає версії цих інструментів та бібліотечного коду з цифровим підписом та що всі розробники підписники хмарних послуг починають користуватися цими інструментами та бібліотеками після перевірки відповідних цифрових підписів.

Модель PaaS у хмарній системі дозволяє розробникам створювати і розгортати додатки в хмарну інфраструктуру, використовуючи мови програмування, бібліотеки, сервіси та інструменти. Розробник програмного забезпечення не керує і не контролює базову хмарну інфраструктуру, але має контроль над розгорнутими додатками (програмним забезпеченням) і, можливо, налаштуваннями конфігурації для середовища.

При аналізі відповідальності між споживачем та постачальниками хмарних послуг за захист хмарних даних, не завжди зрозуміло, чи надає система IaaS тільки обчислювальні ресурси, чи пропонує також віртуальне сховище і мережеві ресурси споживачам для розгортання та запуску довільного програмного забезпечення, в тому числі, включаючи операційні системи та додатки. Споживач, у свою чергу, може мати контроль над віртуальним сховищем, віртуалізованими мережевими компонентами та можливість розгортати власні віртуальні машини і додатки, маючи доступ, наданий хмарним провайдером.

У PaaS і SaaS необхідно враховувати спільну відповідальність за контроль доступу моделі [22]. Наприклад, розробникам програмного забезпечення може знадобитися доступ до даних у системах, наданих PaaS для потреб розвитку та внутрішніх користувачів додатків (тобто користувачів, яким потрібно доступ до системних даних програми) може знадобитися доступ до системних даних програми, тобто керується програмами.

Загалом, для PaaS розробники споживчого програмного забезпечення можуть розділити відповідальність за контроль доступу з постачальниками хмарних послуг; для SaaS, внутрішня програма користувачів може розділити такі обов'язки з постачальниками хмарних послуг.

Зауважимо, що якщо немає спеціального попереднього схвалення від споживача, постачальник PaaS або SaaS повинен керуватися контролем доступу за допомогою постачальника IaaS і споживача (якщо це також не IaaS постачальник). Якщо споживач погоджується, постачальник повинен повідомити споживача про свій намір зберігати вказані дані в постачальнику IaaS, де до них буде доступ, а також обсяг до яких даних може отримати доступ постачальник IaaS, іноземні організації або органи влади.

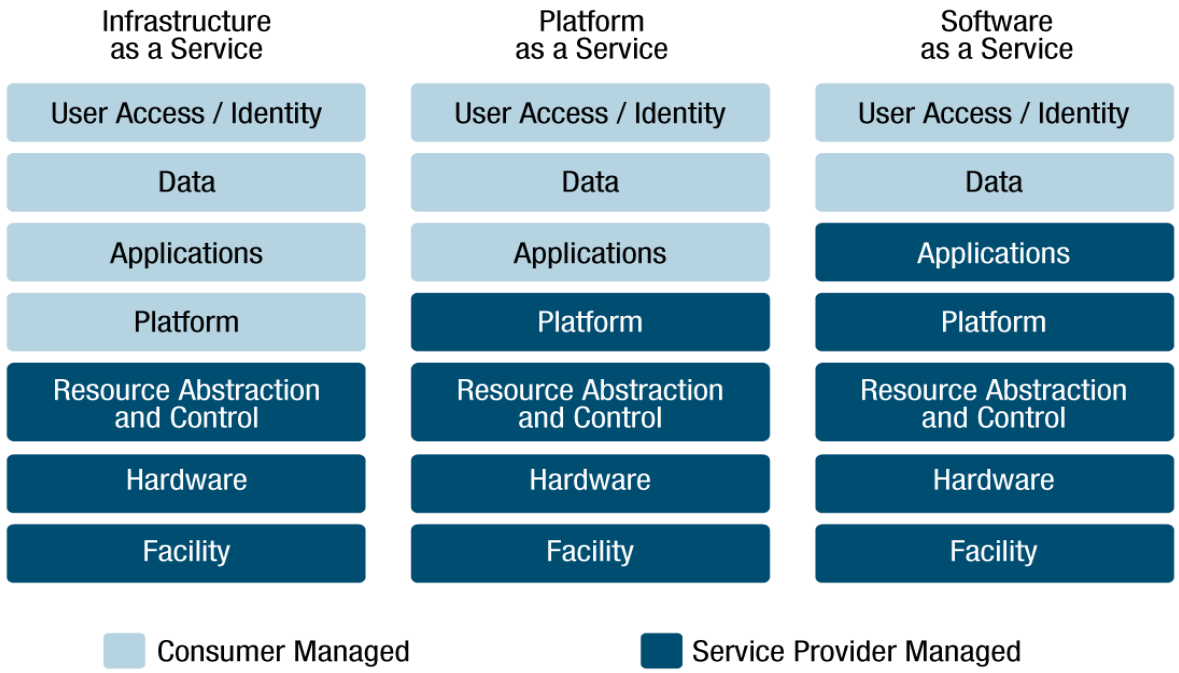


*Рис. 1. Доступи, контрольовані постачальником хмарних послуг і споживачем*

П’ять основних характеристик, які ставлять під сумнів проектування системи контролю доступу, підсумовані таким чином [22]:

1. Широкий доступ до мережі: хмарні служби доступні через мережу та доступні через стандартні механізми, які сприяють використанню різнорідними товстими та тонкими клієнтами платформи (наприклад, мобільні телефони, планшети, ноутбуки, робочі станції). Це підвищує проблеми безпеки з доступом до мережі. Наприклад, атаки на відмову в обслуговуванні (DoS) можуть запускатися проти хмарної системи, роблячи її ресурси недоступними для законних користувачів.

Таким чином, контролем доступу для доступу до мережі слід керувати.

2. Об’єднання ресурсів: обчислювальні ресурси хмарної системи (наприклад, сховище, пам’ять, обробка, пропускна здатність мережі) об’єднуються для обслуговування кількох споживачів за допомогою мультитенантної моделі (тобто один екземпляр програмного забезпечення та його допоміжна інфраструктура обслуговує кілька споживачів) через різні фізичні та віртуальні ресурси, кожен динамічно призначаються та перепризначаються відповідно до вимог споживачів. Може статися витік інформації, якщо до ресурсу, виділеного споживачу, може отримати доступ інший суміжний споживач або якщо виділений ресурс, наприклад пам’ять, не стирається, перш ніж його буде перерозподілено іншому споживач. Існує також відчуття незалежності від місця розташування споживача в цілому не контролює та не знає точного розташування наданих ресурсів. Місцезнаходження може бути визначено на вищому рівні абстракції (наприклад, країна, штат, центр обробки даних), що приносить проблеми безпеки. Таким чином, методи реалізації об’єднання ресурсів під час забезпечення ізоляція спільних ресурсів повинна бути розглянута в проекті контролю доступу.

3. Швидка еластичність: хмарні сервіси можливо еластично надавати та випускати — автоматично, у деяких випадках — для швидкого розширення назовні та всередину відповідно до вимог. До споживача послуги, що доступні для надання, часто здаються необмеженими привласнюються в будь-якій кількості в будь-який час і підтримуються додаванням нових віртуальних машин (VM) із зазначеними обчислювальними ресурсами. Завдання для проектування контролю доступу включає в себе здатність швидко перевіряти безпеку нових віртуальних машин і визначати, чи нещодавно додані віртуальні машини кваліфіковані для виконання конкретного завдання.

4. Вимірюваний сервіс: хмарні системи автоматично контролюють і оптимізують використання ресурсів. Використання можливості вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність, активні облікові записи кінцевих користувачів). Використання ресурсів відстежується, контролюється та звітується для забезпечення прозорості як для постачальника, так і для споживача використаної послуги. Щоб підтримувати використання ресурсів, хмарні споживачі мають право переглядати, але не змінювати власні дані вимірювання, оскільки це може призвести до фальсифікація платежів, необхідних за хмарні послуги. Таким чином, це розумно для контролю доступу розглянути захист даних вимірювання.

5. Обмін даними: Обмін інформацією між різними організаціями не є тривіальним завданням, оскільки хмарна система повинна відповідати однаковим вимогам безпеки організацій, щоб досягти цього. Для полегшення обміну даними необхідно враховувати такі концепції, як довіра до об’єднаних ідентичностей і атрибутів контролю доступу, і створення такої довіри має першорядне значення.

Незалежно від моделі надання послуг споживачі мають право нести відповідальність за безпеку своїх хмарних даних і за те, хто має до них доступ [23] – [32]. З цієї причини дані ніколи не контролюються постачальниками хмарних сервісів, а

завжди залишаються у споживачів хмарних послуг. (Винятком є дані журналів, але все одно слід враховувати, як такі дані впливають на конфіденційність і безпеку).

Хоча постачальник хмарних послуг може стати зберігачем даних споживачів, він не повинен мати доступу до них. Якщо дані споживача не зашифровані, то адміністратори хмарних сервісів можуть їх прочитати. У такому випадку дані споживача повинні бути ідентифіковані (за привілеями доступу провайдера до даних) та позначені червоним прапорцем як такі, що доступні постачальнику послуг, а споживач має бути негайно проінформований про це.

Хмарна віртуалізація додає додатковий тягар управлінню безпекою, вводячи засоби контролю безпеки які виникають при об'єднанні декількох віртуальних машин на одному фізичному комп'ютері, що може мати потенційний негативний вплив, якщо відбудеться компрометація безпеки. Деякі хмарні системи дозволяють легко обмінюватися інформацією між віртуальними машинами, наприклад, дозволяючи користувачам створювати кілька віртуальних машин на одному гіпервізорі, якщо доступно декілька ВМ. Однак ця зручність може також стати вектором атаки, оскільки між віртуальними машинами може статися витік даних. Крім того, віртуалізовані середовища є швидкоплинними, оскільки вони часто створюються і зникають, що ускладнює створення та підтримку необхідних меж безпеки.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі представляється підхід до розуміння проблем контролю доступу в хмарних системах шляхом аналізу аспектів контролю доступу у всіх трьох моделях надання хмарних послуг IaaS, PaaS та SaaS. Також узагальнено такі характеристики, як широкий доступ до мережі, об'єднання ресурсів, швидка еластичність, вимірювання сервісів та обмін даними. Запропоновано рекомендації щодо проектування контролю доступу для IaaS, PaaS і SaaS відповідно до їхніх різних характеристик. Крім того, потенційні правила політики узагальнені для кожної хмарної системи.

Запропоновано технології захисту безпеки на кожному з 3 основних рівнів хмарних сервісів: рівні додатків, проміжного програмного забезпечення та віртуальних машин, через відмінності в організації, яка контролює кожен з цих рівнів. Виявлено, що для будь-якого рівня можливо забезпечити більш ефективний захист, якщо той самий суб'єкт контролює рівень, що знаходиться нижче. Оскільки мережевий, апаратний та рівень абстракції ресурсів у всіх моделях хмарних сервісів контролюються хмарним провайдером, він має в своєму розпорядженні більш ефективні засоби захисту.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nogueira, M., Sun, X., & De Sousa, R. T. (2019). Cybersecurity in Cloud Computing: Threats and Solutions. *IEEE Communications Surveys & Tutorials, 21(1).*
2. Kshetri, N. (2019). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Journal of Business Research, 92.*
3. ISACA. (2022). *State of cybersecurity 2022: cyber workforce challenges.*
4. Verizon. (2023). 2023 *Data Breach Investigations Report.*
5. Bleeping Computer. (2022). *MFA fatigue: hackers 'new favorite tactic in high-profile breaches.*
6. Integrity Systems. (n.d.) *Хмарні обчислення.* http://integritysys.com.ua/solutions/pricatecloud-solution
7. Wikipedia. (n.d.). *Безпека як послуга.* https://uk.wikipedia.org/wiki/Безпека_як_послуга
8. Microsoft Azure. (n.d.). *What is IaaS? Infrastructure as a Service.* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas

9. Петров, К. Е., & Захарченко Д. О. (2022). Дослідження та використання хмарних технологій в процесі проектування ІТ-інфраструктури організаційних систем. *In Scientific Collection «InterConf», (116): with the Proceedings of the 12th International Scientific and Practical Conference «Scientific Research in XXI Century»*, 410−413.
10. Deloitte. (2021). *The cloud imperative Asia Pacific's unmissable opportunity*. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/technology/sg-techcloud-imperative-executive-summary.pdf
11. NIST (National Institute of Standards and Technology). (2020). Security and Privacy Controlsfor Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
12. Abid, A., Manzoor, M.F., Farooq, M.S., Farooq, U., & Hussain, M. (2020). Challenges and issues of resource. allocation techniques in cloud computing. *KSII Transactions on Internet and Information Systems (TIIS), 14(7),* 2815–2839.
13. Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using Technology-organization-environment framework. *Internet of Things, 15, 100407.*
14. Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics, 35(1),* 38–54.
15. Tverdokhlib, A. O., & Korotin, D. S. (2022). Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz dannykh. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, (6).*
16. Tsvyk, O. S. (2023). Analiz i osoblyvosti prohramnoho zabezpechennia dlia kontroliu trafiku. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ceriia: Tekhnichni nauky, (1).*
17. Лемешко, А. В., Антоненко, А. В., Балвак, А. А., & Новіченко, Є. О. (2023). Актуальні засади створення алгоритмів обробки інформації для логістичних центрів. *Таврійський науковий вісник. Серія: Технічні науки, (1),* 25–32. https://doi.org/10.32851/tnv-tech.2023.1.3
18. Attaran, M., & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship, 31(6),* 495–519.
19. Contributors to Wikimedia projects. (2007). *Cloud computing - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Cloud_computing#Service_models
20. Marko, K., & Bigelow, S. J. (2022). *The pros and cons of cloud computing explained*. TechTarget.
21. Ryan, M. D. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM, 54(1),* 36–38. https://doi.org/10.1145/1866739.1866751
22. Kanaker, H., et al. (2022). Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies, 16(24*), 81–106. https://doi.org/10.3991/ijim.v16i24.35763
23. Gartner. (2022). *Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025*. https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending
24. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., & Smirnov, O. (2023). The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning. *Advanced Information Systems, 7(2),* 49–56. https://doi.org/10.20998/2522-9052.2023.2.07
25. Smirnov, O., Alimseitova, Zh., Adranova, A., Akhmetov, B., Lakhno, V., & Zhilkishbayeva, G. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of theoretical and applied information technology, 98(21),* 3334–3346.
26. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., & Aleksander, M. (2020). Method of fractal traffic generation by a model of generator on the graph. *2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks, 2616,* 366–379.
27. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., & Kundyz, M. (2019). QoE optimization technique for media delivery in 5G networks. *IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology,* 597–601. https://doi.org/10.1109/PICST47496.2019.9061469
28. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., & Hryhorenko, V. (2019). Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids. *IEEE 6th International Conference On Energy Smart Systems,* 353–358. https://doi.org/10.1109/ESS.2019.8764195
29. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., & Kuznetsova, K. (2019). Malware Correlation Monitoring in Computer Networks of Promising Smart Grids. *IEEE 6th International Conference On Energy Smart Systems,* 347–352. https://doi.org/10.1109/ESS.2019.8764228

30. Smirnov, A. A., Kuznetsov, A. A., Danilenko, D. A., & Berezovsky, A. (2015). The statistical analysis of a network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering, 74(1),* 61–78. https://doi.org/10.1615/TelecomRadEng.v74.i1.60
31. Смірнов, О. А., Смірнова, Т. В., Буравченко, К. О., Кравченко, С. С., & Горбов, В.О. (2021). Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин. *Сучасні інформаційні системи, 5(4),* 79–95. https://doi.org/10.20998/2522-9052.2021.4.12
32. Смірнов, О. А., Смірнова, Т. В., Поліщук, Л. І., Буравченко, К. О., & Макевнін, А. О. (2020). Дослідження хмарних технологій як сервісів, *Кібербезпека: освіта, наука, техніка, 3(7),* 43–62. https://doi.org/10.28925/2663-4023.2020.7.4362

**Tetiana Smirnova**
PhD, Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-6896-0612
*sm.tetyana.gmail.com*

**Oksana Konoplitska-Slobodeniuk**
Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9981-5194
*ksuha80@gmail.com*

**Kostiantyn Buravchenko**
PhD, Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-6195-7533
*buravchenkok@gmail.com*

**Serhii Smirnov**
PhD, Associate Professor, Associate Professor of Cybersecurity &
Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-7649-7442
*smirnov.ser.81@gmail.com*

**Oksana Kravchuk**
HR department inspector
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0009-0008-8453-0557
*vov-14@i.ua*

**Nataliia Kozirova**
Assistant of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0009-0005-8753-5132
*natalidonchenko23@gmail.com*

**Oleksii Smirnov**
Doctor of Sciences, professor, head of
Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9543-874X
*dr.smirnovoa@gmail.com*

# RESEARCH OF CYBER SECURITY TECHNOLOGIES OF CLOUD SERVICES IAAS, PAAS AND SAAS

**Abstract.** Cybersecurity threats are constantly evolving, and cloud computing is no exception. Attackers are improving attack techniques aimed at identifying vulnerabilities in IaaS, PaaS, and SaaS. The work examines the following problematic issues: insufficient analytical tools; data privacy and security; financial and organizational costs to ensure cyber security of IaaS, PaaS and SaaS cloud technologies. The aim of the work is to investigate how the common models of cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) need to properly implement adequate and appropriate protection measures to ensure cyber security. For this purpose, the paper examined models of cloud technologies, it was determined that cloud services include various models that allow users to access various types of resources via the Internet. It has been found that there are three generally accepted models of cloud services: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), and two main players: the cloud provider and the cloud subscriber. The set of levels over which each of these players has control depends on the model of the

cloud service or environment. For each of these cloud services, its description was given, recommendations were given for access control, privacy assurance, terms of use were defined, advantages and disadvantages were given, and market trends of these services were considered. Proposed approaches to the formation of a secure application development environment in cloud services. Features such as wide network access, resource pooling, fast elasticity, service metering, and data sharing are also summarized. Guidelines for designing access control for IaaS, PaaS, and SaaS according to their different characteristics are proposed. In addition, the security policy rules for each cloud system are summarized. Technologies are proposed to protect security at each of the three main layers of cloud services: the application, middleware, and virtual machine layers, due to differences in the organization that controls each of these layers. It was found that for any level it is possible to provide more effective protection if the same subject controls the level below. Since the network, hardware, and resource abstraction layer in all cloud service models are controlled by the cloud provider, it has more effective protections at its disposal.

**Keywords:** cyber security; access control; privacy; computer science; cloud services; telecommunication system; IaaS; PaaS; SaaS.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Nogueira, M., Sun, X., & De Sousa, R. T. (2019). Cybersecurity in Cloud Computing: Threats and Solutions. *IEEE Communications Surveys & Tutorials, 21(1).*
2. Kshetri, N. (2019). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Journal of Business Research, 92.*
3. ISACA. (2022). *State of cybersecurity 2022: cyber workforce challenges.*
4. Verizon. (2023). 2023 *Data Breach Investigations Report.*
5. Bleeping Computer. (2022). *MFA fatigue: hackers 'new favorite tactic in high-profile breaches.*
6. Integrity Systems. (n.d.). *Cloud computing.* http://integritysys.com.ua/solutions/pricatecloud-solution
7. Wikipedia. (n.d.). *Security as a service.* https://uk.wikipedia.org/wiki/Безпека_як_послуга
8. Microsoft Azure. (n.d.). *What is IaaS? Infrastructure as a Service.* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas
9. Petrov, K. E., & Zakharchenko, D. O. (2022). Research and use of cloud technologies in the process of designing the IT infrastructure of organizational systems. *In Scientific Collection "InterConf", (116): with the Proceedings of the 12th International Scientific and Practical Conference "Scientific Research in XXI Century"*, 410−413.
10. Deloitte. (2021). *The cloud imperative Asia Pacific's unmissable opportunity*. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/technology/sg-techcloud-imperative-executive-summary.pdf
11. NIST (National Institute of Standards and Technology). (2020). Security and Privacy Controlsfor Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
12. Abid, A., Manzoor, M.F., Farooq, M.S., Farooq, U., & Hussain, M. (2020). Challenges and issues of resource. allocation techniques in cloud computing. *KSII Transactions on Internet and Information Systems (TIIS), 14(7),* 2815–2839.
13. Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using Technology-organization-environment framework. *Internet of Things, 15, 100407.*
14. Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics, 35(1),* 38–54.
15. Tverdokhlib, A. O., & Korotin, D. S. (2022). Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz dannykh. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, (6).*
16. Tsvyk, O. S. (2023). Analiz i osoblyvosti prohramnoho zabezpechennia dlia kontroliu trafiku. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ceriia: Tekhnichni nauky, (1).*
17. Lemeshko, A. V., Antonenko, A. V., Balvak, A. A., & Novichenko, Ye. O. (2023). Current principles of creating information processing algorithms for logistics centers. *Taurida Scientific Herald. Series: Technical Sciences, (1),* 25–32. https://doi.org/10.32851/tnv-tech.2023.1.3

18. Attaran, M., & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship, 31(6),* 495–519.
19. Contributors to Wikimedia projects. (2007). *Cloud computing - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Cloud_computing#Service_models
20. Marko, K., & Bigelow, S. J. (2022). *The pros and cons of cloud computing explained*. TechTarget.
21. Ryan, M. D. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM, 54(1),* 36–38. https://doi.org/10.1145/1866739.1866751
22. Kanaker, H., et al. (2022). Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies, 16(24*), 81–106. https://doi.org/10.3991/ijim.v16i24.35763
23. Gartner. (2022). *Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025*. https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending
24. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., & Smirnov, O. (2023). The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning. *Advanced Information Systems, 7(2),* 49–56. https://doi.org/10.20998/2522-9052.2023.2.07
25. Smirnov, O., Alimseitova, Zh., Adranova, A., Akhmetov, B., Lakhno, V., & Zhilkishbayeva, G. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of theoretical and applied information technology, 98(21),* 3334–3346.
26. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., & Aleksander, M. (2020). Method of fractal traffic generation by a model of generator on the graph. *2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks, 2616,* 366–379.
27. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., & Kundyz, M. (2019). QoE optimization technique for media delivery in 5G networks. *IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology,* 597–601. https://doi.org/10.1109/PICST47496.2019.9061469
28. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., & Hryhorenko, V. (2019). Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids. *IEEE 6th International Conference On Energy Smart Systems,* 353–358. https://doi.org/10.1109/ESS.2019.8764195
29. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., & Kuznetsova, K. (2019). Malware Correlation Monitoring in Computer Networks of Promising Smart Grids. *IEEE 6th International Conference On Energy Smart Systems,* 347–352. https://doi.org/10.1109/ESS.2019.8764228
30. Smirnov, A. A., Kuznetsov, A. A., Danilenko, D. A., & Berezovsky, A. (2015). The statistical analysis of a network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering, 74(1),* 61–78. https://doi.org/10.1615/TelecomRadEng.v74.i1.60
31. Smirnov, O. A., Smirnova, T. V., Buravchenko, K. O., Kravchenko, S. S., & Gorbov, V.O. (2021). A cloud-based decision support system for the technological process of restoring the surfaces of structures and machine parts. Modern information systems, 5(4), 79–95. https://doi.org/10.20998/2522-9052.2021.4.12
32. Smirnov, O. A., Smirnova, T. V., Polishchuk, L. I., Buravchenko, K. O., Makevnin, A. O. (2020). Research of cloud technologies as services. *Cybersecurity: education, science, technology, 3(7),* 43–62. https://doi.org/10.28925/2663-4023.2020.7.4362