КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.857
УДК 004. 004.056.5:004.415.5:004.7

**Костюк Юлія Володимирівна**
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0001-5423-0985
*y.kostiuk@kubg.edu.ua*

**Хорольська Карина Вікторівна**
PhD in Computer Science
доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0003-3270-4494
*karynakhorolska@gmail.com*

**Бебешко Богдан Тарасович**
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0001-6599-0808
*b.bebeshko@kubg.edu.ua*

**Довженко Надія Михайлівна**
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ,
ORCIDID:0000-0003-4164-0066
*nadezhdadovzhenko@gmail.com*

**Коршун Наталія Володимирівна**
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
ORCID ID: 0000-0003-2908-970X
*n.korshun@kubg.edu.ua*

**Пазинін Андрій Сергійович**
аспірант
Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ
ORCID 0009-0002-9506-9539
*Pazinin@gmail.com*

# ІНСТРУМЕНТАЛЬНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІД ПРИХОВАНИХ ЗАГРОЗ В ІНФРАСТРУКТУРІ ХМАРНИХ ОБЧИСЛЕНЬ

**Анотація**. У хмарних обчисленнях дедалі частіше виникає проблема протидії прихованим загрозам інформаційної безпеки, що обумовлено високою динамічністю управління ресурсами, складністю верифікації міжпроцесної взаємодії та використанням віртуалізованих середовищ. Особлива увага приділяється загрозам, які реалізуються на рівні гіпервізора або внаслідок неконтрольованих транзакцій між гостьовими операційними системами та керуючими підсистемами хмари, що унеможливлює їх виявлення традиційними засобами моніторингу. У відповідь на ці виклики запропоновано інструментальний підхід, який реалізує механізми виявлення та нейтралізації латентних атак шляхом безперервного контролю над запитами до системних ресурсів та оцінки поведінкових моделей взаємодії компонентів. У межах дослідження розроблено формалізовану модель інформаційної взаємодії, що відображає логіку послідовних і паралельних операцій, які ініціюються віртуальними машинами в процесі доступу до

обчислювальних, мережевих та сховищних ресурсів. Така модель дозволяє не лише структурувати динамічні інформаційні потоки, а й формалізувати критичні залежності між транзакціями, що можуть бути використані як вектори прихованих атак. Застосовано метод предикативної ідентифікації загроз, що враховує контекст виконання системних викликів, включаючи ознаки аномальної активності та невідповідності діючій політиці безпеки. Отримані результати свідчать про практичну доцільність використання формалізованих моделей транзакційної взаємодії та предикативного аналізу для підвищення рівня захищеності хмарних сервісів від складновиявлюваних, зокрема — прихованих, загроз інформаційної безпеки, що особливо актуально в контексті розширення застосування технологій контейнеризації, оркестрації та розподілених обчислень, зокрема у середовищах AWS, Azure, Google Cloud Platform та Kubernetes.

**Ключові слова:** інформаційна безпека; хмарні обчислення; приховані загрози; гіпервізор; віртуалізація; інструментальні засоби; динамічне середовище; політика безпеки; моніторинг; хмарні сервіси; хмарно-орієнтовані архітектури.

## ВСТУП

Широке впровадження хмарних обчислень у корпоративні та державні інформаційні системи супроводжується суттєвими ризиками, пов’язаними з новими типами кіберзагроз. Особливої небезпеки набувають приховані загрози, які залишаються непомітними для гостьових операційних систем, але реалізуються через системні виклики до гіпервізора або неконтрольовані транзакції розподілу ресурсів [1], [2]. Такий тип загроз є викликом для традиційних засобів захисту, оскільки вони не передбачають глибокого аналізу внутрішніх процесів віртуалізації у хмарному середовищі, де ресурси постійно змінюються відповідно до вимог сервісу [3], [4]. З огляду на це, актуальним є розроблення нових інструментальних засобів захисту, що враховують архітектуру гіпервізора, динамічне виділення ресурсів та контекст виконання транзакцій [5-6]. У роботі під віртуалізацією розглядається саме віртуалізація у хмарному середовищі, що функціонує з використанням гіпервізорів, контейнеризації та мікросервісів.

Особливості хмарних обчислень, зокрема багатокористувацький доступ (наприклад, у сервісах Amazon EC2, Google Cloud Compute Engine, Azure Virtual Machines), автоматичне масштабування, використання ізольованих середовищ (віртуальних машин і контейнерів), створюють додаткові вектори атак, які можуть бути використані як зовнішніми, так і внутрішніми порушниками [8]. У хмарній інфраструктурі компоненти постійно взаємодіють через API, оркестратори та служби балансування навантаження, що ускладнює простежування повного ланцюга подій, пов’язаних із потенційною загрозою [10]. Особливістю хмарних обчислень є постійна зміна стану ресурсів, що реалізуються через автоматизовані процеси оркестрації та масштабування, які ускладнюють застосування класичних засобів захисту. Динамічна природа хмарних середовищ передбачає часті зміни у конфігурації віртуальних ресурсів, що створює умови для реалізації латентних атак у моменти оновлення, міграції або масштабування [4], [12]. Крім того, орендовані обчислювальні потужності часто поділяються між незалежними клієнтами (multi-tenancy), що підвищує ризик міжвіртуальних атак за умови недосконалого розмежування доступу. Стандарти безпеки для хмарних обчислень, зокрема ISO/IEC 27017 і NIST SP 800-207 (Zero Trust Architecture), акцентують на необхідності постійного моніторингу міжкомпонентної взаємодії, що неможливо реалізувати без спеціалізованих інструментальних засобів. У цьому контексті виникає потреба у формалізованих методах аналізу транзакцій, які

дозволяють відстежувати, верифікувати та блокувати аномальну активність у режимі реального часу на рівні гіпервізора та системних викликів.

**Постановка проблеми.** Інфраструктура хмарних обчислень характеризується високим рівнем віртуалізації, що, з одного боку, забезпечує гнучкість і масштабованість сервісів, а з іншого — створює додаткові вектори атак [5], [18]. Більшість прихованих загроз реалізуються на рівні взаємодії гостьових ОС з гіпервізором, де спостерігається складність у відстеженні транзакцій, що стосуються виділення ресурсів [4], [11]. Традиційні засоби інформаційної безпеки не адаптовані до аналізу таких взаємодій у динамічному контексті [2], [15]. Це зумовлює потребу у створенні нових моделей і алгоритмів, здатних формалізувати потоки інформації та виявляти небажані впливи, які можуть призвести до модифікації коду, підміни суб'єктів доступу або порушення цілісності системних сервісів [6], [9], [13], [17]. Таким чином, проблема полягає у відсутності ефективних інструментальних засобів виявлення й блокування прихованих загроз у середовищах з високим рівнем віртуалізації та хмарних обчисленнях.

**Аналіз останніх досліджень і публікацій.** Аналіз наукових джерел із проблематики виявлення та нейтралізації прихованих загроз в інфраструктурі хмарних обчислень свідчить про зростаючу увагу дослідників до інструментальних засобів безпеки, здатних функціонувати на рівні гіпервізора та гостьових операційних систем. Особливу актуальність становлять латентні атаки, що маскуються під легітимну активність і не виявляються традиційними методами контролю. У цьому контексті ефективність систем кіберзахисту значною мірою залежить від здатності здійснювати контекстний аналіз транзакцій доступу до ресурсів у динамічному хмарному середовищі.

Одним із перших напрямів досліджень є виявлення прихованих аномалій у поведінці гостьових віртуальних машин через моніторинг системних викликів. У роботі Aldribi et al. [1] запропоновано метод інтелектуального виявлення загроз (IDS), який функціонує на рівні гіпервізора, застосовуючи багатовимірний аналіз змін характеристик роботи ВМ у реальному часі. Результати показали високу ефективність у виявленні невідомих атак без значного навантаження на систему.

Водночас Althobaiti [2] вивчав захист Virtual Machine Monitor (VMM) від атак, пов'язаних із міжвіртуальним витоком даних, і запропонував багаторівневу архітектуру з використанням віртуальних TPM-модулів і віртуалізованих міжмережевих екранів. Дослідник наголошує на необхідності вбудованого контролю доступу до гіпервізора як інструментального засобу захисту від атак типу VM escape. Зі свого боку, Korkin (2015) акцентує увагу на проблемі stealth-гіпервізорів, які маскують свою присутність, і пропонує механізми їх виявлення через моніторинг таймерів і стану оперативної пам'яті.

Іншим перспективним напрямом є застосування алгоритмів глибокого навчання для формування поведінкових моделей доступу до ресурсів. He & Lee [3] у своїй роботі представили систему CloudShield, яка здійснює детекцію аномалій у хмарних обчисленнях на основі аналізу системних метрик. Система досягає точності понад 99 % у виявленні критичних загроз, включаючи атаки типу Spectre та Meltdown, при низькому рівні хибнопозитивних спрацювань. Це підтверджує доцільність інтеграції методів глибокого навчання в інструментальні засоби реального часу.

Додатково варто відзначити підхід Jindal et al. [4], які запропонували метод непрямої індикації загроз (IAD) у віртуалізованих середовищах через аналіз параметрів навантаження на ресурси гостьових ОС. Їхній підхід дозволяє виявляти аномалії у поведінці віртуальних машин із точністю понад 83 %, що свідчить про ефективність непрямих метрик як альтернативи прямому аналізу вмісту трафіку чи коду.

Огляд літератури Zakiyyah et al. [5] систематизує підходи до побудови адаптивних засобів захисту з використанням штучного інтелекту та машинного навчання. Автори акцентують увагу на важливості автоматизованої реакції, інтелектуального аналізу ризиків і гнучкої інтеграції захисних механізмів у масштабовані хмарні архітектури. Застосування таких рішень дозволяє реалізувати концепцію Zero Trust у хмарному середовищі, з мінімізацією довіри до будь-яких компонентів системи. Окремий напрям досліджень присвячено захисту хмарно-орієнтованих інфраструктур, які будуються на основі мікросервісної архітектури, контейнеризації та оркестрації (наприклад, Kubernetes). Особливістю таких середовищ є постійна зміна стану компонентів, динамічне масштабування, автоматичне оновлення, що значно ускладнює виявлення прихованих загроз. У роботах підкреслюється важливість адаптивного моніторингу, який враховує саме хмарно-орієнтованих специфіку взаємодії між сервісами в розподіленій хмарній платформі.

Окремий клас досліджень, представлений Enoch et al. [6], стосується використання графових моделей атак для моделювання загроз в інфраструктурі хмарних обчислень. Автори пропонують поєднання класичних дерев атак, графів залежностей і гібридних структур (HARM) для побудови механізмів виявлення складнокомпонентних загроз із використанням контекстної інформації. Ці моделі є основою для побудови інструментальних засобів із можливістю адаптивного реагування на зміну загрозового профілю середовища.

Таким чином, аналіз останніх досліджень свідчить про наявність широкого спектру інструментальних підходів до забезпечення інформаційної безпеки в хмарних обчисленнях. Найбільш перспективними є поєднання контекстно-орієнтованого моніторингу, глибинного навчання, графових моделей та предикативного аналізу транзакцій. Вони дозволяють ефективно виявляти та блокувати приховані загрози, підвищуючи стійкість хмарної інфраструктури до складних кібернетичних впливів і знижуючи ризик порушення конфіденційності, цілісності та доступності ресурсів. З огляду на складність трасування транзакцій у середовищах Kubernetes, AWS, Azure та GCP, такі інструменти особливо важливі для забезпечення цілісності даних у динамічних хмарних платформах.

**Мета статті.** Метою статті є розробка інструментального підходу до виявлення та нейтралізації прихованих загроз інформаційної безпеки в інфраструктурі хмарних обчислень шляхом формалізації транзакційної взаємодії, аналізу поведінкових моделей компонентів системи та впровадження адаптивних засобів моніторингу на рівні гіпервізора і гостьових операційних систем. Запропонована концепція забезпечує контекстно-орієнтований контроль інформаційних потоків у динамічному середовищі віртуалізації, враховуючи багатокористувацький доступ, розподіл ресурсів та гнучку архітектуру хмарних платформ. Основою є формалізована модель транзакцій, яка дозволяє виявляти латентні атаки через аналіз поведінкових відхилень системних процесів. Використано методи предикативного аналізу, декомпозиції викликів і оцінки відповідності транзакцій політикам безпеки. Результат реалізовано у вигляді програмного засобу моніторингу, здатного фіксувати загрози, недоступні традиційним засобам захисту. Модель адаптована до масштабування на платформах Kubernetes, Azure Functions, AWS Lambda, Google Cloud Run та OpenShift. Це підвищує ефективність кіберзахисту хмарної інфраструктури, знижує ризики компрометації та посилює довіру до хмарних сервісів у критичних середовищах.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні хмарні обчислення є ключовою технологією цифрової трансформації, що широко застосовується в державному, корпоративному та науковому секторах. Разом із перевагами масштабованості, доступності та автоматизації, хмарні платформи створюють новий клас загроз інформаційної безпеки, які мають латентний або прихований характер. Особливу небезпеку становлять атаки, що здійснюються за допомогою обфускованих або недекларованих можливостей програмного забезпечення, і залишаються невидимими для традиційних засобів виявлення [14], [16]. У цьому контексті зростає значення інструментальних засобів, здатних забезпечувати глибокий контекстно-орієнтований аналіз транзакцій, поведінки системних процесів і взаємодії компонентів у хмарному середовищі.

Сучасні дослідження свідчать про ефективність побудови систем виявлення прихованих загроз на основі аналізу поведінкових моделей гостьових віртуальних машин і системних викликів у середовищах з підтримкою гіпервізора [1] – [5]. Зокрема, атаки типу VM escape, privilege escalation, lateral movement та living-off-the-land базуються на використанні легітимних інтерфейсів і обхід традиційних засобів захисту, таких як антивірусне ПЗ або сигнатурні IDS [15], [20]. Приховані загрози маскуються під штатні процеси віртуальних середовищ, що функціонують у межах IaaS-, PaaS- або контейнеризованої архітектури (наприклад, Kubernetes), та реалізуються через підміни команд, ін’єкції в API або зміни у поведінці сервісів доступу до сховищ.

Інструментальні обмеження класичних засобів виявлення вторгнень пов’язані з відсутністю доступу до телеметрії з гіпервізора, обмеженістю трасування eBPF-подій та неврахуванням специфіки взаємодії між ізольованими мікросервісами. Дослідження також вказують на обмеження платформ SIEM/SOAR без підтримки потокової обробки метаданих і графового представлення залежностей між транзакціями, що унеможливлює своєчасне виявлення багатокрокових прихованих атак [15]. Запропоновані засоби враховують специфіку хмарної інфраструктури, де ресурси розподілені між кількома хостами, часто змінюються та управляються за допомогою хмарних оркестраторів, що ускладнює традиційні методи моніторингу.

Особливої актуальності набуває виявлення внутрішніх загроз (insider threats), реалізованих з боку скомпрометованих контейнерів, внутрішніх API, хмарних функцій (Function-as-a-Service) або неправомірного доступу до системи з уже отриманими привілеями [14], [16], [20]. Такі загрози зазвичай обходять perimeter-based моделі безпеки та потребують глибшого аналізу контексту взаємодії, типових поведінкових шаблонів і системних подій на рівні ядра віртуальної машини.

З метою подолання вказаних обмежень у роботах [6] – [8] пропонуються моделі інструментального виявлення прихованих загроз, що базуються на поєднанні предикативного аналізу, машинного навчання, графових структур (HARM, attack trees, knowledge graphs) та адаптивного оцінювання відповідності транзакцій політикам безпеки (RBAC, ABAC, Zero Trust). Поширеним підходом є побудова мультиграфа транзакцій із контекстним маркуванням вузлів, що дозволяє виявляти аномальні послідовності дій у взаємодії між хмарними сервісами.

Таким чином, аналіз сучасного стану досліджень свідчить про необхідність створення інструментальних засобів нового покоління, які б поєднували здатність до глибокого моніторингу на рівні гіпервізора [1], [14], підтримку телеметрії в режимі реального часу [10], [20], інтеграцію з системами реагування (SOAR) та динамічне формування моделей поведінки [9], [15]. Такі засоби мають забезпечити не лише

виявлення, а й проактивне блокування прихованих загроз до моменту їхньої реалізації, з мінімальним впливом на продуктивність хмарного середовища.

У статті запропоновано модель прихованих загроз інформаційної безпеки, що враховує динамічний характер суб'єктів і об'єктів інформаційної взаємодії, а також контекст виконання транзакцій в середовищі хмарних обчислень [14], [16], [21]. Особливу увагу приділено моделюванню інструментальних механізмів протидії загрозам, які залишаються невидимими для гостьових операційних систем, але реалізуються внаслідок специфіки архітектури віртуалізації, гіпервізорів та платформ керування ресурсами (зокрема KVM, Xen, Hyper-V, а також хмарних оркестраторів [2], [4] на зразок Kubernetes або OpenStack).

Запропоновано вісімрівневу ієрархічну структуру побудови інструментальних засобів виявлення і блокування прихованих загроз [7], яка охоплює рівні планування ресурсів, ізоляції середовищ виконання, диспетчеризації апаратних запитів, API-інтерфейсів, інтерпретації системних викликів, аналізу логів, політик безпеки та динамічного моніторингу поведінки компонентів. Для формалізації процесів інформаційної взаємодії розроблено модель операцій, що здійснюються на різних рівнях функціонування хмарного середовища, включаючи системний рівень гіпервізора, гостьові ОС, контейнеризовані сервіси та міжкластерні API.

У межах цієї моделі компоненти гіпервізора розглядаються як потенційні носії загроз, що можуть реалізовуватись шляхом поширення шкідливого програмного забезпечення, ін'єкцій у середовище виконання або ініціалізації некоректних процесів, які порушують цілісність, конфіденційність і доступність ресурсів. Відповідно, інструментальні засоби виявлення прихованих атак базуються на формалізованому описі загроз у вигляді послідовностей некоректних транзакцій, що взаємодіють із модулями гіпервізора або використовують недокументовані можливості системного чи прикладного ПЗ.

Такі транзакційні послідовності дозволяють класифікувати операції, що використовуються порушниками для реалізації прихованих атак, зокрема шляхом маніпуляцій із системними викликами, API-процедурами доступу до віртуальних дисків, портів введення/виведення, переривань та інших критичних функцій гостьових ОС [3], [5]. Запропоновано формалізований опис операцій, який дозволяє інструментально ідентифікувати спроби «вбудовування» шкідливих кодів у середовище виконання на рівні планувальника задач, диспетчера апаратного забезпечення або служби автозавантаження.

Підхід до опису операцій базується на класифікації ризиків порушення політики безпеки та аналізі контексту виконання команд, які можуть передавати дані в обхід декларативно визначених обмежень. Такі ситуації, зокрема, виникають під час непрямого доступу до компонентів з нижчим рівнем безпеки або при підміні авторизованих транзакцій.

У межах запропонованої моделі операції описуються як взаємодії між множинами суб'єктів і об'єктів доступу, яким присвоєно різні рівні безпеки, відповідно до політики багаторівневого контролю доступу (наприклад, на основі ролей або атрибутів — RBAC/ABAC). Для інструментального контролю процесів створення нових суб'єктів запропоновано умову інваріантності об'єкта, що породжує новий суб'єкт [6]. Це означає, що породження нового суб'єкта доступу можливе лише за умови незмінності атрибутів породжуючого об'єкта у момент часу $t > t_0$, де $t_0$ — час ініціалізації операції. Таким чином, формальною умовою є $O_n[t] = O_m[\,t_0]$, де $Subj$ — суб'єкт доступу, $Obj$ — об'єкт, а $j, m$ — відповідні індекси у специфікації моделі хмарного середовища.

У рамках цієї моделі формалізовано множини суб'єктів $S$ і об'єктів $O$, яким призначено рівні довіри $\lambda \in L$, де $L$ — впорядкована множина рівнів безпеки, що підтримує концепції Zero Trust (наприклад, untrusted, trusted, privileged) [8]. Операція доступу $\delta: S_i \to O_j$ вважається допустимою, якщо виконується умова $\lambda(S_i) \geq \lambda(O_j)$, що гарантує контроль вертикальних і горизонтальних взаємодій у хмарному середовищі.

Особливу увагу приділено інструментальному опису динаміки створення нових суб'єктів доступу, зокрема процесів, контейнерів чи функцій у моделі Function-as-a-Service. Для цього запропоновано умову інваріантності породжувального об'єкта: породження нового суб'єкта $S_k = Create(O_j, t)$ є припустимим лише за умови незмінності атрибутів породжуваного об'єкта у проміжку часу $t > t_0$, тобто виконується рівність $O_n[t] = O_m[t_0]$ [17]. Це дозволяє інструментально запобігати прихованому «розмноженню» шкідливих компонентів у середовищі виконання.

Для формалізації операцій доступу до ресурсів розглядається транзакція у вигляді кортежу $\tau = \langle S_i, O_j, op, t \rangle$, де $op \in \{read, write, execute, modify\}$ — тип операції, а $t$ — час її виконання. Набір транзакцій $T = \langle \tau_1, \tau_2, \ldots, \tau_k \rangle$ формується у вигляді мультиграфа доступу $G = (S \cup O, T)$ [6, 21], на основі якого реалізується модуль інструментального моніторингу.

У мультиграфі можуть бути виявлені аномальні шаблони поведінки, зокрема цикли підвищення прав доступу, транзакції до ресурсів із вищим рівнем довіри або ланцюжки дій, нехарактерні для нормального режиму функціонування. Для цього використовується порівняння з поведінковою моделлю $M_{norm}$, що може бути побудована на основі машинного навчання або правил експертної системи. Динамічний аналіз мультиграфа дозволяє виявляти приховані залежності між подіями, які не можна розпізнати традиційними методами контролю. Виявлені відхилення можуть бути використані для формування сигнатур нових атак або адаптації існуючих політик безпеки. Крім того, побудова і візуалізація мультиграфів дає змогу аналітикам отримувати інтуїтивне уявлення про складні сценарії зловживань. Таким чином, модель забезпечує не лише детекцію, а й підтримку процесу пояснюваного аналізу інцидентів у хмарному середовищі.

Прихована загроза вважається виявленою, якщо задовольняється хоча б одна з таких умов [9], [15], [19]:

- спрацювання по відомому сигнатурному шаблону (чорному списку): $\exists \tau: op = execute \wedge payload(\tau) \in blacklist$;
- виявлення послідовності транзакцій, не сумісної з моделлю $M_{norm}$: $\exists (\tau_1, \tau_2) \in T: Sequence(\tau_1, \tau_2) \notin M_{norm}$;
- порушення політики довіри: $\exists \tau: \lambda(S_i) < \lambda(O_j)$ [7].

З метою забезпечення глибокого моніторингу інструментальний модуль виконує відображення кожної транзакції $\tau$ у відповідний контекст виконання $\sigma(\tau)$, який містить дані про UID, IP-джерело, тип контейнера, вузол виконання, використаний API, системні виклики та інші метадані. Ці дані передаються у середовище потокового моніторингу (наприклад, через eBPF або telemetry bus) для подальшого аналізу засобами SIEM або XDR [10], [15], [20]. Таким чином, запропонована модель забезпечує формалізовану основу для побудови інструментальних засобів виявлення прихованих загроз у хмарних обчисленнях. Її використання дозволяє не лише виявляти аномалії на рівні поведінки, а й автоматично формувати правила реагування на порушення політик безпеки, із можливістю інтеграції у Zero Trust-архітектуру або сервіси типу CSPM/SOAR [5], [10].

У процесі обробки кожна транзакція супроводжується генерацією унікального цифрового відбитка, що зберігається в лог-журналі для подальшого аудиту. Це дозволяє не лише простежити повний ланцюг дій користувача чи процесу, але й локалізувати джерело потенційного компрометування. На основі накопичених метаданих будується граф залежностей між транзакціями, що полегшує виявлення складних атак типу APT або lateral movement. У моделі передбачено також механізм навчання на нормальній активності для побудови профілів допустимої поведінки контейнерів. У разі виявлення відхилень генерується тригер, який ініціює ізольовану перевірку підозрілих вузлів та контейнерів. Таким чином, реалізовано не лише пасивний моніторинг, а й проактивний механізм реагування у хмарному середовищі.

На рис. 1 представлено контекстно-орієнтовану DFD-модель першого рівня, що демонструє логіку роботи інструментального засобу для виявлення прихованих загроз у хмарній інфраструктурі. Вхідні дані — системні виклики, запити до ресурсів та поведінкові дії гостьових ОС — обробляються гіпервізором і передаються до модуля телеметрії [1], [4]. Контекстна інформація (audit logs, eBPF, події ядра, мережеві метадані) аналізується модулем поведінкового аналізу на відповідність еталонній моделі ($M_{norm}$). У разі аномалій перевіряються політики RBAC/ABAC, а у разі порушень формується тригер, який SIEM-система фіксує або блокує активність [9], [18]. Така інтеграція забезпечує проактивне виявлення загроз і реакцію в реальному часі.

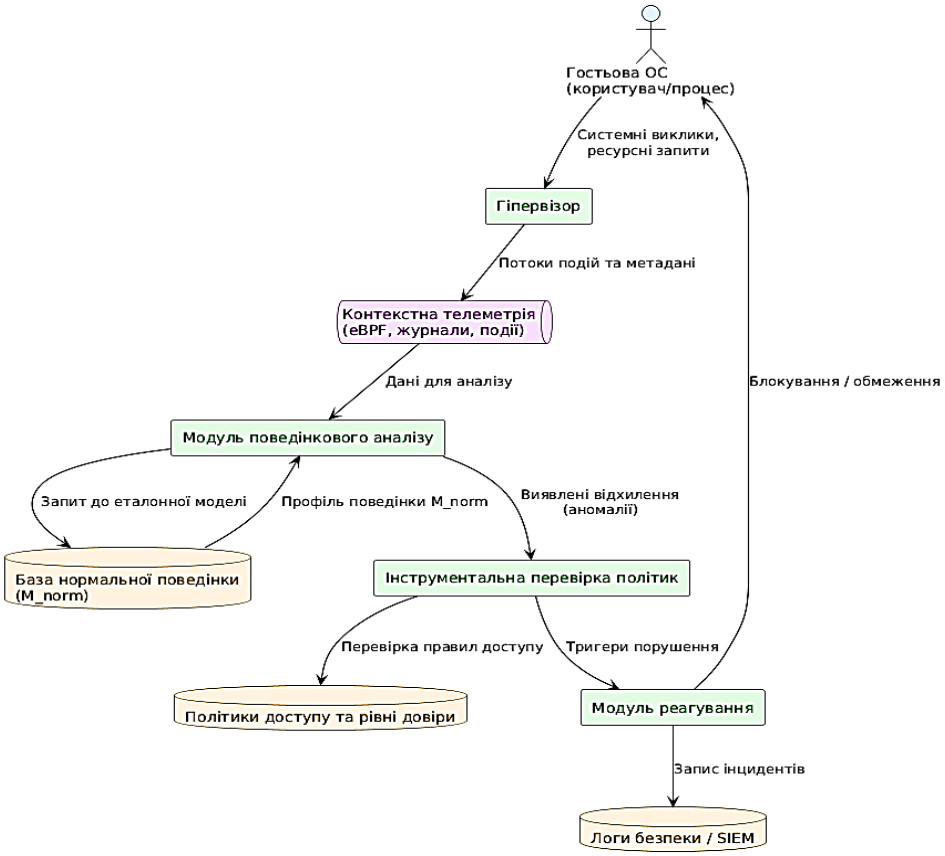


*Рис. 1. DFD-модель інструментального виявлення прихованих загроз у хмарному середовищі*

*Джерело: розроблено автором (знімок з екрану)*

У роботі розглядається формалізована модель прихованих загроз в інфраструктурі хмарних обчислень з урахуванням динамічного характеру суб'єктів і об'єктів інформаційної взаємодії, а також контексту виконання операцій у середовищі віртуалізації [1], [2]. Запропоновано оновлену восьмирівневу ієрархічну структуру аналізу, яка відображає взаємодію між компонентами гіпервізора, гостьовими операційними системами та прикладними програмами [4], [7], [10]. Модель враховує сучасні підходи до гіпервізорів типу KVM, Xen, ESXi, а також принципи Zero Trust Access та ролі безпеки (Security Roles).

Для деталізації моделі було введено чотири рівні привілеїв команд: Priv0 — команди процесора, Priv1 — ядро гостьової ОС, Priv2 — адміністратор сервера віртуалізації, Priv3 — користувачі віртуальної машини. З метою контролю незмінності об'єктів у контексті динамічної ролі суб'єктів запропоновано механізм верифікації контексту виконання операцій на основі логічної предикатної функції:

$$P_i = (s, Ord, Context\_type), \quad (1)$$

де $s$— предикат підвищення/пониження привілеїв, $Ord$ — родинність процесу, $Context_{type} \in \{1, 0, -1\}$ — режим взаємодії з пам'яттю (читання/запис/очікування).

Ці контексти застосовуються для побудови автомата функціонування гіпервізора:

$$mode1 = (E_i, R_i, start, Priv_i, F_i, P_i, V_i), \quad (2)$$

де $R_i$ — стани компонентів гіпервізора, $F_i$ — функція переходу між станами, $V_i$ — зовнішні впливи (легітимні запити або атаки), $P_i$ — дозволена функція стану згідно з (1).

На основі цього опису сформовано предикативну функцію виявлення прихованих загроз, що охоплює такі компоненти [6], [9]:

$$< Source, Services, Devices, \{proc\}, Actions, \{liv\}, \{vm\}, SecurityRoles >, \quad (3)$$

де $Source$ — атакувальний суб'єкт, $Devices$ — ресурси ВМ, $Actions$ — потенційно небезпечні операції (create, read, write, execute), {proc} — шкідливі процеси, $SecurityRoles$ — механізми контрольованого доступу, що визначають дозволені політики. У рамках графової моделі безпеки вузли типу Source ідентифікують атакувальні суб'єкти, які ініціюють аномальні або несанкціоновані дії. Вузли Devices відображають цільові ресурси віртуальних машин, що можуть бути скомпрометовані через ланцюжки взаємодій. Орієнтовані ребра з мітками Actions фіксують критичні операції, зокрема create, read, write та execute, які здійснюються над цими ресурсами. При цьому підмножина процесів {proc}, виявлених як шкідливі, порушує обмеження, визначені політиками SecurityRoles, що реалізують принцип контрольованого доступу та ізоляції.

У рамках моделі розглядаються приклади прихованих загроз, які виникають унаслідок: нетипового виконання команд гостьовою ОС [3], модифікації станів гіпервізора [4], несанкціонованого доступу до даних між різними ВМ [5], використання гіпервізора як елемента APT-атаки (Advanced Persistent Threat) [18]. У хмарному середовищі із використанням гіпервізорів виникає низка прихованих загроз, які здатні порушити безпеку системи. Зокрема, виконання нестандартних команд на рівні віртуальної машини може призвести до несанкціонованого доступу до системних ресурсів. Порушення допустимих переходів між станами ВМ і гіпервізора здатне спричинити втрату цілісності логіки обробки запитів. Модифікація компонентів гіпервізора створює умови для вбудовування шкідливого коду й ескалації привілеїв. Окрім того, перехресний доступ між віртуальними машинами загрожує витоком даних і порушенням конфіденційності ізольованих середовищ. Ці загрози визначають ключові вектори атак, що потребують постійного контролю та моніторингу у межах інструментальних засобів забезпечення інформаційної безпеки.

Окрему категорію становлять приховані загрози, що реалізуються у процесі взаємодії між компонентами сучасних хмарних платформ, зокрема під час використання сервісів AWS Lambda, Google Cloud Workload Identity, Azure Functions та інших функцій як послуг (FaaS) [20]. Атаки можуть здійснюватися шляхом ін'єкції шкідливого коду у подієвий ланцюг, підміни ролей (role assumption) через неправильну конфігурацію IAM-політик, або зловживання правами доступу до облікових даних сервісних облікових записів. Наприклад, у GCP Workload Identity зловмисник може ініціювати міжпроєктний доступ до сервісів з використанням легітимних токенів, якщо не застосовано обмеження на trust-relation [5], [10]. Такі сценарії унеможливлюють ефективний захист на рівні perimeter-based моделей і потребують динамічного інструментального контролю з урахуванням контексту взаємодії та поведінки функціональних компонентів.

У результаті, запропонована модель є базовою для реалізації інструментальних засобів: моніторингу контексту виконання операцій [21], детекції прихованих переходів між рівнями привілеїв [2], контролю за створенням нових суб'єктів і об'єктів доступу [9], аналізу політик безпеки в режимі реального часу [10]. Такі засоби є ключовими компонентами сучасних систем забезпечення інформаційної безпеки у хмарній інфраструктурі, зокрема при розгортанні ізоляції ВМ, контролю цілісності гіпервізора та динамічному управлінні політиками доступу відповідно до стандартів NIST SP 800-207, ISO/IEC 27017 та рекомендацій OWASP хмарно-орієнтованих.

Рис. 2 ілюструє часову взаємодію основних компонентів системи інструментального контролю: гостьової ОС, гіпервізора, модуля моніторингу, телеметричного колектора, підсистеми аналізу поведінки, контекстного контролера, транзакційного модуля та модуля реагування. Показано послідовність викликів, перевірок і реакцій на аномальні дії, що дозволяєь своєчасно виявити приховану активність, порушення політик доступу чи спроби ескалації привілеїв у середовищі віртуалізації. Ця модель дозволяє простежити логіку передачі сигналів, їх обробку та реалізацію механізмів блокування чи сповіщення відповідно до контексту загрози.

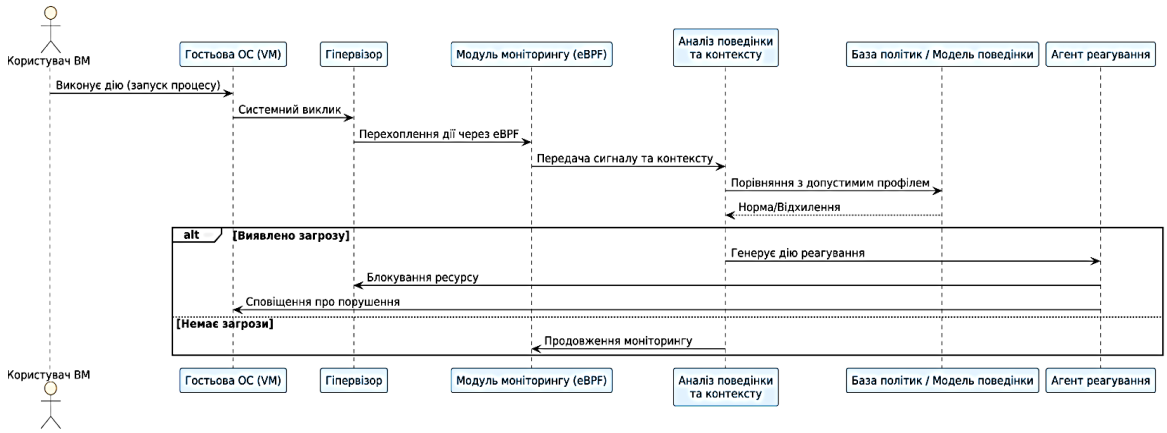


*Рис. 2. Діаграма послідовності реагування на приховану загрозу у хмарній інфраструктурі*
*Джерело: розроблено автором (знімок з екрану)*

У сучасних хмарних обчислювальних середовищах загострюється потреба в інструментальних засобах забезпечення інформаційної безпеки, здатних ефективно виявляти та нейтралізувати приховані загрози, що виникають у гіпервізорі та пов'язані з неконтрольованими транзакціями між віртуальними машинами (ВМ) та компонентами

середовища виконання [1], [2], [4], [6], [7]. З метою формалізації таких загроз запропоновано багаторівневу модель, яка відображає структуру взаємодії системних і прикладних процесів.

Ієрархічна модель гіпервізора передбачає вісім рівнів: рівень прикладних процесів (S1), ядро гостьової ОС (S2), обробники переривань (S3), менеджер пам'яті (S4), підсистема введення/виведення (S5), планувальник задач (S6), диспетчер взаємодії з обладнанням (S7) та виконавчий процесор (S8). На рівнях S1–S5 працюють традиційні засоби захисту інформації (СЗІ) [9], які реалізують політики доступу та авторизації. Водночас приховані загрози переважно локалізовані на рівнях S6–S8, які залишаються поза сферою спостереження традиційних СЗІ.

У хмарній інфраструктурі особливу небезпеку становлять вектори атак, притаманні саме хмарно-орієнтованим середовищам. Сучасні хмарні платформи активно використовують оркестратори контейнерів (наприклад, Kubernetes), сервіси функцій як послуги (Serverless/FaaS), а також шлюзи керування запитами (API Gateway), що створює унікальні точки уразливості. Для Kubernetes характерні такі загрози, як неправильне конфігурування правил доступу RBAC, публічний доступ до kube-apiserver або зловживання привілеями у kubelet. Ці вектори дозволяють здійснювати несанкціоноване виконання команд, втручання в кластер або підвищення привілеїв.

У середовищах Serverless поширеними є атаки типу ін'єкція подій (Event Injection), коли зловмисник ініціює неочікувану подію, що призводить до небажаного виконання функції. Через короткочасність існування таких функцій традиційні засоби захисту часто не встигають їх виявити або зреагувати. Для подолання цієї вразливості запропоновано використання контекстного трекінгу подій, що дозволяє встановлювати ланцюжки викликів і перевіряти їх відповідність допустимому сценарію. Зокрема, кожна подія фіксується разом із її джерелом, параметрами виклику, типом тригера та рівнем довіри. Це дозволяє виявляти невідповідності між очікуваними та фактичними сценаріями виконання. У разі виявлення аномалій система може автоматично блокувати виконання або перенаправляти подію до sandbox-середовища для безпечного аналізу. Також реалізується збереження журналів подій із короткотерміновим TTL для підтримки forensics. Таким чином, забезпечується підвищення стійкості Serverless-архітектур до атак ін'єкційного типу та зниження ризику несанкціонованого виконання.

API Gateway, що виступає посередником між сервісами, може піддаватися атакам типу API fuzzing, маніпуляція токенами, надмірне розкриття даних. Неналежна обробка JWT-токенів або відсутність перевірки прав доступу призводить до обхідних сценаріїв автентифікації. Актуальними залишаються і атаки ланцюга постачання (Supply Chain), коли зловмисники інтегрують шкідливий код у процеси CI/CD або до контейнерних залежностей [10]. Такі загрози є складними для виявлення і вимагають спеціалізованих механізмів аналізу.

Отже, хмарно-орієнтовані архітектури формують нові вектори прихованих загроз, які виходять за межі класичних моделей віртуалізації. Ефективне виявлення таких загроз потребує адаптації інструментальних засобів безпеки до специфіки Kubernetes, AWS Lambda, Google Cloud Functions, Istio, Envoy та інших сучасних хмарних платформ. Таким чином, сучасна хмарна інфраструктура має враховувати специфіку хмарно-орієнтованих загроз при побудові засобів виявлення, блокування та реагування, адаптованих до таких платформ як Kubernetes, AWS Lambda, Google Cloud Functions, Azure Functions, Istio, Envoy, API Gateway. Це передбачає глибоку інтеграцію засобів безпеки на рівні сервісної сітки, контейнерного оркестратора та serverless-тригерів. Необхідно забезпечити підтримку потокового аналізу подій, міжсервісного шифрування,

контролю політик доступу та анонімізації трафіку. Також важливо впроваджувати контекстно-орієнтовані правила обробки транзакцій з урахуванням ролей, навантаження та джерела запиту. Системи моніторингу мають бути здатні працювати з метаданими в реальному часі та формувати динамічні профілі безпечної поведінки. Крім того, має бути забезпечена сумісність із Zero Trust-архітектурою та автоматичне оновлення сигнатур і моделей загроз. Такий підхід дозволяє забезпечити комплексний захист у розподіленому хмарному середовищі з високим ступенем динаміки.

Для опису динаміки обробки запитів запропоновано використання мультиграфа транзакцій $G = \langle R, D, I \rangle$, де $R$ — множина станів, $D$ — множина допустимих переходів, $I$ — матриця інциденцій. Ліві дуги описують звичайні транзакції без зміни контексту, праві — контекстно-залежні переходи, які можуть ініціюватися модифікованими (шкідливими) компонентами. У такій моделі особливу увагу приділено виявленню правих дуг, що порушують типову логіку переходів між станами. Їх поява може свідчити про втручання сторонніх агентів або виконання дій поза встановленими політиками безпеки. Для кожного вузла стану зберігається контекст виконання, що включає атрибути сеансу, привілеї, тип ініціатора та часові характеристики. Аналіз зваженого мультиграфа дозволяє визначати аномальні маршрути з високим ризиком або низькою довірою. Матриця інциденцій III оновлюється в реальному часі для підтримки динамічного реагування на нові шаблони активності. Таким чином, модель забезпечує формалізований підхід до моніторингу складних транзакцій у хмарному середовищі з підтримкою оцінки контекстної аномальності.

Сучасні інструментальні засоби захисту мають забезпечувати виявлення прихованих загроз через аналіз контексту операцій. У цьому зв'язку сформульовано умову розв'язності задачі як теорему спостережуваності: зміни станів транзакційного графа мають бути ідентифіковані за допомогою простих або комбінованих предикатів. Ключовим елементом моделі є множина подій $E$, що складається з двох підмножин: $Ehv$ — події гіпервізора, $Evm$ — події від ВМ. Атаки можуть запускатися через $Evm$ шляхом впровадження шкідливих команд у нижні рівні, які не відслідковуються класичними СЗІ. Прикладами таких атак є IceBrute, RuStock, Red Dragon, VICE Toolkit, що змінюють транзакції між ВМ1 і ВМ2 через перехоплення драйверів доступу. Отже, поєднання моделі мультиграфа транзакцій із просторово-контекстною декомпозицією дозволяє формалізовано виявляти порушення політик безпеки на всіх рівнях гіпервізора, створюючи підґрунтя для ефективного виявлення як явних, так і прихованих загроз у хмарному середовищі.

Для цього кожна подія з множини EEE маркується атрибутами часу, джерела, цілі, типу виклику та рівня довіри. Таке маркування дозволяє відслідковувати нелегітимні взаємодії між ВМ, зокрема ті, що відбуваються поза межами дозволеної політики маршрутизації. Додатково використовується механізм квантування активності, що агрегує події у часові вікна для виявлення повторюваних шаблонів поведінки. При виявленні критичних відхилень активується реактивна політика — наприклад, переміщення контейнера у карантин або обмеження доступу до спільних ресурсів. Інтеграція моделі у систему SIEM або XDR дозволяє здійснювати кореляційний аналіз між подіями на різних рівнях віртуалізації. Таким чином, запропонований підхід підвищує обґрунтованість рішень щодо блокування загроз у реальному часі в умовах хмарної інфраструктури.

На рис. 3 подано формалізовану модель транзакційної взаємодії між рівнями гіпервізора у вигляді мультиграфа. Вершини ($R_1$–$R_8$) відповідають ієрархічним станам — від прикладного рівня до процесора, а дуги — переходам між ними. Ліві дуги ($p_1$–$p_7$)

ISSN 2663 - 4023

позначають дозволені переходи без зміни контексту, праві ($q_1$–$q_7$) — потенційно небезпечні, що виникають через втручання шкідливого ПЗ. Модель демонструє перехоплення системного виклику гостьової ОС, що дозволяє атакувати інші ВМ через рівні S5–S7, порушуючи безпеку хмарної інфраструктури.

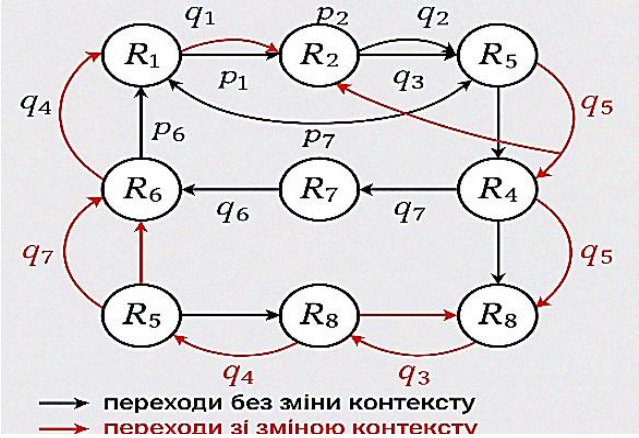


*Рис. 3. Модель аналізу привілейованих транзакцій у віртуалізованому хмарному середовищі*

*Джерело: розроблено автором (знімок з екрану)*

Сценарій ілюструє вертикальне просочування впливу від рівня користувача до апаратного забезпечення з подальшим поверненням у контекст іншої віртуальної машини. Такі переходи, позначені як праві дуги, є нетиповими для нормального функціонування системи та вказують на загрозу типу lateral movement. Аналіз мультиграфа дозволяє виявити подібні траєкторії шляхом зіставлення з нормативною поведінковою моделлю. Виявлені відхилення можуть бути маркерами для формування сигнатур атак або тригерів динамічного реагування. Зокрема, система може автоматично змінювати права доступу, обмежувати ресурси або ізолювати підозрілу ВМ. Таким чином, модель на рис. 3 є базою для побудови інструментів детекції складних прихованих загроз на міжвіртуалізаційному рівні.

Рис. 4 показує послідовність дій під час прихованої атаки через перехоплення системного виклику, ініційованого користувачем у віртуальній машині (ВМ1). Виклик, переданий гіпервізором, перехоплюється шкідливим модулем (наприклад, VICE Toolkit, IceBrute або Red Dragon), модифікується та надсилається до драйвера, що забезпечує несанкціонований доступ до іншої ВМ (ВМ2), порушуючи ізоляцію. Сценарій підкреслює важливість контролю нижніх рівнів взаємодії та необхідність моніторингу на рівні гіпервізора.

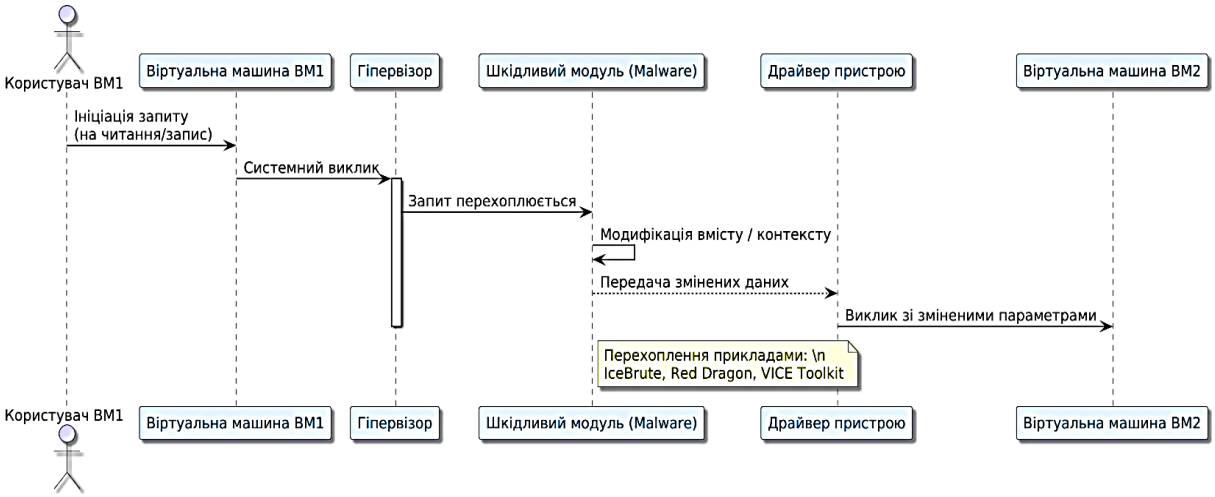


*Рис. 4. Діаграма послідовності перехоплення системного виклику на рівні гіпервізора*
*Джерело: розроблено автором (знімок з екрану)*

Атака використовує слабкі місця в реалізації системних викликів, які гіпервізор не завжди здатен своєчасно відфільтрувати без додаткових засобів аналізу. Унаслідок цього зловмисник отримує можливість впливати на ресурси інших віртуальних машин у тій самій хмарній інфраструктурі. Така поведінка порушує модель довіри та компрометує базові принципи багатокористувацької ізоляції. Для виявлення подібних сценаріїв необхідно застосовувати інструментальні засоби з контекстною перевіркою послідовностей системних викликів. Також ефективним є впровадження механізмів журналювання та трасування на рівні гіпервізора з використанням eBPF або аналогічних технологій. Таким чином, послідовність на рис. 4 демонструє критичність глибокого моніторингу взаємодій у віртуалізованих середовищах.

Рис. 5 ілюструє вертикальну ієрархію рівнів гіпервізора (від S1 до S8), через які проходить системний виклик, ініційований користувачем у віртуальній машині (VM1). На рівні S5 здійснюється перехоплення запиту модулем шкідливого ПЗ, який змінює логіку виконання, передаючи втручання до цільової віртуальної машини (VM2). Інструмент IDS/EDR виконує контроль за аномальними діями та формує відповідь системи. Модель наочно демонструє, на якому етапі можливе втручання зловмисника та як інструментальні засоби можуть виявити загрозу. Ця модель дозволяє ідентифікувати критичні точки контролю, де необхідне впровадження механізмів спостереження та реагування. Рівні S1–S4 зазвичай охоплюють користувацькі та прикладні компоненти, тоді як рівні S5–S8 відповідають за системну, віртуалізаційну та апаратну взаємодію. Втручання на рівні S5 свідчить про порушення ізоляції, яке може залишитися непоміченим без глибокого моніторингу. Інструменти типу IDS/EDR мають бути здатні фіксувати неочікувані переходи між цими рівнями з контекстною перевіркою викликів. Виявлення таких аномалій дозволяє запобігти розширенню привілеїв і поширенню атак між віртуальними машинами. Отже, рис. 5 акцентує увагу на важливості вертикального моніторингу у хмарно-орієнтованих середовищах.

ISSN 2663 - 4023

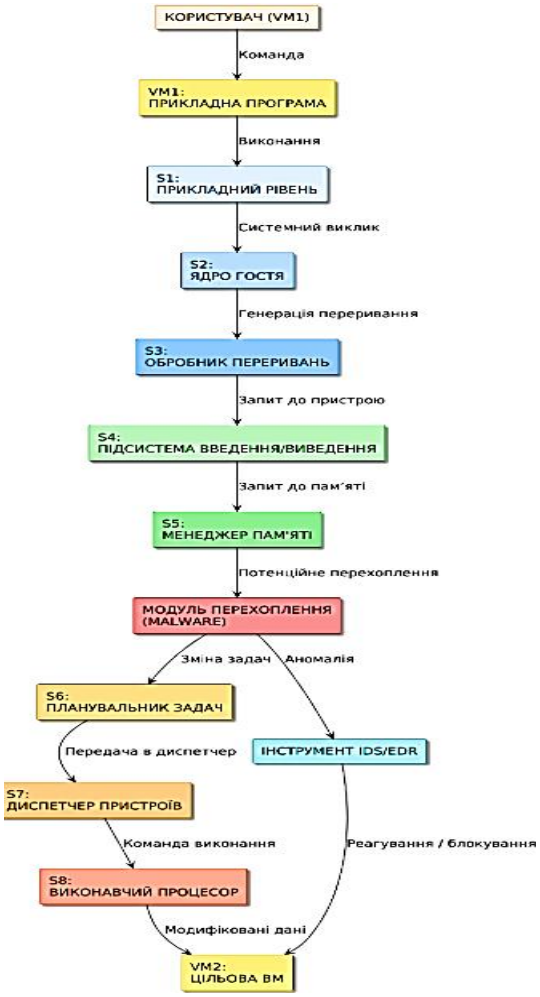


*Рис. 5. Архітектурна модель перехоплення системного виклику у віртуалізованому хмарному середовищі*
*Джерело: розроблено автором (знімок з екрану)*

У сучасній хмарній інфраструктурі запропоновано метод виявлення прихованих загроз на основі предикативного аналізу мультиграфа транзакцій [6], [21]. Алгоритм ідентифікує загрози шляхом верифікації команд і перевірки їх відповідності політикам безпеки на рівні гостьової ОС і гіпервізора. Уведено поняття «контекст виконання переходів» як дерево графів із мітками — кортежами змінних: стану (s), родоводу (Ord) та типу контексту (Context_type) [6]. Зміни контексту описуються інцидентною матрицею. Незважаючи на неконтрольовані стани, предикатні функції залишаються розв'язними завдяки спостережуваним змінним. [9] Метод включає побудову мультиграфа, формалізацію контексту запиту, перевірку команд згідно з політиками, що описують послідовності операцій з обмеженнями на зміну привілеїв [10]. На рівнях S1–S8 фіксується журнал подій із часом і результатами [7]. Дозволеність переходів перевіряється логічною функцією станів, а контроль потоків базується на принципі найменших привілеїв.

У межах сформованої політик безпеки встановлено, що:

- Якщо s = 0, Context_type = -1 — стан заборонено (спроба пошкодження компонентів гіпервізора).

- Якщо s = 0, Context_type = 1 — стан заборонено (спроба модифікації конфігурацій ВМ).
- Якщо s = 1 — стан дозволено (контрольований перехід).
- Якщо s = 0, Ord = 0, Context_type = 0 — очікування користувацьких запитів.

Запропоновано модель виявлення шкідливого ПЗ у компонентах гіпервізора та гостьових ОС на основі запитів від користувачів віртуальних машин [18]. Вхідними даними є операції системного рівня — зокрема планувальник задач (S6), диспетчер обладнання (S7) і елементи віртуалізації (S8) [20], [21]. Пошук прихованих загроз здійснюється як цикл аналізу запитів: при Pi = true процес дозволено, при Pi = false — блокується. Формується оновлювана база даних шкідливого ПЗ [19]. Також реалізовано фільтрацію мережевого трафіку відповідно до таблиць дозволених операцій. У результаті запропонований підхід забезпечує ефективне виявлення прихованих загроз у хмарній інфраструктурі на основі логіко-графової моделі, що відповідає сучасним стандартам інформаційної безпеки.

Діаграма (рис. 6) демонструє поетапний процес аналізу активностей у віртуальному середовищі. Вона охоплює побудову мультиграфа транзакцій, формування контексту виконання, перевірку на відповідність політиці безпеки, логічне розгалуження рішень і оновлення бази даних загроз.

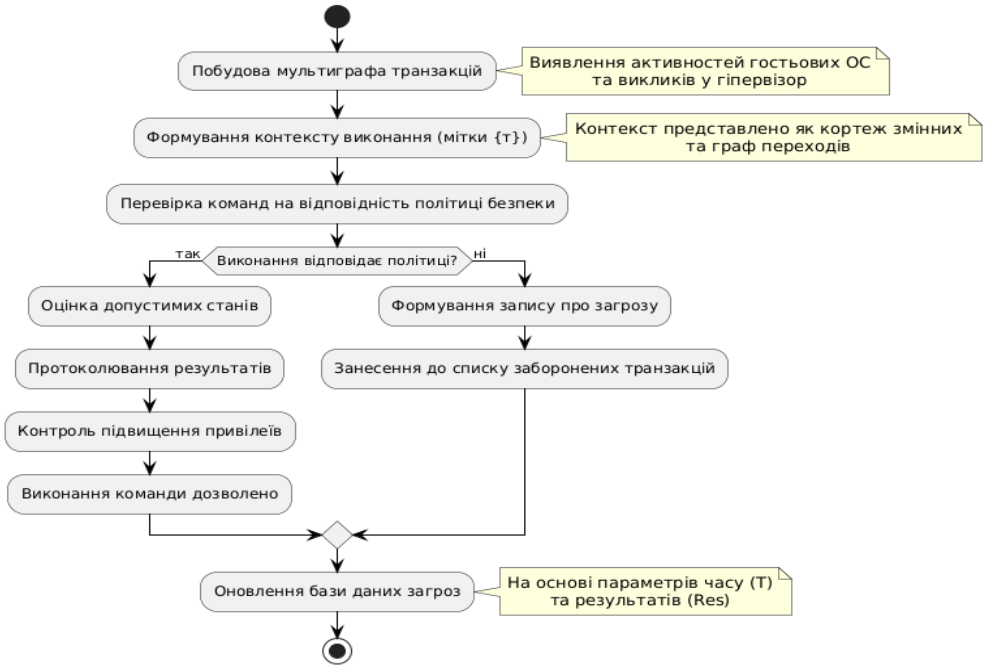


*Рис. 6. Алгоритм ідентифікації прихованих загроз у віртуалізованому хмарному середовищі*

*Джерело: розроблено автором (знімок з екрану)*

Розвиток хмарних обчислень вимагає ефективного захисту від прихованих загроз на рівні гіпервізора та гостьових ОС. Експерименти показали неефективність традиційних антивірусів і фаєрволів у віртуалізованому середовищі, особливо при наявності прихованих каналів між ВМ. Зловмисники обходять захист через нестандартний доступ, модифікацію гіпервізора або перехоплення обробників пам'яті та I/O [21]. У відповідь створено програмно-апаратний комплекс із проксуючим ядром та

верифікаційним модулем, що аналізує команди на рівні апаратного виконання. Це дозволяє виявляти аномалії без глибоких змін у системі.

Модель операцій адаптовано до багаторівневої структури гіпервізора з рівнями S1–S8, кожен з яких відповідає певному типу доступу чи контролю. Ефективність системи перевірено на тестовому стенді, що імітує корпоративну хмарну мережу з понад 50 вузлами, двома серверами та 60 робочими станціями, із використанням VPN і VIPNET. У ході експериментів застосовано зразки шкідливого ПЗ (BluePill, Storm, Legend, VICE Toolkit, Rustock) для перевірки здатності виявляти загрози, які не фіксують стандартні сканери. Порівняння показало, що розроблений комплекс «Альфа-монітор» суттєво перевершує традиційні засоби захисту (Kaspersky, Norton, VIPNET Firewall), особливо в умовах пікових навантажень. Він ефективно розпізнає приховані транзакції, модифіковані виклики та несанкціонований доступ до міжвіртуальних каналів. Застосування предикативної логіки, інструментального перехоплення та моделювання поведінки ГОС забезпечує надійний захист у хмарній інфраструктурі та знижує ризики атак типу rootkit і hyperjacking.

Модель (рис. 7) відображає вертикальну архітектуру засобів інформаційної безпеки у віртуалізованому хмарному середовищі, що охоплює гостьові ОС, гіпервізор і хмарну інфраструктуру [21]. До її складу входять: проксуючий модуль ядра ГОС, модуль перехоплення транзакцій, верифікаційний блок, система моніторингу та журналювання. Компоненти взаємодіють через багаторівневу модель (S1–S8), забезпечуючи детекцію, контроль і блокування прихованих атак (rootkit, hyperjacking) на всіх етапах виконання.

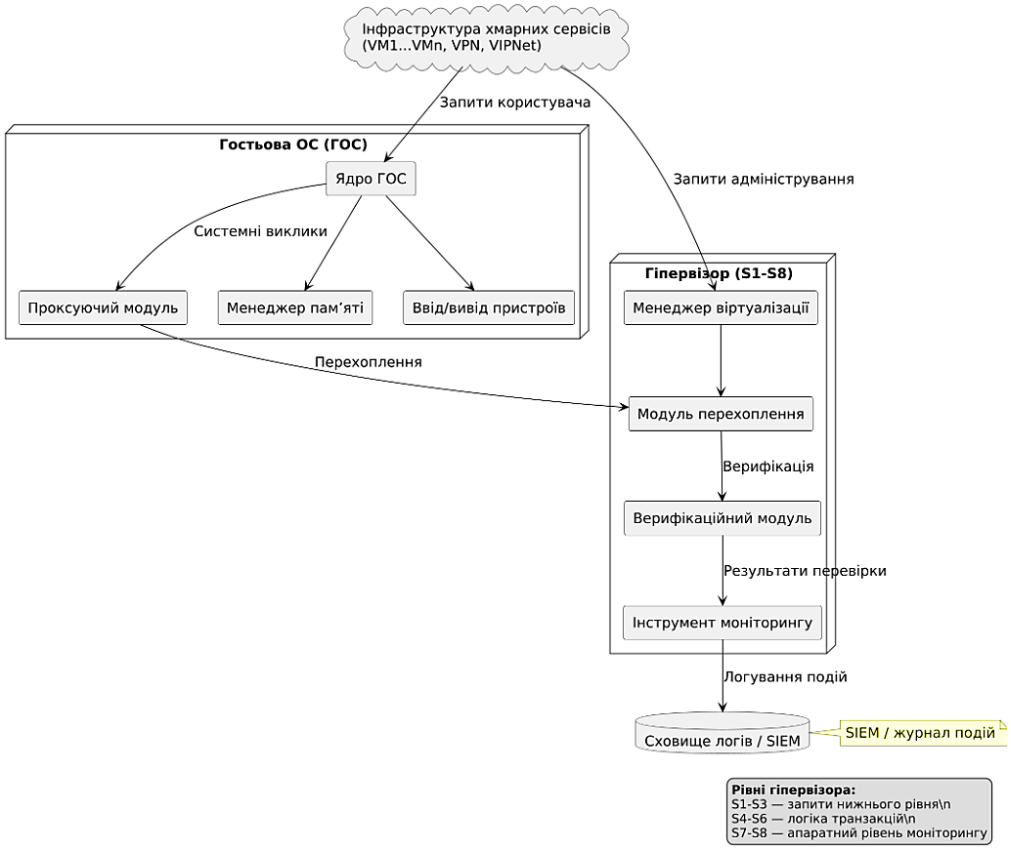


*Рис. 7. Комбінована архітектурна модель інструментального захисту хмарної інфраструктури від прихованих загроз*
*Джерело: розроблено автором (знімок з екрану)*

Отримані результати дозволили апробувати дослідний зразок програмного комплексу в умовах реального функціонування вітчизняних систем захисту, що підтверджує його практичну придатність і перспективність використання для забезпечення цілісності та конфіденційності інформації в середовищі віртуалізованих хмарних платформ.

На рис. 8 показано графічне представлення порівняльної ефективності засобів захисту за рівнями S1–S8. Позитивні результати (успішне виявлення загроз) позначено знаком «+» (зелений колір), а негативні — «−» (відсутність виявлення, світлі клітинки). Альфа-Монітор продемонстрував найвищу ефективність серед розглянутих засобів. У порівнянні з іншими засобами, він виявив найбільшу кількість прихованих атак, включаючи ті, що реалізуються через гіпервізор. Це свідчить про здатність системи ефективно реагувати на аномальні транзакції в середовищах з високим ступенем віртуалізації. Традиційні засоби показали обмежену ефективність на нижчих рівнях, що вказує на їхню непридатність у сценаріях з контекстно-залежними загрозами. Графічна інтерпретація наочно підтверджує перевагу комплексного підходу до захисту. Отже, Альфа-Монітор може розглядатися як перспективне рішення для багаторівневого захисту в хмарних інфраструктурах.

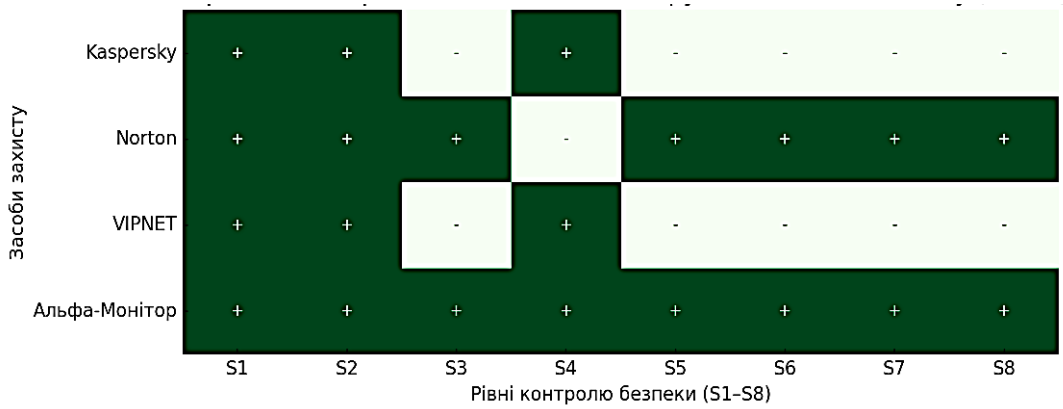


*Рис. 8. Порівняльна ефективність засобів інструментального захисту в віртуалізованому хмарному середовищі*
*Джерело: розроблено автором (знімок з екрану)*

Під час апробації було зафіксовано успішне виявлення прихованих транзакцій, які не фіксувалися класичними засобами захисту. Комплекс продемонстрував здатність адаптації до динаміки хмарного середовища без потреби в суттєвому втручанні в його архітектуру. Особливо ефективним виявився модуль контекстної перевірки системних викликів із використанням мультиграфової моделі. Інтеграція з існуючими SIEM- та SOAR-системами відбулася без конфліктів, забезпечивши автоматизовану реакцію на виявлені інциденти. Протестовані сценарії охоплювали як вертикальні, так і горизонтальні вектори атак, що дозволило перевірити стійкість моделі. Таким чином, комплекс може бути рекомендований до впровадження в інфраструктуру критично важливих об’єктів інформаційної безпеки.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У контексті сучасних хмарних обчислень у роботі комплексно досліджено проблему виявлення та протидії прихованим загрозам інформаційній безпеці у хмарних обчислювальних середовищах із віртуалізованою інфраструктурою. На основі глибокого аналізу вразливостей гіпервізорів і гостьових операційних систем (ГОС) було розроблено формалізовану багаторівневу модель операцій із позначенням контрольних рівнів (S1–S8) та побудовано DFD-, UML-діаграми, які відображають логіку взаємодії компонентів інструментального комплексу безпеки. Модель застосовна до хмарно-орієнтованих платформ із мікросервісною архітектурою та високою динамікою змін транзакційних потоків.

Запропоновано архітектуру програмно-апаратного комплексу, що включає проксуючі модулі для перехоплення системних транзакцій і верифікаційні модулі команд із контролем на рівні виконавчих регіонів процесора. Моделі і алгоритми були реалізовані як у вигляді UML-діаграм, так і у вигляді структурно-функціональних схем, що дозволяє масштабувати запропонований підхід до різних типів хмарних платформ і гіпервізорів. Модель сумісна з хмарно-орієнтованими сервісами та середовищами, зокрема AWS Lambda, Azure Functions, Kubernetes, Google Cloud Run, що підтверджує її гнучкість і технологічну незалежність.

Проведено експериментальну верифікацію системи на тестовому стенді, який моделює корпоративну віртуальну інфраструктуру, з використанням відомих зразків шкідливого ПЗ (BluePill, Storm, VICE Toolkit, Rustock тощо). Порівняльний аналіз ефективності засобів захисту показав, що «Альфа-Монітор» значно перевищує традиційні продукти, такі як Kaspersky Antivirus, Norton Security та VIPNET Firewall, особливо у випадках атак через приховані міжвіртуальні канали. Загалом, модель адаптована до особливостей хмарних платформ із мікросервісною архітектурою, що підтримують автоматичне масштабування та динамічний розподіл транзакцій між ізольованими контейнерами.

Таким чином, застосування інструментальних засобів на основі моделювання поведінки, предикативної логіки та структурного аналізу транзакцій забезпечує якісно новий рівень виявлення загроз, що не фіксуються класичними методами. Отримані результати можуть бути масштабовані до хмарно-орієнтованих середовищ, у яких класичні методи моніторингу втрачають ефективність через високу динаміку, мікросервісну ізоляцію та складність трасування транзакцій між контейнерами. Це, у свою чергу, дозволяє підвищити рівень інформаційної безпеки в середовищах хмарних обчислень, зокрема в умовах мікросервісної архітектури, контейнеризації та Serverless-обчислень.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aldribi, A., Traore, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Computers & Security, 88, 101646.* https://doi.org/10.1016/J.COSE.2019.101646
2. Althobaiti, A. (2017) Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment. *Journal of Information Security*, *8*, 1–7. doi: 10.4236/jis.2017.81001
3. He, Z., Hu, G., & Lee, R. B. (2023) CloudShield: Real-time Anomaly Detection in the Cloud. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy. *Association for Computing Machinery*, 91–102. https://doi.org/10.1145/3577923.3583639

4. Jindal, A., Shakhat, I., Cardoso, J., Gerndt, M., & Podolskiy, V. (2022). IAD: Indirect Anomalous VMMs Detection in the Cloud-Based Environment. *Service-Oriented Computing – ICSOC. Lecture Notes in Computer Science, vol 13236.* https://doi.org/10.1007/978-3-031-14135-5_15
5. R. Zakiyyah, D. Permana, D. Valencio, A. Chowanda, Y. Muliono and Z. N. Izdihar (2024) Security Challenges and Issues in Cloud Computing, *International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6, https://doi.org/10.1109/ISNCC62547.2024.10758966
6. S. Y. Enoch, M. Ge, J. B. Hong and D. Seong Kim (2021) Model-based Cybersecurity Analysis: Past Work and Future Directions, *Annual Reliability and Maintainability Symposium (RAMS)*, 1–7. https://doi.org/10.1109/RAMS48097.2021.9605784
7. Kostiuk, Y.V. & Voytkevich, A.A. (2024) Research on Technologies for Detection and Identification of Intruders for Corporate Network Protection. *"Science and Technology Today" (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Engineering"), 4(32),* 1017–1032.
8. Yesilyurt, M., Yalman, Y. (2016) New approach for ensuring cloud computing security: using data hiding methods. *Sādhanā, 41,* 1289–1298.
9. Kostiuk, Y.V. & Shapran, V.O. (2024) Technologies for Detection of Anomalous Events and Signatures in Real-Time. *"Science and Technology Today" (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Engineering"), 4(32),* 1069–1084.
10. Balbela, J. P. et al. (2023) Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing Advances in Science. *Technology and Engineering Systems Journal, 8(6),* 107–119.
11. Kryvoruchko, O., Kostiuk, Y., & Desiatko, A. (2024) Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods. *Ukrainian Scientific Journal of Information Security, 30(1),* 140–149.
12. Sanagana, D. P. R., & Tummalachervu, C. K. (2024) Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems, *Second International Conference on Data Science and Information System (ICDSIS),* 1–6.
13. Kostiuk, Y., Bebeshko, B., Kryuchkova, L., Litvinov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information Protection and Data Exchange Security in Wireless Mobile Networks with Authentication and Key Exchange Protocols. Electronic Professional Scientific *Journal "Cybersecurity: Education, Science, Technology*", *1(25),* 229–252.
14. Achbarou, O., El Kiram, M. A., Bourkoukou, O., & Elbouanani, S. (2018) A new distributed intrusion detection system based on multi-agent system for cloud environment. *Int. J. Commun. Netw. Inf. Secur, 10, 526.*
15. Kostiuk, Y., Bebeshko, B., Skladannyi, P., Rzaieva, S., & Khorolska, K. (2025). Buffer and priority optimization for ensuring security in Bluetooth networks. *Information Systems and Technologies Security, 2(8),* 5–16.
16. Kannadhasan, S., Nagarajan, R., & Thenappan, S. (2022) Intrusion detection techniques based secured data sharing system for cloud computing using msvm. *In Proceedings of the 9th International Conference on Computing for Sustainable Global Development (INDIACom),* 50–56.
17. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaieva, S. (2025). Method for protecting GRID environment from malicious code during computational task execution. *Electronic Scientific Journal "Cybersecurity: Education, Science, Technology*", *3(27),* 22–40.
18. Hatef, M.A., Shaker, V., Jabbarpour, M.R., Jung, J., & Zarrabi, H. (2025) HIDCC: A hybrid intrusion detection approach in cloud computing. *Concurr. Comput. Pract. Exp, 30, 4171.*
19. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Electronic Scientific Journal "Cybersecurity: Education, Science, Technology*", *3(27),* 534–548.
20. Zhang, J., Peter, J.D., Shankar, A., & Viriyasitavat, W. (2024) Public cloud networks oriented deep neural networks for effective intrusion detection in online music education. *Computers and Electrical Engineering, 115.*
21. Skladannyi, P.M., Kostiuk, Y.V., Mazur, N.P., & Pitaichuk, M.A. (2025). Investigation of characteristics and performance of access protocols to cloud computing environments based on universal testing. *Telecommunications and Information Technologies, 1(86),* 61–74.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

**Yuliia Kostiuk**
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
*y.kostiuk@kubg.edu.ua*

**Karyna Khorolska**
PhD in Computer Science
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-3270-4494
*karynakhorolska@gmail.com*

**Bohdan Bebeshko**
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-6599-0808
*b.bebeshko@kubg.edu.ua*

**Nadiia Dovzhenko**
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID:0000-0003-4164-0066
*nadezhdadovzhenko@gmail.com*

**Nataliia Korshun**
Doctor of Science, Professor,
Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-2908-970X
*n.korshun@kubg.edu.ua*

**Pazynin Andrii**
Postgraduate student
Institute of Telecommunications and Global Information
Space of the National Academy of Sciences of Ukraine, Kyiv
ORCID ID: 0009-0002-9506-9539
*Pazinin@gmail.com*

# INSTRUMENTAL MEANS OF ENSURING INFORMATION SECURITY AGAINST HIDDEN THREATS IN CLOUD COMPUTING INFRASTRUCTURE

**Abstract.** In cloud computing, the challenge of countering hidden information security threats is becoming increasingly critical due to the high dynamism of resource management, the complexity of verifying interprocess interactions, and the widespread use of virtualized environments. Particular attention is paid to threats that emerge at the hypervisor level or result from uncontrolled transactions between guest operating systems and cloud control subsystems, which renders them undetectable by traditional monitoring tools. To address these challenges, an instrumental approach is proposed that implements mechanisms for detecting and neutralizing latent attacks through continuous monitoring of system resource requests and behavioral analysis of component interactions. A formalized model

of information interaction has been developed within this study, representing the logic of sequential and parallel operations initiated by virtual machines when accessing computing, networking, and storage resources. This model enables not only the structuring of dynamic information flows but also the formalization of critical dependencies between transactions that could serve as vectors for hidden attacks. A threat identification method based on predicate logic is applied, taking into account the context of system call execution, including signs of anomalous activity and deviations from the active security policy. The results obtained confirm the practical feasibility of using formalized models of transactional interaction and predicate analysis to enhance the security of cloud services against complex and hidden information security threats. This is especially relevant in the context of the growing adoption of containerization, orchestration, and distributed computing technologies, particularly in environments such as AWS, Azure, Google Cloud Platform, and Kubernetes.

**Keywords:** information security, cloud computing, hidden threats, hypervisor, virtualization, instrumental tools, dynamic environment, security policy, monitoring, cloud services, cloud-oriented architectures.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Aldribi, A., Traore, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Computers & Security, 88, 101646.* https://doi.org/10.1016/J.COSE.2019.101646
2. Althobaiti, A. (2017) Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment. *Journal of Information Security*, *8*, 1–7. doi: 10.4236/jis.2017.81001
3. He, Z., Hu, G., & Lee, R. B. (2023) CloudShield: Real-time Anomaly Detection in the Cloud. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy. *Association for Computing Machinery*, 91–102. https://doi.org/10.1145/3577923.3583639
4. Jindal, A., Shakhat, I., Cardoso, J., Gerndt, M., & Podolskiy, V. (2022). IAD: Indirect Anomalous VMMs Detection in the Cloud-Based Environment. *Service-Oriented Computing – ICSOC. Lecture Notes in Computer Science, vol 13236.* https://doi.org/10.1007/978-3-031-14135-5_15
5. R. Zakiyyah, D. Permana, D. Valencio, A. Chowanda, Y. Muliono and Z. N. Izdihar (2024) Security Challenges and Issues in Cloud Computing, *International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6, https://doi.org/10.1109/ISNCC62547.2024.10758966
6. S. Y. Enoch, M. Ge, J. B. Hong and D. Seong Kim (2021) Model-based Cybersecurity Analysis: Past Work and Future Directions, *Annual Reliability and Maintainability Symposium (RAMS)*, 1–7. https://doi.org/10.1109/RAMS48097.2021.9605784
7. Kostiuk, Y.V. & Voytkevich, A.A. (2024) Research on Technologies for Detection and Identification of Intruders for Corporate Network Protection. *"Science and Technology Today" (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Engineering"), 4(32),* 1017–1032.
8. Yesilyurt, M., Yalman, Y. (2016) New approach for ensuring cloud computing security: using data hiding methods. *Sādhanā, 41,* 1289–1298.
9. Kostiuk, Y.V. & Shapran, V.O. (2024) Technologies for Detection of Anomalous Events and Signatures in Real-Time. *"Science and Technology Today" (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Engineering"), 4(32),* 1069–1084.
10. Balbela, J. P. et al. (2023) Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing Advances in Science. *Technology and Engineering Systems Journal, 8(6),* 107–119.
11. Kryvoruchko, O., Kostiuk, Y., & Desiatko, A. (2024) Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods. *Ukrainian Scientific Journal of Information Security, 30(1),* 140–149.
12. Sanagana, D. P. R., & Tummalachervu, C. K. (2024) Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems, *Second International Conference on Data Science and Information System (ICDSIS)*, 1–6.
13. Kostiuk, Y., Bebeshko, B., Kryuchkova, L., Litvinov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information Protection and Data Exchange Security in Wireless Mobile Networks with Authentication and Key Exchange Protocols. Electronic Professional Scientific *Journal "Cybersecurity: Education, Science, Technology*", *1(25),* 229–252.

14. Achbarou, O., El Kiram, M. A., Bourkoukou, O., & Elbouanani, S. (2018) A new distributed intrusion detection system based on multi-agent system for cloud environment. *Int. J. Commun. Netw. Inf. Secur, 10, 526.*
15. Kostiuk, Y., Bebeshko, B., Skladannyi, P., Rzaieva, S., & Khorolska, K. (2025). Buffer and priority optimization for ensuring security in Bluetooth networks. *Information Systems and Technologies Security, 2(8),* 5–16.
16. Kannadhasan, S., Nagarajan, R., & Thenappan, S. (2022) Intrusion detection techniques based secured data sharing system for cloud computing using msvm. *In Proceedings of the 9th International Conference on Computing for Sustainable Global Development (INDIACom),* 50–56.
17. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaieva, S. (2025). Method for protecting GRID environment from malicious code during computational task execution. *Electronic Scientific Journal "Cybersecurity: Education, Science, Technology", 3(27),* 22–40.
18. Hatef, M.A., Shaker, V., Jabbarpour, M.R., Jung, J., & Zarrabi, H. (2025) HIDCC: A hybrid intrusion detection approach in cloud computing. *Concurr. Comput. Pract. Exp, 30, 4171.*
19. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Electronic Scientific Journal "Cybersecurity: Education, Science, Technology", 3(27),* 534–548.
20. Zhang, J., Peter, J.D., Shankar, A., & Viriyasitavat, W. (2024) Public cloud networks oriented deep neural networks for effective intrusion detection in online music education. *Computers and Electrical Engineering, 115.*
21. Skladannyi, P.M., Kostiuk, Y.V., Mazur, N.P., & Pitaichuk, M.A. (2025). Investigation of characteristics and performance of access protocols to cloud computing environments based on universal testing. *Telecommunications and Information Technologies, 1(86),* 61–74.