Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз технічних реалізацій процесів забезпечення безпеки для хмарних обчислювальних сервісів

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Михайловський О.П. (прізвище та ініціали)

Керівник (підпис) Карпінський М.П. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«___» червня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Михайловський Олександр Петрович
(прізвище, ім'я, по батькові)

1. Тема роботи **Аналіз технічних реалізацій процесів забезпечення безпеки для хмарних обчислювальних сервісів**

Керівник роботи **д.т.н., проф. Карпінський М.П.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *квітня* 2023 року № *4/7-349*

2. Термін подання студентом завершеної роботи « » червня 2023 р.

3. Вихідні дані до роботи Літературні джерела з тематики роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
ВСТУП. РОЗДІЛ 1. АНАІЗ ПРОБЛЕМИ ФОРМУВАННЯ ВИМОГ В РОЗПОДІЛЕНИХ КОМАНДАХ 1.1 Критерії відбору 1.2 Виділення характеристик безпеки хмарних обчислень 1.3 Висновки до розділу РОЗДІЛ 2. АНАЛІЗ ПУБЛІКАЦІЙ ВІДПОВІДНО ДО КЛАСИФІКАЦІЇ 2.1 Вразливості, загрози та атаки 2.2 Безпека хмарних сервісів 2.3 Забезпечення безпеки 2.4 Узагальнення результатів огляду літературних джерел РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 3.1 Охорона праці та її актуальність в ІТ-сфері 3.2 Шкідлива дія шуту та вібрації і захист від неї ВИСНОВОК ПЕРЕЛІК ПОСИЛАНЬ

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М.І., к.т.н., доц.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.23-27.01.23	*Виконано*
2.	Підбір джерел по темі роботи	28.01.23 – 01.04.23	*Виконано*
3.	Оформлення першого розділу	15.04.2023	*Виконано*
4.	Оформлення другого розділу	30.04.2023	*Виконано*
5.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи охорони праці»	15.05.2023	*Виконано*
6.	Оформлення кваліфікаційної роботи	07.06.2023	*Виконано*
7.	Перевірка на плагіат	07.06.2023	*Виконано*
8.	Нормоконтроль	09.06.2023	*Виконано*
9.	Попередній захист кваліфікаційної роботи	11.06.2023	*Виконано*
10.	Захист кваліфікаційної роботи	13.06.2023	

Студент _____ Михайловський О.П.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Карпінський М.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз технічних реалізацій процесів забезпечення безпеки для хмарних обчислювальних сервісів // Кваліфікаційна робота освітнього рівня "Бакалавр" // Михайловський Олександр Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. – 62, рис. – 6, табл. – 1, кресл. – 10, додат. – 0, бібліогр. – 70.

Ключові слова: хмарні обчислення, безпека, забезпечення безпеки, реалізація процесів.

Парадигма хмарних обчислень стала основним рішенням для розгортання бізнес-процесів і програм. У загальнодоступному хмарному баченні послуги інфраструктури, платформи та програмного забезпечення надаються споживачам (тобто клієнтам і постачальникам послуг) на основі оплати за використання. Орендарі хмари можуть використовувати хмарні ресурси за нижчими цінами, з вищою продуктивністю та гнучкістю, ніж традиційні локальні ресурси, не турбуючись про керування інфраструктурою. Тим не менш, орендарі хмари залишаються стурбовані рівнем обслуговування хмари та нефункціональними властивостями, на які можуть розраховувати їхні програми.

В останні кілька років дослідницьке співтовариство зосередилося на нефункціональних аспектах парадигми хмари, серед яких виділяється безпека хмари. Дослідження в цій роботі зосереджено на інтерфейсі між безпекою в хмарі та процесами забезпеченням безпеки в хмарі. По-перше, пропонується огляд рівня безпеки в хмарі. Потім подано поняття забезпечення безпеки хмари та аналіз його зростаючого впливу. В роботі наведено ряд рекомендацій стосовно безпеки при використанні хмарних обчислень.

ANNOTATION

Analysis of technical implementations of security processes for cloud computing services // Qualification work of the educational level "Bachelor" // Oleksandr Mykhailovskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department, Group СБ-41 // Ternopil, 2023 // p. – 62, fig. – 6, references – 70, posters – 10, annexes – 0.

Keywords: cloud computing, security, security assurance, processes implementation.

The cloud computing paradigm has become the primary solution for deploying business processes and applications. In the public cloud vision, infrastructure, platform, and software services are provided to tenants (i.e., customers and service providers) on a actually utilized services fee basis. Cloud clients can use cloud resources at lower prices, with higher performance and flexibility than traditional on-premises resources. They do not worry about infrastructure management. However, cloud tenants remain concerned about cloud service levels and the non-functional features their applications can expect.

Recent few years, the major researches was focused on the non-functional aspects of the cloud computing paradigm, with cloud security standing out. The research in this paper focuses on the interface between cloud security and cloud security processes. First, we provide an overview of the current state of cloud security. We then introduce the concept of cloud security and analyze its growing impact. The work gives a number of recommendations regarding security when using cloud computing for development.

ЗМІСТ

ВСТУП

Хмарні обчислення підтримують таке бачення IT, де ресурси та послуги надаються на вимогу на основі оплати за використання. Провайдер надає послуги інфраструктури, платформи та програмного забезпечення, відомі як IaaS, PaaS і SaaS відповідно, зменшуючи зусилля, необхідні для управління обчислювальною інфраструктурою. Досвід показує, що хмара може зробити послуги IT дешевшими, простішими, гнучкими та доступними для кожного, не вимагаючи досвіду, необхідного для володіння, експлуатації та керування традиційними локальними системами. Хмарні клієнти можуть зосередитися на розробці послуг, тоді як хмарні провайдери можуть зосередитися на управлінській діяльності, надаючи інфраструктуру, яка створює у клієнтів ілюзію наявності нескінченних ресурсів.

Незважаючи на те, що хмарні обчислення забезпечують усі ці переваги, багато потенційних користувачів все ще не бажають використовувати їх. Хмарні обчислення фактично змушують постачальників послуг і клієнтів втрачати, принаймні частково, контроль над статусом своїх даних і додатків, погіршуючи їх здатність оцінювати ризики. Відповідно до кількох опитувань, проведених постачальниками послуг хмарних обчислень, постачальниками рішень безпеки та багатьма дослідниками, наприклад, [1, 2, 3], передбачувана відсутність безпеки є однією з головних причин, що перешкоджають клієнтам і власникам бізнесу сприймати хмарні рішення.

За останні кілька років спільнота дослідників безпеки наполегливо працювала, щоб покращити безпеку хмарної інфраструктури та довіру користувачів хмари до того, що їхні програми та інформація правильно керуються та захищаються. Однак поширення спеціальних рішень безпеки, які спрямовані на дуже невелику частину всієї проблеми, ускладнює справедливу та обґрунтовану оцінку сучасного рівня безпеки в хмарі. Тут ми виходимо з уявлення про те, що парадигму хмарних обчислень можна повністю

використовувати, лише якщо розширити участь клієнтів і постачальників послуг в управлінні безпекою, підвищивши їх довіру.

Слідуючи цьому поняттю, методи забезпечення безпеки програмного забезпечення підвищують прозорість хмари, а також підвищують впевненість споживачів послух хмари в тому, що хмарні служби поводяться, як очікувалося. Згідно зі стандартними визначеннями гарантії безпеки програмного забезпечення, гарантію безпеки хмари можна визначити як спосіб отримати обґрунтовану впевненість у тому, що інфраструктура та/або програми постійно демонструватимуть одну або більше властивостей безпеки та працюватимуть належним чином, незважаючи на збої.

Гарантія (забезпечення) безпеки є набагато ширшим поняттям, ніж власне сама безпека, оскільки включає методології для збору та перевірки доказів, що підтверджують властивості безпеки. У цьому дослідженні ми аналізуємо сучасний рівень безпеки в хмарі, зосереджуючись на появі гарантії безпеки в хмарі (для стислості – хмарна гарантія). Ми визначаємо таксономію хмарної безпеки/забезпечення та надаємо аналіз

і) методів хмарної безпеки та

іі) відповідних процесів гарантії.

Також подається огляд результатів дослідження разом з наведенням певних рекомендацій щодо проектування та розробки методів безпеки/забезпечення хмарної безпеки наступного покоління.

РОЗДІЛ 1. АНАІЗ ПРОБЛЕМИ ФОРМУВАННЯ ВИМОГ В РОЗПОДІЛЕНИХ КОМАНДАХ

1.1 Критерії відбору

У поточній стверджується, що розробка хмарної парадигми включає три основні фази. На першому етапі відбувається налаштування хмарної інфраструктури та здійснюється проектування та розробка всіх функціональних аспектів хмари. Результати цих зусиль призвели до впровадження поточних стеків хмарних протоколів.

Другий етап реалізовує перехід від функціональних до нефункціональних властивостей і включає проектування та розробку методів керування хмарною безпекою, надійністю та продуктивністю.

Третя фаза охоплює розробку чи адаптацію процесів гарантування безпеки. Методи гарантування для хмари спрямовані на перевірку, підтвердження та забезпечення нефункціональних властивостей хмарних процесів і програм. У цій роботі представлено огляд підходів до хмарної безпеки та надійності, визначаючи існуючі тенденції та висвітлення прогалин, які необхідно усунути, щоб сприяти прийняттю хмари в критичних для безпеки сценаріях. Враховуючи величезну кількість літератури, ми визначили наступний набір критеріїв відбору.

– Охоплення: відбір джерел був максимально широким. Розглянуто рішення безпеки, які задовольняють усі вимоги безпеки, пов’язані з хмарою, і обговорено механізми безпеки для всіх рівнів стеку хмарних протоколів.

– Практичність: публікації були відібрані на основі впливу на конкретні рішення та кінцеві продукти. Цей вибір дозволив визначити, що сьогодні можна реально реалізувати та інтегрувати в реальні системи.

– Своєчасність: відбір публікацій для аналізу стосувався останніх двадцяти років, щоб зробити аналіз актуальним. Рішення, представлені на початку епохи

хмарних обчислень, насправді могли бути нестабільними або незастосовними в поточних хмарних середовищах.

– Якість: вибір статей здійснювався за суворою оцінкою якості. З цією метою наукові та архівні публікації були привілейованими, надаючи перевагу статтям у журналах і конференціях ACM, IEEE та Elsevier.

1.2 Виділення характеристик безпеки хмарних обчислень

Окрім дотримання обґрунтованих критеріїв відбору, дослідження має реалізувати організацію відібраного матеріалу наукових публікацій. Ми почали з визначення деяких ключових аспектів безпеки та впевненості, що відповідають основним властивостям безпеки [4]. Початково задачу реалізації процесів безпеки можна поділити на три аспекти (рис. 1.1):

– аналіз вразливостей;
– механізми безпеки хмарних обчислень;
– гарантування безпеки.

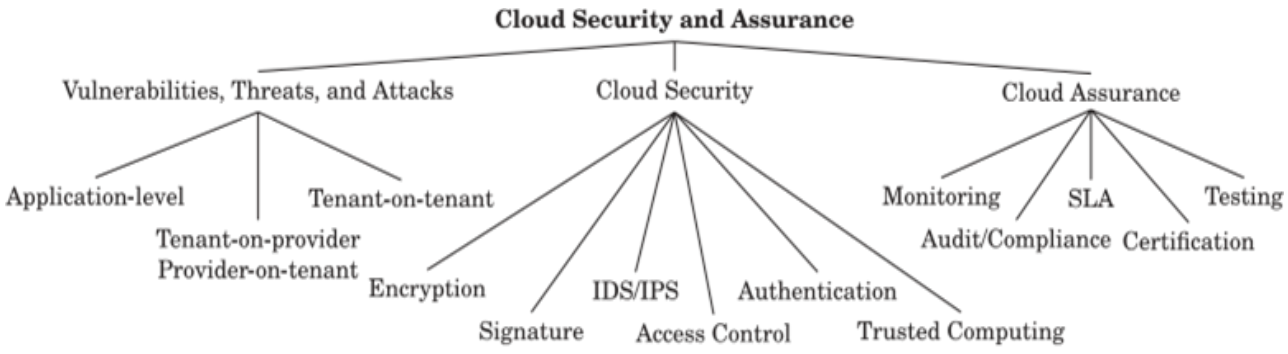

Рисунок 1.1 – Таксономія забезпечення безпеки хмарних обчислень

Атаки на безпеку додатково уточнюються в трьох областях шляхом визначення поверхні атаки:

1) рівень прикладної програми, де атаки можуть здійснюватися будь-яким учасником хмари та націлені на рівень SaaS, включаючи його служби та дані;

2) орендар на клієнта, де атаки здійснюються зловмисними хмарними орендарями на інших хмарних орендарів і спрямовані на рівні PaaS та IaaS, включаючи їхні ресурси, процеси та дані;

3) постачальник на клієнта та орендар на постачальника, де атаки здійснюються зловмисними хмарними постачальниками (відповідно орендарями) на цільових орендарів (відповідно хмарних постачальників) і спрямовані на рівень IaaS, включаючи його ресурси, процеси, і дані.

Класифікація методів безпеки додатково уточняється в шести областях залежно від реалізованих механізмів безпеки:

1) шифрування;

2) сигнатура;

3) система виявлення вторгнень (IDS)/система запобігання вторгненням (IPS);

4) контроль доступу;

5) автентифікація;

6) довірені обчислення.

Методи забезпечення безпеки в хмарі можуть використовуватися на всіх рівнях хмарного стеку, щоб підтвердити заявлені характеристики безпеки, зроблені постачальником щодо його механізмів безпеки, і можуть бути додатково вдосконалені в п’яти сферах:

1) тестування;

2) моніторинг;

3) сертифікація;

4) аудит/відповідність;

5) угода про рівень обслуговування (SLA).

Усі області спрямовані на підвищення довіри користувачів до хмари та надання їм більшої можливості оцінювати стан безпеки хмарного стеку, де зберігаються їхні програми/дані.

Крім того виконувався аналіз публікацій по просторово-часових характеристиках. Поточний аналіз визначає, коли, де, що та як рішення безпеки та надійності зміцнюють середовище хмарних обчислень.

1.3 Висновки до розділу

Отже, у цьому розділі розглянуто низку дослідницьких робіт щодо вразливостей, загроз і атак, розрізняючи їх на основі цілей атак у відповідності до класифікації на рисунку 1.1.

Перш за все, слід відзначити, що проаналізовані публікації зосереджені на атаках на рівні додатка та клієнгт-клієнт. Це пов’язано з тим фактом, що, з одного боку, атаки на рівні додатків розглядали з моменту появи Інтернету, а отже, відповідні вразливості, загрози та атаки були застосовані з моменту появи хмарних обчислень; з іншого боку, атаки ипу клієнт-клієнт розглядалися в кількох роботах, спрямованих на захист віртуалізованих середовищ, які можна розглядати як попередників поточних хмарних систем. Атаки постачальника на клієнта та клієнта на постачальника є специфічною для хмари і тому менш досліджена, хоча інтерес до неї зростає в контексті атак на конфіденційність і приватність даних клієнтів і доступності хмарних інфраструктур.

РОЗДІЛ 2. АНАЛІЗ ПУБЛІКАЦІЙ ВІДПОВІДНО ДО КЛАСИФІКАЦІЇ

2.1 Вразливості, загрози та атаки

Після моделювання хмари як набору з трьох сутностей, включаючи користувачів, служби та постачальників хмарних сервісів, можна визначити кожну атаку як набір взаємодій у цій моделі. По-перше, атаки, спрямовані на взаємодію між користувачами та службами, схожі на атаки, відомі для традиційних розподілених комунікацій (наприклад, відмова в обслуговуванні – DoS, SQL-ін’єкції, кроссайтові скрипти – XSS). Однак атаки, властиві хмарному середовищу, також стосуються інтерфейсів, якими керує провайдер хмари. Потім вони визначають шість поверхонь атаки, які використовуються, можливо, у комбінації, для виконання атаки.

Тут ми застосовуємо підхід до моделювання загроз, класифікуючи публікації про вразливості, загрозах та атаках: на рівні додатка, на рівні клієнт-клієнт та на рівні провайдер-клієнт / клієнт-провайдер.

2.1.1 Рівень програми

Вразливості, загрози та атаки на рівні додатків загрожують інфраструктурі інформаційно-комунікаційних технологій з перших днів Інтернету, і вони в основному спрямовані на взаємодію між користувачами та службами. Іншими словами, вони зосереджуються на послугах і даних на найвищому рівні хмарного стеку та розглядають модель обслуговування SaaS. Далі ми надаємо огляд вразливостей, загроз і атак, які зосереджені на хмарі та її особливостях.

В праці [6] демонструють слабкість у службі керування Amazon EC2 на основі SOAP проти атак із загортанням підпису. Зловмисник зміг модифікувати перехоплене повідомлення, підробивши алгоритм перевірки сигнатури, і

виконував команди від імені легальних користувачів. У [6] представляють проблеми безпеки в хмарних обчисленнях, враховуючи XML-підпис, безпеку браузера, цілісність хмари та лавинні атаки. Автори також представляють атаку з ін'єкціями зловмисного програмного забезпечення у хмару, коли зловмисний користувач намагається додати реалізацію служби та заплутати хмарного постачальника, дозволяючи йому вважати зловмисну службу звичайною. Автори пропонують нову методологію для аналізу публічних хмарних інтерфейсів і обговорюють можливі засоби протидії виявленим атакам. Автори [7] зосереджують увагу на двох атаках, які можуть бути спрямовані на хмару, а саме на відмову в обслуговуванні HTTP та відмову в обслуговуванні на основі XML. Зокрема, вони відтворюють вищезазначені атаки, представляють рішення для визначення джерела атаки та запроваджують підхід для виявлення та фільтрації цих атак. В принципі, цей вид атак також може застосовуватися до поверхонь для атак типу «клієнт-клієнт».

2.1.2 Рівень клієнт-клієнт

Уразливості, загрози та атаки між клієнтами типові для віртуалізованих середовищ, де різні орендарі мають спільну інфраструктуру та можуть розміщуватися на одному фізичному обладнанні. Дослідники, які працюють у цій галузі, в основному розглядають сценарії, коли зловмисний клієнт намагається атакувати інших клієнтів, розташованих на тому ж обладнанні, використовуючи неправильну конфігурацію та вразливі місця в інфраструктурі віртуалізації (наприклад, ізоляцію віртуальної машини (VM)). Іншими словами, уразливості, загрози та атаки від клієнта на клієнта зосереджуються на ресурсах, процесах і даних на найнижчих рівнях хмарного стеку та розглядають моделі обслуговування PaaS та IaaS. Далі подано огляд праць, які зосереджуються на атаках від клієнта до клієнта.

Автори [8] описують атаку на конфіденційність інформації запущених екземплярів служби. Їхня атака базується на тому факті, що віртуальна машина зловмисника та цільова служба знаходяться на одному апаратному забезпеченні, і тому перша може розпочати атаку, генеруючи трафік і відстежуючи власну (або гіпервізорів) продуктивність. Автори [9] обговорюють проблему каналів синхронізації в хмарі та представляють підхід до запобігання атак синхронізації, заснований на детермінованому виконанні провайдера. У роботі [10] представляють атаку стороннього каналу, яка дозволяє зловмисним віртуальним машинам викрасти особисту інформацію цільової віртуальної машини, що працює в тій самій віртуальній мережі на основі гіпервізора Xen. Автори [11] спочатку аналізують стан вразливостей стороннього каналу, пов'язаного з кеш-пам'яттю центрального процесора, потім визначають недоліки існуючих засобів захисту при застосуванні в хмарі та, нарешті, представляють серверне рішення для пом'якшення атак такого типу.

2.1.3 Рівень провайдер-клієнт та клієнт-провайдер

Вразливості, загрози та атаки від провайдера на клієнта і клієнта на провайдера характерні для хмари, де користувачі, підприємства та власники бізнесу переміщують свої активи в ненадійну інфраструктуру. Дослідники, які працюють у цій галузі, в основному розглядають сценарії, коли хмарний провайдер є зловмисним (або, принаймні, чесним, але цікавим) і атакує своїх клієнтів. Крім того, вони розглядають контексти, в яких один або кілька скомпрометованих клієнтів (наприклад, ботнети для атак на відмову в обслуговуванні) використовуються для атаки на хмарну інфраструктуру (клієнт-провайдер). Іншими словами, уразливості, загрози та атаки постачальників на клієнтів і навпаки зосереджені на ресурсах, процесах і даних, що надаються за допомогою моделі обслуговування IaaS. Далі ми надаємо огляд праць, які

зосереджуються на поверхні атаки постачальника на клієнта та клієнта на провайдера.

В роботі [12] представлено нову форму атаки на відмову в обслуговуванні, яка націлена і насичує пропускну здатність віртуальної мережі. Очевидно, що цей тип атаки також може бути запущений на рівні програми, де метою атаки є дана програма на певній машині. В [13] автори представляють огляд загроз конфіденційності хмари, створених зловмисними інсайдерами (до яких можна включати постачальника хмарних послуг), обговорюють можливі механізми захисту та описують їх обмеження. Робота [14] описує проблему захисту клієнта від атак з боку хмарних провайдерів, також враховуючи сценарій, що включає зловмисних аутсайдерів (атаки типу клієнт-клієнт). Зокрема, вони розглядають проблему захисту криптографічних операціїв, оскільки провайдери можуть отримати доступ до збережених ключів, а споживачі не мають права розгортати свої ключі лише під час виконання. Потім автори визначають архітектуру, що реалізує керовану клієнтом криптографію як послугу (CaaS). CaaS надає домен виконання для клієнта, де всі операції шифрування захищені та керовані.

2.2 Безпека хмарних сервісів

Проблеми хмарної безпеки є дуже складними через:

1) неоднорідність хмарних стеків;

2) відсутність формальних і семантично еквівалентних вимог безпеки (які часто відрізняються залежно від розглянутої області);

3) відсутність стабільної категоризації методів ;

4) потреба в балансі між безпекою, гнучкістю та високою продуктивністю;

5) відсутність прозорості щодо дій і подій, що відбуваються в хмарі.

Багато дослідницьких робіт представляють часткові, спеціальні рішення, кожна з яких стосується невеликої частини проблеми. Ця ситуація ускладнює загальну оцінку сучасного рівня безпеки в хмарі. Додаткові ускладнюючі

фактори включають потенційне втручання між механізмами безпеки на різних рівнях хмарного стеку.

У цьому розділі ми представляємо огляд хмарних рішень безпеки. Підходи до класифікації хмарної безпеки обрано згідно рисунком 1.1: шифрування, сигнатура, контроль доступу, IDS/IPS, автентифікація, довірені обчислення.

2.2.1 Шифрування

Перший напрямок дослідження спирається на методи шифрування для підвищення безпеки хмари шляхом захисту даних, зв’язку та дій у хмарі від зловмисників, які прагнуть порушити нормальну роботу хмари, зменшуючи доступність хмарних служб та/або виводячи/доступ до секретних даних хмарних орендарів та їх діяльності.

Більшість публікацій пропонують методи шифрування для досягнення конфіденційності, а також націлені на додаткові властивості, такі як цілісність, доступність, автентичність і конфіденційність. У роботі [15] автор представив High-Availability and Integrity Layer (HAIL) – систему, яка підтримує цілісність файлів даних і доступність на різних серверах або незалежних службах зберігання. HAIL використовує підхід підтвердження можливості відновлення для тестування віддалених серверів зберігання та заміни їх у разі виявлення збоїв. Автори в роботі [16] описали різні можливі архітектури конфіденційності та запропонували компонент менеджера конфіденційності для підвищення захисту приватних даних за допомогою обфускації на основі шифрування. Вони також надали зразок програми, спрямованої на захист метаданих спільних фотографій.

У [17] автори розробили захищене сховище для підтримки не лише безпеки та цілісності даних, але й доступності та відмовостійкості, а в [18] автори представили комбінацію повторного шифрування проксі та децентралізованого

коду стирання для формування надійне сховище, яке забезпечує конфіденційність, приватність і доступність.

Автори в роботі [19] представляють підхід, заснований на довіреній третій стороні (TTP) для захисту програм користувача. TTP відповідає за безпечне встановлення довірчої сітки між об'єктами, що утворюють хмарні сузір'я. Третя сторона використовується для гарантії конфіденційності, цілісності та автентичності спільної інформації та повідомлень.

У роботі [20] розглянуто проблему безпечного резервного копіювання ключів шифрування для:

1) підвищення безпеки та доступності даних;

2) зменшення ризику втрати даних через недоступність ключів;

3) обмеження ризику розкриття ключа та порушення конфіденційності.

Автори представляють схему під назвою відновлюване шифрування за допомогою шумового секрету, яка дозволяє зберігати резервні копії ключів на одній машині та є стійкою до дешифрування за допомогою атак грубої сили. Насправді розшифровка займає багато обчислень і часу.

У [21, 22] автори зосереджуються на міграції корпоративних даних у публічну хмару, зберігаючи при цьому рівень довіри та видимість щодо правильності операцій орендарів. Їхній підхід базується на криптографічних протоколах і спрямований на забезпечення надійного захисту переміщених даних. Він покладається на структуру аудиту для перевірки внутрішніх властивостей хмари та забезпечення бажаного рівня впевненості в тому, що корпоративні дані керуються з метою збереження безпеки та надійності.

Робота [23] описує структуру під назвою BigSecret для безпечного аутсорсингу та захисту зашифрованих даних у сховищах ключ-значення. BigSecret надає три моделі шифрування в основі підходу, що підтримує:

1) безпечне керування даними в напівнадійних постачальників;

2) запити до зашифрованих даних.

Моделі використовують криптоіндекси на основі сегментації або псевдовипадкових функцій і дозволяють операції видалення, отримання та сканування над зашифрованими даними. BigSecret також забезпечує евристику, що підтримує безпечний розподіл даних і робочих навантажень для підвищення продуктивності та ефективності. Він розглядає хмарний сценарій, що складається з кількох провайдерів з грошовими обмеженнями та ризиками розкриття інформації.

У [24] пропонують протокол для безпечного аутсорсингу даних у хмару. Протокол, заснований на схемі шифрування на основі атрибутів, механізмі групового ключа та повторному шифруванні, захищає дані від хмарного постачальника. Він підтримує відкликання та дозволяє користувачам із потрібними атрибутами отримувати доступ до даних. Протокол також розроблено для підтримки мобільних пристроїв з обмеженими ресурсами, делегуючи обчислення постачальнику хмарних послуг третім сторонам.

Методи шифрування також використовувалися виключно для забезпечення властивостей, відмінних від конфіденційності. Наприклад, в [25] представлено проміжне програмне забезпечення під назвою CloudProtect, яке забезпечує функції шифрування для захисту конфіденційності даних у хмарі. CloudProtect реалізує набір функціональних можливостей, прозорих для додатків, які дозволяють зберігати зашифровані дані в постачальника послуг і працювати безпосередньо з ними, коли це можливо. У разі необхідності відкритих текстових даних CloudProtect реалізує протокол, який надає доступ до них протягом обмеженого періоду часу.

В статті [25] автори представляють протокол, який дозволяє програмам зі збігом шаблонів отримувати доступ до даних також у зашифрованій формі. Їхній підхід заснований на оцінці детермінованого файлового автомата на зашифрованому файлі, що зберігається в хмарі. Підхід дозволяє клієнту ідентифікувати будь-яку неправильну поведінку хмарного постачальника.

2.2.2 Сигнатури

Деякі підходи використовують сигнатури на основі шифрування для підтримки цілісності, конфіденційності або обох властивостей. Зокрема в статті [26] автор представляє сервіс Venus, який робить взаємодію користувачів із ненадійним хмарним сховищем більш безпечною. Venus забезпечує цілісність і узгодженість програм за допомогою служби зберігання об’єктів на основі ключів, яка не вимагає довірених компонентів або змін у провайдерові сховища. У статті [28] представлено схему мультисекретного обміну, засновану на блочній криптографії, секретному обміні та хеш-функціях, у якій використовуються два типи підписів для підтримки доступності та цілісності даних. Перший – це внутрішній підпис, створений з усіх даних у кожному спільному блоці даних, який використовується для перевірки цілісності даних. Другий – зовнішній підпис, створений з кожного зашифрованого блоку даних, який дозволяє швидко ідентифікувати та виправляти помилкові блоки даних і зберігати доступність даних.

Автори у статті [28] визначають рішення, засноване на посереднику безпеки, який реалізує анонімний підхід до перевірки цілісності хмарних даних. Метадані перевірки на основі підписів використовуються для надання анонімних доказів володіння даними. Крім того, посередник безпеки не дізнається інформацію про дані, завантажені в хмару.

В [29] автори пропонують протокол аудиту для запобігання обману конфіденційності. Їхня пропозиція базується на пакетній перевірці, а також на спеціальних механізмах імовірнісної вибірки. Робота [30] заснована на підписах, але не спрямована на цілісність і конфіденційність. Автори представляють програмне забезпечення Service Signature (S3) – рішення, яке спрямоване на вирішення проблем вільного використання SaaS, де зловмисники можуть намагатися максимізувати свої переваги у використанні сервісу. Основна ідея S3 полягає в тому, щоб підвищити безпеку за допомогою автентифікації за

допомогою проксі-підпису, щоб запити на обслуговування завжди можна було перевірити.

2.2.3 Управління доступом

Існуючі системи контролю доступу для розподілених середовищ безпосередньо не застосовуються до хмари. Як наслідок, дослідницьке співтовариство визначило нові підходи до контролю доступу в хмарі. Ми розглядаємо їх у цьому розділі разом із рішеннями безпеки, які:

1) реалізують механізми авторизації;

2) використовують підходи моніторингу, щоб розрізнити безпечний і зловмисний доступ до хмарних ресурсів.

Отже, представником першого пункту є робота [31] представив рішення для автоматизації та конфігурації політики безпеки та відповідності. Вони підтримували створення технічної політики відповідно до трансформації, керованої моделлю. Крім того, вони надали підхід до звітування про інциденти та керування авторизаціями додатків. Надається реалізація на основі OpenPMF, повноцінного продукту безпеки на основі моделі, що підтримує моделювання, автоматичне створення, примусове виконання, моніторинг і автоматичне оновлення політик.

Період десятирічної давнини був періодом інтенсивних досліджень контролю доступу до хмари. Так, в роботі [32] автори представляють метод контролю доступу на основі політики, який спирається на вибіркове шифрування з гарантованим видаленням файлів. Їхній підхід використовує набір операцій шифрування, які обслуговуються набором незалежних менеджерів ключів, кількість яких перевищує заданий поріг. Автори в статті [33] надають підхід тимчасового контролю доступу для хмари, який пов’язує політику доступу щодо тимчасових атрибутів з кожним зовнішнім ресурсом. У їхньому підході повторне

шифрування проксі-сервера використовується для відповідності політикам доступу та атрибутам користувача в запиті на доступ.

Публікація [34] пропонує рішення, спрямоване на захист приватної інформації в політиках контролю доступу, а також моделі доступу користувачів від цікавих очей постачальника хмарних послуг. Автори визначають систему контролю доступу, яка працює на двох рівнях:

1) на стороні хмари, використовуючи грубе керування доступом для обмеження обсягу інформації, доступної хмарному провайдеру;

2) на стороні клієнта, використовуючи детальне вибіркове шифрування доступу для гарантування належного рівня виразності.

У [35] автори пропонують схему контролю доступу на основі ієрархічного шифрування на основі набору атрибутів (HASBE) з користувачами, організованими в ієрархічну структуру.

В роботі [36] оцінили придатність контролю інформаційних потоків (IFC), підходу обов'язкового контролю доступу, для захисту хмарних інфраструктур. Вони представили різні рішення IFC і децентралізовані IFC (DIFC), головним чином зосереджені на рівні PaaS (який вважається найбільш прийнятною моделлю для інтеграції DIFC), і оцінили проблеми та виклики впровадження IFC і DIFC у хмарних сценаріях.

В [37] автори представили децентралізовану схему контролю доступу для безпечного зберігання даних у хмарах, яка здатна перевірити автентичність наданої інформації без необхідності знати особу користувача, а також облікові дані авторизації (так звані макаруни) для хмарних служб, що підтримують децентралізоване делегування на основі вкладених і ланцюжкових кодів автентифікації повідомлень (MAC).

2.2.4 Аутентифікація

Також було виконано певну роботу щодо додавання автентифікації та керування ідентифікацією в хмару.

В роботі [38] автори представили TrustCube – підхід, що підтримує керування автентифікацією в хмарі для мобільних користувачів. TrustCube надає незалежну платформу на основі політики для хмарної автентифікації, яка об’єднує низку методів автентифікації.

Пізніше у публікації [39] було представлено огляд питань безпеки та конфіденційності в хмарі з акцентом на керуванні ідентифікацією та доступом (IAM), життєвому циклі IAM, а також стандартах і протоколах IAM (наприклад, мова розмітки формування безпеки). (SAML), протокол відкритої автентифікації (OAuth).

Колектив авторів в роботі [40] пропонує проект ієрархічної архітектури для хмарних обчислень, яка використовує криптографію на основі ідентифікації для підтримки як конфіденційності даних, так і автентифікації користувача.

В роботі [41] представлено протокол автентифікації та авторизації, який плавно інтегрується з системою керування ідентифікацією (IDMS) для збереження конфіденційності користувачів. Згідно з підходом авторів, анонімність забезпечується в протоколі автентифікації та авторизації шляхом заміни справжніх ідентифікацій користувачів анонімними ідентифікаційними даними та ключами, створеними та керованими IDMS.

2.2.5 Довірені обчислення

Довірені обчислення покладаються на модулі довіреної платформи (TPM) і відповідне апаратне забезпечення для підтвердження цілісності програмного забезпечення, процесів і даних. Однак поява хмари потребує адаптації апаратного TPM до віртуалізованих середовищ.

Фундаментальною є [42], яка визначає приватну віртуальну інфраструктуру для розподілу відповідальності між користувачами та провайдерами хмари та зниження загального ризику впливу. Запропонований підхід базується на понятті віртуального довіреного модуля платформи (vTPM), який забезпечує безпечне зберігання та криптографічні функції TPM для програм і операційних систем, що працюють у віртуальних машинах. vTPM складається з екземплярів vTPM, кожен з яких пов'язаний з віртуальною машиною, якій потрібні функції TPM, і менеджера vTPM, який створює екземпляри vTPM і мультиплексує запити, що надходять від віртуальних машин.

Автори у своїй статті [43] використовують довірені обчислення для вирішення проблем безпеки реплікації ВМ, яка запускається для покращення доступності даних і послуг у хмарі.

Не всі надійні обчислювальні методи, застосовні до хмари, базуються на шифруванні. Наприклад, платформа MyCloud, що реалізує архітектуру для захисту конфіденційності, відходить від традиційних механізмів шифрування [44]. MyCloud максимально зменшує довірену обчислювальну базу (наприклад, виводить контроль над віртуальними машинами за межі своєї сфери) і дозволяє клієнтам налаштовувати свій захист конфіденційності, одночасно зменшуючи можливість постачальника хмарних послуг змінювати параметри конфіденційності.

2.2.6 IDS/IPS

Доступність обчислювальних ресурсів як товарів на вимогу робить хмару потужною зброєю в руках зловмисників, які можуть використовувати ресурси хмари для атак (наприклад, розподілена атака на відмову в обслуговуванні (DDoS)), і інструментом в руках експертів з безпеки, які можуть використовувати хмарні ресурси для розгортання IDS та IPS. В роботі авторів [45] розглянуnj різні атаки, що впливають на доступність, конфіденційність і

цілісність, і розглянули підходи до забезпечення IDS та IPS у хмарі. Автори зосереджуються на інсайдерських атаках, атаках flooding, атаках користувача на root, скануванні портів, атаках на гіпервізор або віртуальні машини та атаках на бекдор-канал. Потім вони представляють еволюцію IDS і IPS і пояснюють, як IDS і IPS використовувалися для підвищення безпеки хмари. Автори також представляють класифікацію існуючих підходів IDS (Таблиця 2.1), обговорюючи їхні переваги та недоліки.

Таблиця 2.1 – Класифікація систем IDS

Назва	Використана техніка	Позиціонування	Плюси	Мінуси
Архітектура IDS для Хмарного середовища	Виявлення на основі сигнатур і виявлення аномалій за допомогою нейронних мереж.	На кожному вузлі	Швидкість помилок для невідомої атаки нижча, оскільки використовується ANN.	Вимагає більше часу навчання та зразків для точності виявлення.
IDS, сумісні з архітектурою віртуальних машин	Виявлення на основі сигнатур	На кожній ВМ	Безпечна віртуальна машина на основі конфігурації користувача.	Необхідно кілька екземплярів IDS, що погіршує продуктивність.
Виявлення DDoS атак на віртуальній машині	Виявлення на основі сигнатур	На кожній ВМ	Захищає віртуальну машину від DDoS-атак.	Може виявляти лише відомі атаки, оскільки використовується лише snort.
NIDS у хмарі з відкритим кодом	Виявлення на основі сигнатур	У традиційній мережі	Може виявити кілька відомих атак.	Він не може виявити інсайдерські атаки, а також відомі атаки, оскільки використовується лише snort.
Підхід на основі кооперативних агентів	Виявлення на основі сигнатур	На кожній хмарі область	Запобігання одноточкової відмови системи.	Не можна використовувати для всіх типів атак. Високі накладні витрати на обчислення.
Підхід на основі мобільного агента	Виявлення аномалій	На кожній ВМ	Надає IDS для хмарних додатків незалежно від їх місцезнаходження.	Створення навантаження на мережу зі збільшенням віртуальних машин, підключених до МА.
Архітектура на основі VMI-IDS	Виявлення аномалій	На гіпервізорі	Виявляти атаки на віртуальні машини.	VMI IDS може бути атаковано. Дуже складний метод.
Брандмауер на основі Xen	Профілактика	На кожному хості	Запобігання за допомогою налаштованих користувачем правил.	Не використовується для запобігання невідомим атакам.
Підхід на основі CP	Виявлення аномалій	–	Використовується для виявлення всіх видів атак. Усуває обмеження часу обчислення.	Жодних експериментальних результатів не показано.

Нижче подано деякі підходи до виявлення та запобігання вторгненням у хмарі.

Стосовно традиційного IDS в [46] розглядають важливий аспект хмарної безпеки, а саме безпеку віртуальних машин (ВМ), на яких розгортаються хмарні служби та функції. Вони пропонують підхід до посилення інтроспекції ВМ і забезпечити архітектуру, що гарантує віртуалізовані навантаження клієнтів. Цей підхід не передбачає цілісності віртуальних машин. У роботі також описується служба виявлення та відновлення руткітів, що працює поза віртуальною машиною, як застосування представленого підходу до самоаналізу.

В [47] пропонують багаторівневу систему виявлення вторгнень, яка перевіряє інформацію про автентифікацію користувачів і застосовує до них різні рівні безпеки залежно від ступеня аномалії. Рівень аномалії користувачів визначається на основі їх конфігурації (наприклад, IP-покриття та вразливі порти), а потім регулярно оновлюється на основі їхньої поведінки під час використання хмари.

Розглядаючи IPS, автори [48] представляють туманне обчислення, рішення для пом’якшення атак крадіжки даних з боку інсайдерів у хмарі. Їхня пропозиція базується на технології приманки, яка запускає дезінформаційну атаку, коли за допомогою моніторингу виявляється внутрішня атака. В [49] автори визначають рішення для розподілу ресурсів на основі серверів запобігання вторгненням, що дозволяє протидіяти DDoS-атакам. Пропоноване рішення зосереджено на захисті серверів, уразливих до DDoS-атак; з цією метою використовуються різні сервери запобігання вторгненням, щоб відрізнити зловмисний трафік від звичайного, спрямованого на атаковану сутність. Змінні поверхні атак також використовувалися як стратегія пом’якшення атак.

2.2.7 Узагальнення огляду методик забезпечення безпеки в хмарі

У цьому розділі розглядається набір документів, головною метою яких є визначення нових підходів до посилення безпеки хмари проти різних загроз, вразливостей і атак.

Перш за все, відповідно до результатів попередніх досліджень, виявлено, що конфіденційність і цілісність все ще є найбільш дослідженими категоріями властивостей. Більшість рішень зосереджено на методах шифрування та системах контролю доступу. Однак останнім часом зросла кількість досліджень щодо IDS/IPS і довірених обчислень, а також досліджень, спрямованих на захист конфіденційності споживачів хмарних сервісів. Ми також зауважимо, що хоча методи підпису часто використовуються для посилення безпеки, вони переважно використовуються разом з іншими методами. Дослідження доступності було метою невеликої кількості робіт, зосереджених на DDoS-атаках. Цей висновок головним чином пояснюється тим фактом, що доступність часто розглядається як властивість на межі між областями досліджень безпеки, надійності та продуктивності.

2.3 Забезпечення безпеки

Прогрес у дослідженнях хмарної безпеки сприяв розробці методів гарантії, що підвищує впевненість користувачів у тому, що хмарний стек і його служби відповідають їхнім нефункціональним вимогам. Як обговорювалося вище, гарантування безпеки є набагато ширшим поняттям, ніж власне безпека, визначена багатьма джерелами як «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення».

Дійсно, у хмарі цілком можливо мати хорошу безпеку та низьку надійність, як, наприклад, коли роботу надійних механізмів безпеки не видно користувачам.

Однак часто погана гарантія йде поруч з поганою безпекою. Що ще важливіше, погана гарнтія зазвичай не дозволяє довести, що властивості безпеки та конфіденційності процесу відповідають законам і нормам.

Концепція прозорості, тобто вищий доступ до низькорівневих (back-end) даних, створених хмарною інфраструктурою, і до доказів, зібраних щодо безпеки хмарних даних і програм, була визнана основою для ефективного підходу до забезпечення безпеки хмарних сервісів [50, 51]. Відсутність прозорості фактично робить хмару та її проблеми безпеки незрозумілими для кінцевих користувачів. Загрози безпеці вимагають від клієнта хмари шукати більше прозорості та контролю. Угоди про рівень обслуговування та контракти не надають технічного та вимірюваного методу визначення статусу контролю безпеки хмарних додатків/даних. Вони представляють підхід, що підтримує вимірювання стану безпеки системи. Зокрема, вони пропонують систему вимірювання безпеки (Security Management System – SMS), яка взаємодіє з хмарними додатками для отримання метричної інформації.

Є три основні аспекти, які слід враховувати для забезпечення безпеки бізнесу, який переходить у хмару:

1. Існує потреба в рішенні для оцінки та управління ризиками, оцінки впливу переходу в хмару на бізнес.
2. Прозорість, тобто клієнти хмари повинні бути добре обізнані про практику хмарних провайдерів.
3. Політика та відповідність стають обов’язковими.

Хмарні провайдери, дотримуючись вимог прозорості, повинні не лише демонструвати свою відповідність стандартам/регуляціям і підтримуваним політикам, але також пояснювати, як вони досягають і підтримують свої рівні відповідності згідно з принципом «виконуй або поясню» [52]. Концепція прозорості вводиться як спосіб документувати, оцінювати та спостерігати за технічним контролем (наприклад, аудит, контроль доступу, конфігурація системи, шифрування), управлінським контролем (наприклад, оцінка

вразливості, оцінка ризику, система та отримання послуг) і операційний контроль (наприклад, управління конфігурацією, обізнаність і навчання, управління змінами).

Крім того, прозорість має на меті забезпечити надійну хмарну службу, яка оцінює постачальників хмарних послуг та їхню надійність. У цьому контексті CloudTrust Protocol (CTP) – це механізм під керуванням користувача, який дозволяє йому запитувати та отримувати інформацію про інфраструктуру хмарного провайдера. За даними [53] прозорість є фундаментальною для підтримки як інтроспекції, тобто здатності постачальника хмари досліджувати та спостерігати за своїми внутрішніми процесами, так і аутроспекції, тобто здатності клієнтів і постачальників послуг досліджувати та спостерігати за внутрішніми процесами хмари, залучення їх діяльності, даних і програм з метою безпеки.

Належне рішення для забезпечення гарантій у хмарімає охоплювати як самоаналіз постачальників хмари, так і зовнішню перевірку клієнтів хмари (загалом орендарів) і, отже, збалансувати тягар процесів безпеки та контролю між постачальниками та клієнтами.

У цьому розділі ми розглядаємо підходи до верифікації та перевірки хмарних інфраструктур. Підходи до хмарної гарантії класифіковано відповідно до зображення на рисунку 1.1:

– тестування,
– моніторинг,
– сертифікація,
– аудит/відповідність
– SLA.

Ці категорії рішень спрямовані на підвищення довіри до хмарної інфраструктури, можуть бути націлені на всі рівні хмарного стеку та націлені на розширення можливостей користувачів хмари.

2.3.1 Тестування

Перший клас підходів до валідації та перевірки програмного забезпечення та послуг базується на тестуванні. Згідно з глосарієм ISTQB [54], тестування – це «процес, що складається з усіх дій життєвого циклу, як статичних, так і динамічних, пов’язаних із плануванням, підготовкою та оцінкою програмних продуктів і пов’язаних робочих продуктів, щоб визначити, чи вони задовольняють заданим вимогам, щоб продемонструвати що вони придатні для призначення та для виявлення дефектів».

Підходи, засновані на тестуванні, можуть бути застосовані на всіх рівнях хмарного стеку та можуть бути використані, щоб гарантувати, що певна властивість забезпечується певною хмарною службою/функцією. Зазвичай методи тестування в хмарі можна згрупувати в дві основні категорії: рішення для тестування хмарної інфраструктури та рішення з використанням хмарних ресурсів для тестування програмного забезпечення будь-якого типу (включаючи хмарні служби).

2.3.2 Моніторинг

Крім підходів до тестування програмного забезпечення в хмарі, багато зусиль було зроблено для хмарного програмного забезпечення та моніторингу послуг. Насправді хмара надає обмежений доступ до інформації про статус служб, а також про події та дії, що відбуваються в її серверній частині. Моніторинг може допомогти підвищити рівень прозорості в хмарі та, у свою чергу, загальну безпеку хмари. Існуючі підходи до моніторингу розподіленої системи підтримують різні види моніторингу, починаючи від моніторингу окремих програмних служб (наприклад, [55]), до композицій послуг, робочих процесів або оркестровки (наприклад, [56], інфраструктури для систем на основі

послуг (наприклад, мережа та хмарні системи [57]), SLA (наприклад, [58]), або контекст служби (наприклад, [59]).

Зосереджуючись на хмарних середовищах, кілька універсальних рішень моніторингу можна використовувати для моніторингу безпеки хмари. Запропонований підхід знаходить баланс між накладними витратами на моніторинг і можливостями, керуючи засобами моніторингу в адаптивний спосіб.

Така інфраструктура може автоматично адаптуватися до змін у функціях моніторингу, доступних для систем на основі послуг, а також контролювати та керувати SLA, включаючи угоди про властивості безпеки. Наприклад, система DynaQoS [60] підтримує адаптивний багатоцільовий розподіл ресурсів і диференціацію послуг.

2.3.3 Атестація

Використання методів сертифікації для надання достатніх доказів того, що програмна система має деякі нефункціональні властивості та поводиться правильно, набуло широкого поширення за останні 30 років і також стає важливим у хмарних середовищах. У минулому було запропоновано багато рішень і схем сертифікації. Огляд схем сертифікації, які використовуються для оцінки та сертифікації властивостей безпеки програмного забезпечення загалом і засобів контролю безпеки зокрема, можна знайти в [61]. Однак. існуючі методи сертифікації погано підходять для сценарію сервісів і, у свою чергу, для сценарію хмари. Насправді такі методи зазвичай розглядають статичне та монолітне програмне забезпечення, надають сертифікати у формі зрозумілих людині операторів і розглядають загальносистемні сертифікати для використання під час розгортання та встановлення. Навпаки, у хмарному середовищі схема сертифікації повинна відповідати динамічному, багаторівневому та гібридному характеру хмар. Крім того, він має інтегруватись із спеціальними процесами

виконання в хмарі, включаючи розгортання служби, виявлення, вибір і композицію, а також дії з керування, включаючи міграцію, еластичність і розподіл ресурсів.

Перший крок до хмарної сертифікації полягає у визначенні рішень сертифікації для сервісів. В [61] вивчають питання оцінки та сертифікації роботи SOA за допомогою сертифікатів безпеки, включаючи підписані тест-кейси.

Якщо говорити про хмарні обчислення, то було запропоновано лише кілька попередніх рішень проблеми хмарної сертифікації. Наприклад, автори [62] представляють продукт CERTICLOUD – рішення, яке базується на модулі надійної платформи для захисту та перевірки цілісності постачальників IaaS. CERTICLOUD базується на двох протоколах:

1. Сертифікація віддаленого ресурсу на основі TPM (TCRR) перевіряє цілісність фізичних ресурсів.

2. VerifyMyVM перевіряє цілісність середовища користувача при розгортанні в хмарі.

2.3.4 Хмарний аудит/відповідність

Ще один важливий аспект забезпечення хмари – це можливість спостерігати за поведінкою хмари та оцінювати її відповідність політикам клієнтів і законодавчим нормам. Іншими словами, цю мету можна виразити твердженням «зробити хмару доступною для аудиту». Рішення для аудиту можуть підвищити прозорість хмари, таким чином підвищивши рівень довіри між самою хмарою та її орендарями.

Наприклад, в [63] пропонують аудит безпеки як послугу (SAaaS), хмарну систему аудиту та виявлення інцидентів. Їх мета – представити рішення, яке усуває обмеження традиційних систем аудиту та виявлення вторгнень при перенесенні в хмару та реагує на зміни в хмарній інфраструктурі. SAaaS спрямований на підвищення прозорості хмари, надаючи клієнтам доступ до

даних про інциденти безпеки. Автори також представили мову політики хмарного аудиту для архітектури SAaaS, яка має на меті збагатити SAaaS до визначення повної системи аудиту. Представлений підхід здебільшого націлений на рівень IaaS, зосереджений на моніторингу безпеки та націлений на представлення даних аудиту через стандартний інтерфейс.

2.3.5 Угода про рівень обслуговування (SLA)

Інший клас методів гарантії базується на угодах про рівень обслуговування (SLA). Методи, засновані на SLA, спрямовані на встановлення контрактів між клієнтами та провайдерами послуг, що регулюють їх взаємодію та моделюють їхні очікування з точки зору як функціональних, так і нефункціональних угод. Існуючі методи в основному зосереджені на управлінні та узгодженні SLA (наприклад, [64, 65]) і підходи до вибору послуг на основі QoS і нефункціональних властивостей (наприклад, [66]).

D [67] автори представляють структуру на основі проміжного програмного забезпечення для забезпечення на основі SLA в контексті хмарних баз даних. Пропонований фреймворк підтримує динамічне надання рівня даних і покладається на спеціальні політики програми, що відповідають вимогам клієнта до продуктивності, визначеним у SLA.

В роботі [68] представляють рішення для підтримки малих і середніх підприємств у їх міграції до хмари. Підхід до міграції послуг базується на попередньо визначених шаблонах SLA та аналізі ризиків. Він також надає самозахистну хмарну службу, яка контролює проблеми конфіденційності та механізми захисту.

2.3.6 Узагальнення методів гарантування безпеки

Отже, розглянуто низка дослідницьких робіт, спрямованих на підвищення гарантування безпеки, що надається акторам на всіх рівнях хмарного стеку, оцінюючи, чи сервіс/хмарний стек відповідає функціональним і нефункціональним вимогам акторів. Зокрема, представено набір документів, основна мета яких полягає в тому, щоб підвищити надійність хмари щодо механізмів безпеки та елементів керування.

Перш за все, слід зауважити, що оскільки методи гарантування відносно новіші, ніж методи безпеки, їх важко класифікувати відповідно до властивостей безпеки, на які вони спрямовані. Фактично, поточні підходи зосереджені на забезпеченні загальних методів гарантії, а не на конкретних аспектах безпеки. Крім того, ми зазначаємо, що рішення для тестування, моніторингу та SLA були отримані шляхом адаптації існуючих рішень до хмарного середовища. Справді, підходи до тестування зосереджені на тестуванні хмарних додатків і на підході тестування як послуги, коли інструмент тестування розгортається в хмарі та використовується для перевірки будь-якого програмного забезпечення/послуги. Натомість підходи до моніторингу зосереджені на вимогах до розгортання інфраструктури моніторингу в хмарі. Підходи, засновані на SLA, зосереджені на хмарному забезпеченні з урахуванням SLA з метою підтримки вибору послуг на основі QoS. Нарешті, деякі підходи почали розглядати проблему перевірки властивостей хмарних служб/стеків за допомогою підходів на основі сертифікації (апріорі) або рішень аудиту (апостеріорно).

2.4 Узагальнення результатів огляду літературних джерел

На рисунках у цьому підрозділі представлено огляд стану хмарної безпеки та надійності на основі досліджених джерел. На рисунку 2.1 представлено

розподіл публікацій за період 2009 та 2014 років, розрізняючи підходи безпеки та гарантії.

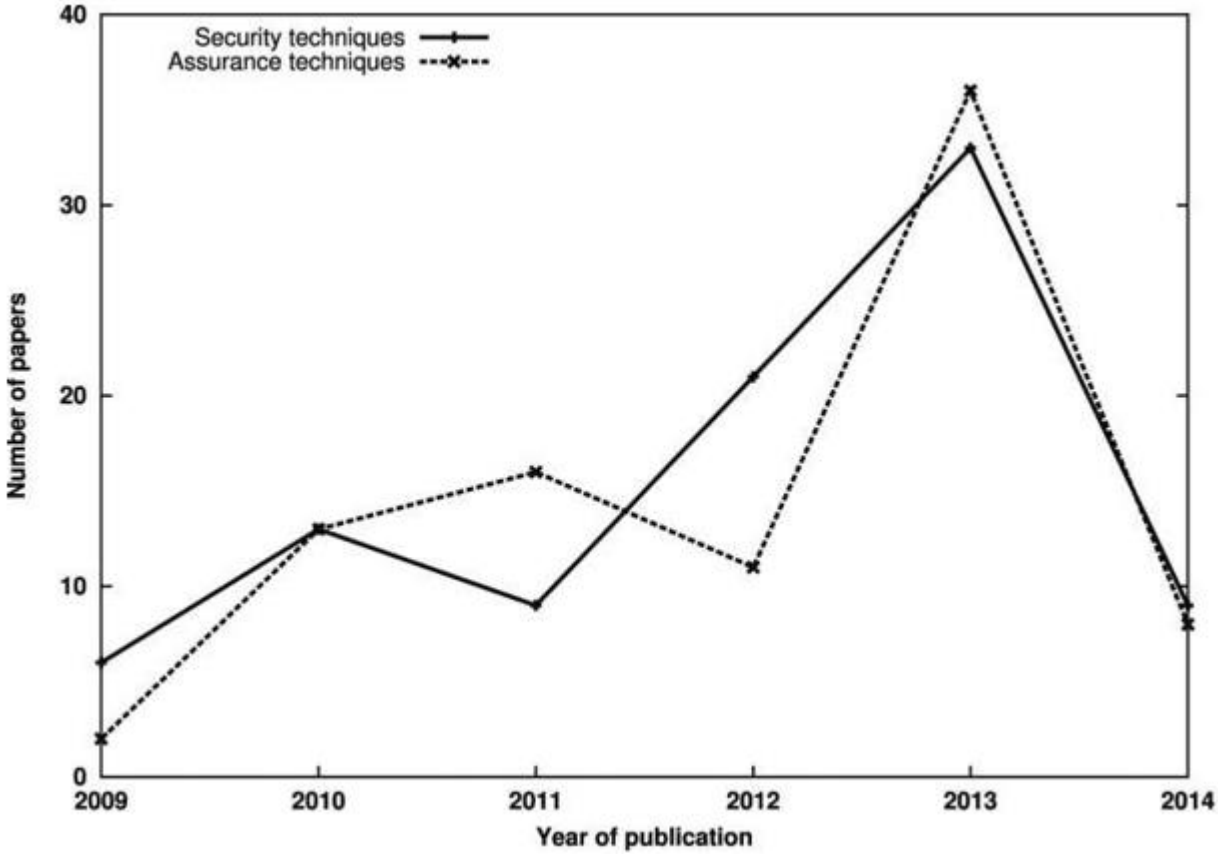

Рисунок 2.1 – Розподіл публікацій на тему безпеки хмарних сервісів за роками

Щоб правильно оцінити розподіл статей на рисунку 2.1, слід пам’ятати, що в цьому дослідженні ми віддали перевагу статтям в період до 2014 року.

На рисунку 2.2 показана тенденція дослідження заходів безпеки та забезпечення щодо об’єкту атаки.

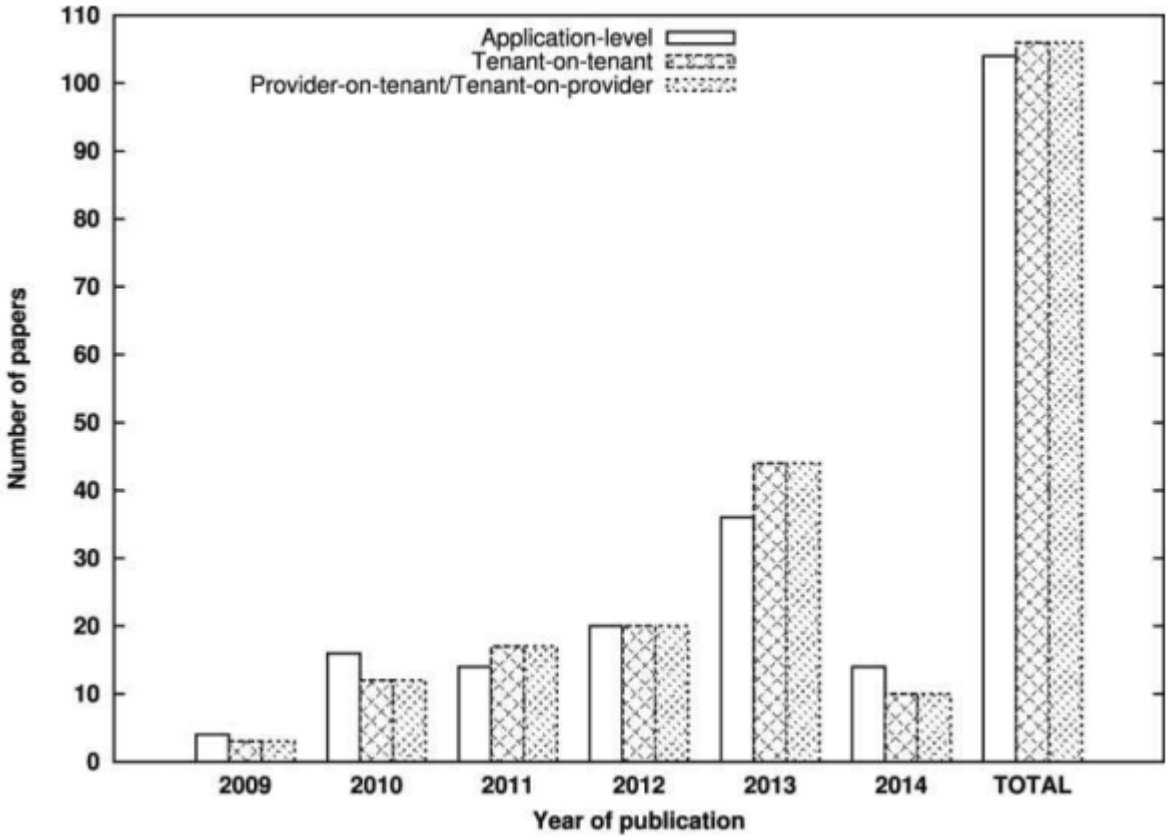

Рисунок 2.2 – Розподіл публікацій щодо рівня забезпечення безпеки

Перш за все варто відзначити, що більше роботи було виконано над рішеннями, що враховують атаки на рівні програми (34,9%) і клієнт-клієнт (35,6%), тоді як менше робіт доступно для рівня провайдер-клієнт і клієнт-провайдер (29,5%). Це пов’язано з тим, що рішення на рівні додатків часто є прямолінійною еволюцією підходів, визначених для сервіс-орієнтованих архітектур, тоді як атаки клієнт-клієнт моделюються вже давно. Ці дані ще більш зрозумілі, якщо взяти до уваги, що понад 50% робіт, зосереджених на рівні провайдер-клієнт і клієнт-провайдер, також розглядають два інші рівні атак, а більше 78% зосереджені на принаймні одному із інших двох рівнях. Також варто зазначити, що кількість визначених рішень зростає для всіх категорій рівнів атаки зі схожими тенденціями.

Рисунок 2.3 показує, що, як і очікувалося, існуючі методи докладають більше зусиль для збереження/захисту конфіденційності (28,3%) і цілісності

(24,3%) властивостей, тоді як менше зусиль було приділено для забезпечення доступності (14%), автентичності (15,4%)) і конфіденційність (18%).

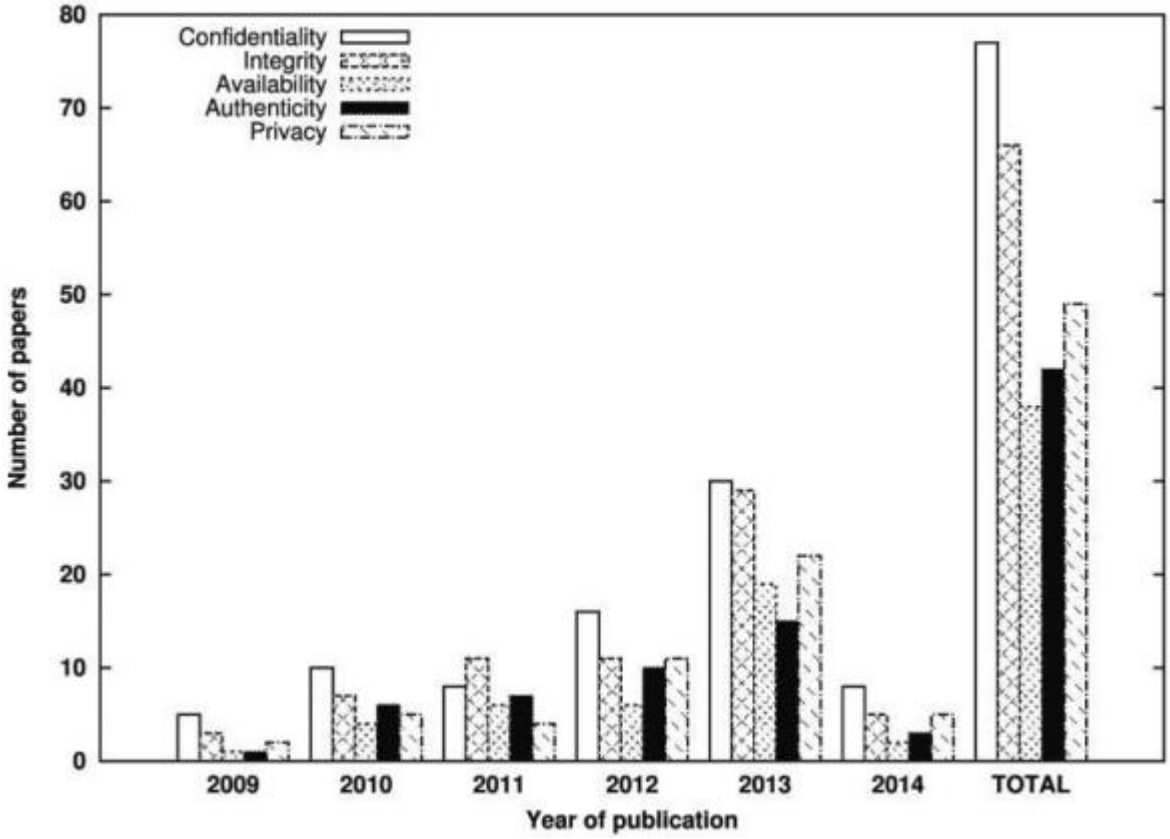

Рисунок 2.3 – Розподіл робіт за характеристиками безпеки

Ці результати підтверджують важливість гарантування конфіденційності та цілісності даних користувачів і додатків під час переміщення в хмару, а також необхідність додаткових досліджень рішень для керування ідентифікацією, що працюють у хмарах. Відносно низька кількість рішень, націлених на доступність, пов’язана з тим, що доступність часто розглядається як властивість на межі між областями дослідження безпеки, надійності та продуктивності. Крім того, рисунок 2.3 показує, що кількість визначених рішень зростає для всіх властивостей безпеки з подібними тенденціями.

На рисунку 2.4 показано, що шифрування (37,2%) і контроль доступу (23,9%) є переважними класами методів для впровадження підходів до хмарної безпеки.

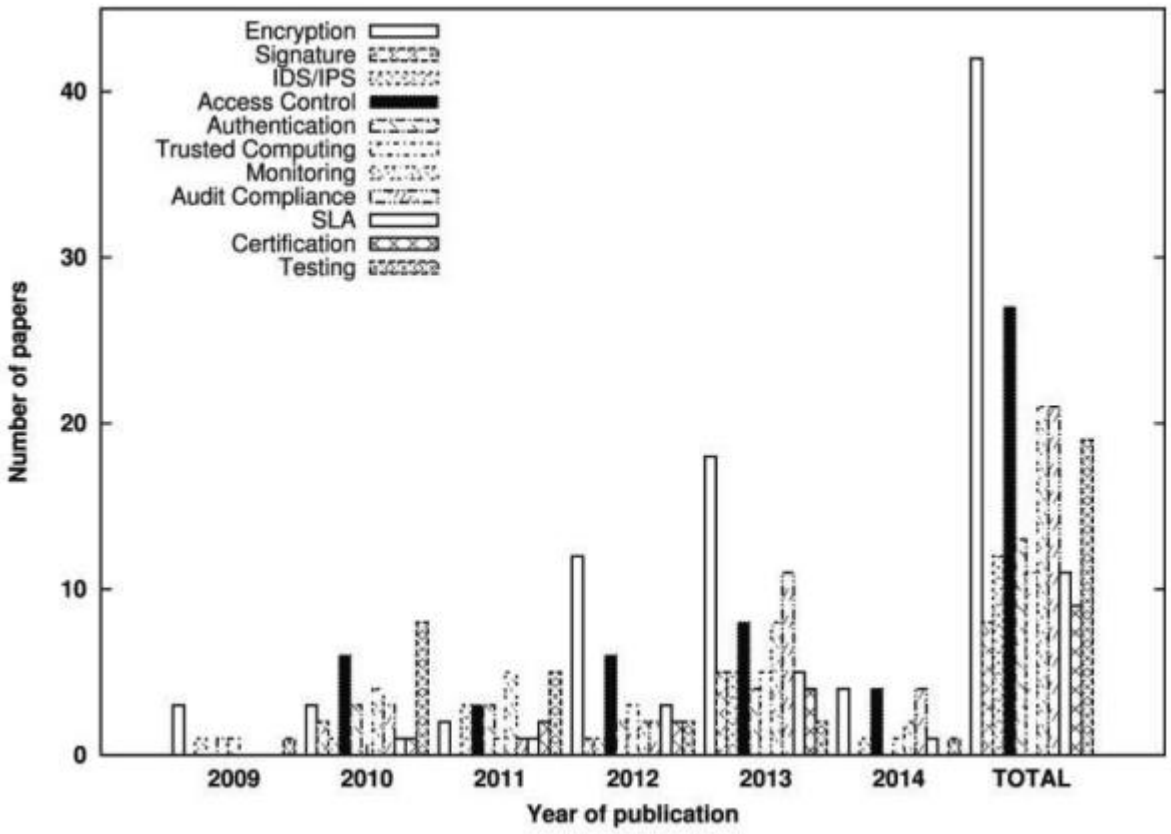

Рисунок 2.4 – Розподіл публікацій за використовуваними методами

Вищезазначені класи доповнені (і частіше інтегровані) підходами, що покладаються на сигнатуру (7,1%) та автентифікацію (11,5%) відповідно. Натомість менше робіт присвячено IDS/IPS (10,6%) і надійних обчислень (9,7%), оскільки обидва методи були запропоновані відносно недавно для віртуальних середовищ. Крім того, досить складно використовувати довірені обчислення, оскільки для цього потрібна підтримка спеціальних апаратних пристроїв, а вартість його розгортання висока. Те саме зауваження можна зробити щодо IDS/IPS, які, переміщені в хмару, створюють додаткові витрати на керування та налаштування.

Успіх класів аудиту, моніторингу та тестування пояснюється тим фактом, що їхні методи часто використовуються для перевірки функціональності розподілених інфраструктур, а потім можуть бути легко застосовані до хмарного середовища. Крім того, дуже часто хмарна інфраструктура використовується для

надання функцій моніторингу та тестування як послуги. Навпаки, SLA та підходи до сертифікації були застосовані до сервісних середовищ лише нещодавно, і тому досі лише іноді використовуються в хмарних інфраструктурах.

Нарешті, на рисунку 2.5 представлено огляд того, як різні методи розподіляються між цільовими властивостями.

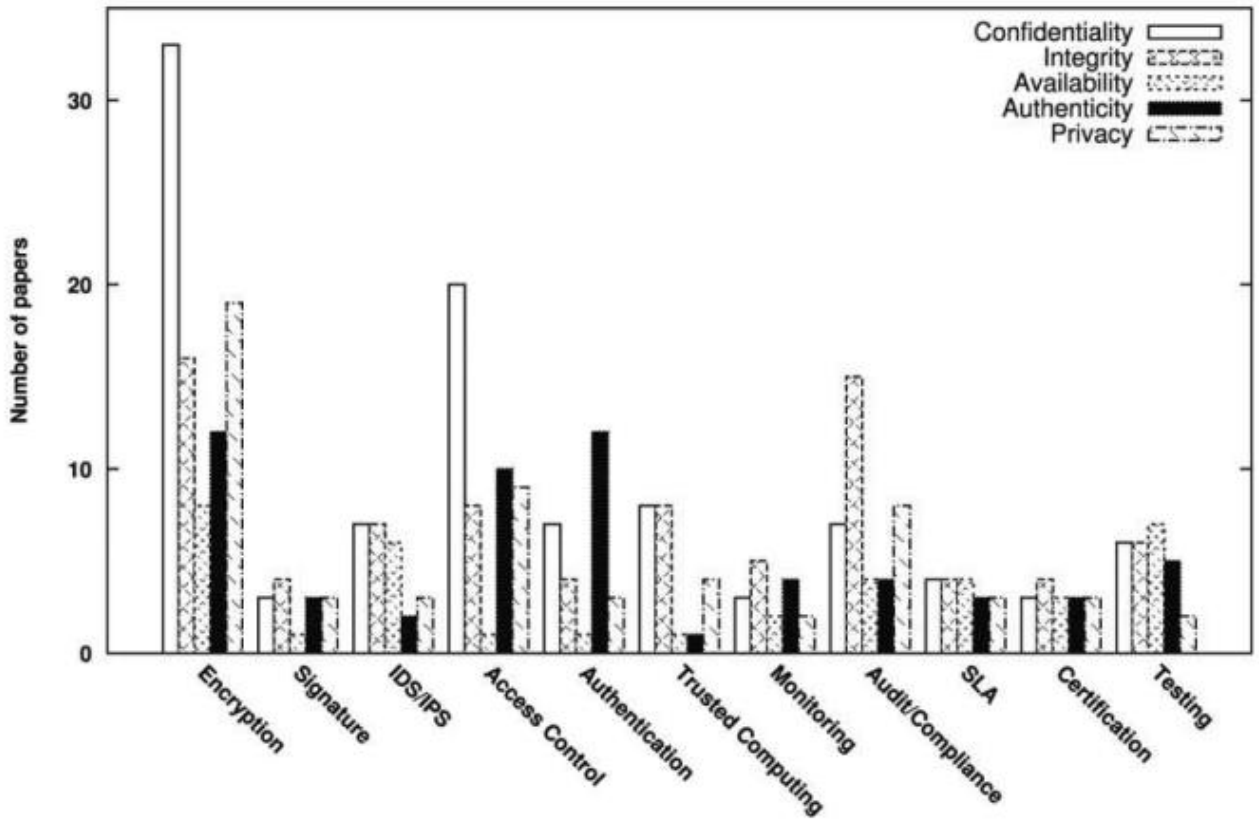

Рисунок 2.5 – Розподіл методів забезпечення безпеки відносно властивостей безпеки

Якщо розглядати методи безпеки, 34,8% націлені на властивість конфіденційності (найвища), тоді як лише 8% націлені на властивість доступності (найнижча). Решта методів майже однаково націлені на властивості цілісності, автентичності та конфіденційності (від 17,9% до 21%). Якщо ми розглядаємо методи гарантування, то їх розподіл є більш однорідним серед класів властивостей, ймовірно, через те, що вони були застосовані до хмарних

середовищ лише нещодавно: 29,8% для цілісності (найвища) і 15,8% для конфіденційності (найнижча).

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1 Охорона праці та її актуальність в ІТ-сфері

Для підвищення ефективності системи управління охорони праці (СУОП) дуже важлива роль належить формуванню і розвитку інформаційної культури фахівців ІТ-технологій, яка впливає на удосконалення інформаційного контуру сучасних підприємств, дозволяє створювати надійні прогнози щодо стану умов праці, показників здоров'я та працездатності, виробничого травматизму і професійної захворюваності, визначати політику розвитку підприємств, установ та організацій на основі різноманітних стратегій охорони праці (інноваційні, маркетингові, інвестиційні, фінансові, технологічні, диверсифікаційні). Поряд з інформаційною культурою важливо використовувати в рамках СУОП «трикутник» її складових: правову, організаційну, управлінську.

В управлінні охороною праці потрібно реалізувати основні положення, окремі теоретико-методологічні підходи інформаційного менеджменту. Головну роль та відповідальність за стан СУОП мають нести фахівці служби охорони праці сучасного підприємства.

Сучасне суспільство називають постіндустріальним, постекономічним, інформаційним, оскільки йдеться про багатосторонні і кардинальні зміни у розвитку цивілізації.

Інформаційне суспільство передбачає докорінну зміну, яка полягає у перетворенні інформації і знань у головний професійно-виробничий потенціал особистості, соціуму і держави.

На постіндустріальному етапі розвитку суспільства вирішальним фактором стає інформація. Її домінування ініціювала науково-технічна революція, яку ще іменують інформаційною, оскільки нею охоплена будь-яка інтелектуальна діяльність, починаючи з інформаційних образів штучного

інтелекту у нових технологіях, економіки, і продовжуючи інформатизацією суспільства в умова світової глобалізації науки й освіти тощо.

Інформаційні технології розглядаються як потужний важіль економічного зростання України. Для цього необхідні значні стратегічні інвестиції у комп'ютерну та комунікаційну інфраструктуру, програми досліджень і розробок, освітню галузь [42].

Під інформаційною культурою розуміють сукупність, складову НІТ (новітні інформаційні технології), технологічну, правову, психологічну, соціологічну та ергономічну підсистеми, що сприяють спрямованому впливу на протікання соціальних процесів у суспільстві, колективі і вихованню свідомого відношення людини до праці, виконання прав та обов'язків [43].

Поняття інформаційної культури виникло в процесі активізації дослідницької уваги до механізмів інформаційного обміну у зв'язку зі значним підвищення ролі інформації в соціокультурних процесах суспільства, яке розглядають як інформаційне суспільство знань, де в центрі знаходяться інформаційні технології.

Робота з інформацією та інформаційна культура в цілому є одним з найважливіших компонентів спроб компанії управляти змінами. Є три принципові причини, в силу яких сьогодні необхідно дбати про інформаційну культуру компанії.

По-перше, вона все більше і більше стає найважливішою частиною загальної організаційної (корпоративної) культури компанії. Все більше компаній розуміють необхідність перетворень, орієнтованих на задоволення очікувань споживача. Щоб сьогодні впливати на майбутнє, потрібно уявляти собі на що вона буде схожа. А для цього потрібно працювати з різноманітною діловою, професійною, технологічною, соціальною, ринковою та політичною інформацією.

По-друге, інформаційні технології роблять можливим створення в компаніях комп'ютерних мереж, за допомогою яких йде спілкування між

менеджерами, але важливо знати, як люди використовують цю інформацію. Саме по собі створення такої мережі з усіма її робочими станціями і мультимедійними можливостями не гарантує того, що інформація буде використовуватися більш розумно і більш ефективно.

По-третє, для різних функціональних служб, підрозділів та робочих груп сучасних підприємств в сфері охорони праці інформаційна культура різна, а це означає відмінність методологічних підходів до процесів усвідомлення, збору, організації, обробки, поширення і використання інформації. Тому багато менеджерів погодяться з тим, що корпоративна інформаційна культура важлива для вироблення різних стратегій охорони праці та запровадження відповідних заходів з її вдосконалення.

Для деяких галузей, таких як розробка програмного забезпечення, інформаційна культура є необхідною умовою виживання, тому що зміна технологій в розробці програмного забезпечення відбувається кожні 6-8 місяців, а інвестиції на підготовку персоналу і освоєння нової технології величезні і у великих компаніях варіюються від 1,5 до 2 млрд. доларів на рік [46].

Аналіз свідчить, що інформатизація та інтеграція комунікаційного простору України сприяє різкому підвищенню інформаційної та професійної компетентності, ділової активності, стимулюванню конкуренції, створенню інноваційних підприємств та організацій, нових робочих місць, зниженню витрат на утримання управлінського апарату [45].

Поряд із задачами і здобутками окреслилися негативи використання інформаційних технологій:

1) надмірне інформаційне навантаження, суть якого полягає у тому, що кількість корисної інформації, яка надходить до мережі, перевищує психофізіологічні можливості її сприйняття людиною;

2) велика кількість інформації, яка сприймається, але не є корисною для фахівців в даний момент;

3) інформаційний голод, причиною якого є саме надлишок інформації, викликаний інформаційним перенавантаженням;

4) «інформоманія» як хвороба людини, яка робить останню знеособленою, залежною від перебування в інформаційному просторі і роботи з комп'ютером і чому вона віддає перевагу, уникаючи «живого» спілкування з людьми;

5) поява «кіберспільнот», що за своїми соціокультурними характеристиками набагато ближчі до представників інших культур у глобальному інформаційному просторі, ніж до своєї етнонаціональної спільноти чи решти населення, не охопленого Інтернетом;

6) індивідуалізм і дегуманізація способу життя «мешканців» Інтернету – відсутність готовності ділитися своїми знаннями.

Слід розуміти, що комп'ютерні технології, а особливо їх мережі істотно впливають на життєдіяльність людини, припускаючи глобалізацію і технократизацію суспільства. Але в ще більшій мірі цей вплив поширюється безпосередньо на центральну нервову систему, яка звикає працювати в дуже інтенсивному режимі багатозадачності, де вже переважають не тривалі логічні роздуми, а інтуїтивно-реактивні ланцюжки розумових формулювань у зв'язку з величезним обсягом оброблюваної щодня інформації, кількість якої зростає за експоненціальною швидкістю. Виникає припущення, що саме збільшення обсягу інформації та прискорення її обробки людиною може згубно вплинути на розвиток розумових здібностей людини.

Аналіз продуктивності розумової праці в найбільших за чисельністю фахівців IT-фірм показав, що велике значення з точки зору впливу на її результати має організаційна (корпоративна) культура. В цьому напрямі влаштовуються різні тімбілдинги, заходи, тренінги для розвитку персоналу. Також кожен керівник повинен добре розуміти свого співробітника, що саме для нього важливо, що його мотивує. Важливо відвести потрібну роль відповідному співробітнику, щоб він виконував ті завдання, які йому цікаві.

На подібних тренінгах в тому числі повинна розглядатися інформаційна культура працівника, в освоєнні, володінні, мотивуванні, застосуванні, перетворенні інформації із застосуванням сучасних інформаційних технологій і використанням цих умінь в навчанні з охорони праці і в подальшій професійній діяльності. Особливо вони будуть корисні, як доповнення до існуючих інструктажів з охорони праці на підприємстві, або як контроль психологічного стану та взаємовідносин у колективі.

Інформаційна культура як інтегративне утворення абсолютно не зводиться до розрізнених знань, вмінь та навичок роботи за комп'ютером. Вона передбачає інформативну спрямованість цілісної особистості, яка володіє мотивацією до застосування і засвоєння нових даних. Інформаційну культуру можна розглядати, як одну з граней особистісного розвитку промислових робітників. Це шлях універсалізації якостей людини.

Оволодіння інформаційною культурою сприяє реальному розумінню особистістю свого місця, себе і своєї ролі у виробничому колективі. Вона має сприяти формуванню нового покоління фахівців інформаційного суспільства, який повинен володіти наступними навичками: виділення релевантної, значущої інформації, диференціації вихідних даних, розробки інформативних критеріїв її оцінки інформації, вміло використовувати її в рамках СУОП.

Сьогодні продовжує діяти стратегічне правило «Можливості комп’ютерної техніки обмежені тільки нашими уявленнями» [44].

3.2 Шкідлива дія шуту та вібрації і захист від неї

Для запобігання шкідливої дії шуму і вібрації на організм працюючих проводяться технічні, організаційні і медикопрофілактичні заходи.

Одним з основних технічних заходів є зменшення при експлуатації та на стадії проектування, конструювання обладнання причин шуму і вібрації в самому джерелі утворення. Досягають цього завдяки використанню раціональної конструкції обладнання, заміни ударної дії деталей і машин

коливальною, з’єднання елементів гнучкими зв’язками, врівноважування обертових частин механізмів, заміни металевих деталей пластмасовими, забезпечення різних власних частот коливань механізму з частотою збуджуючої сили. Аеродинамічний шум може бути зменшений застосуванням глушників та повітропроводів зі змінним перерізом. Шум трансформаторів (електромагнітний шум) знижується, якщо застосувати листи заліза як складових осердя трансформатора з малою магнітострикцією, серцевини.

Якщо неможливо ізолювати чи знизити шум і вібрацію самого джерела, потрібно:

– ізолювати джерело шуму або вібрації від навколишнього середовища засобами вібро- та звукоізоляції

– раціонально планувати виробничі приміщення, що мають інтенсивні джерела шуму;

– збільшувати звукопоглинання внутрішніх поверхонь приміщення шляхом звукопоглинальних покриттів.

Принцип роботи звукоізоляційних екранів оснований на відбиванні звукової хвилі від різних екранів, стін, кожухів обладнання. Шумливі агрегати слід закривати звукоізоляційними кожухами з виводом назовні органів керування та контрольних приладів. Звукоізоляційні екрани виготовляють з металу, деревини, пластмаси та інших щільних матеріалів. Екрани зсередини покривають звукопоглинаючими матеріалами (скловатою пінополіуретаном), а по периметру кожуха – віброізоляційними підкладками (гума).

Вихідними даними для розрахунку параметрів необхідного екрану є спектр шуму, який необхідно ослабити, кількість екранів, через які проходить шум, їх площа, акустичні характеристики приміщення.

За розрахованими значеннями необхідної звукової ізоляційної здатності екрану підбирається матеріал конструкції й екрану.

Принцип звукопоглинання оснований на явищі трансформації коливальної енергії звуку в теплову через втрати при терті. Найбільші втрати при терті мають

пористі, волокнисті і перфоровані матеріали: поролон, пемзолітові і деревоволокнисті плити тощо.

Енергія звукової хвилі переходить у теплову енергію, причому, ефект звукоізоляції збільшується з ростом частоти звукової хвилі. Звукопоглинаючими матеріалами оббивають стелі, стіни. Щоб одержати ефективну звукоізоляцію, найбільш доцільно застосовувати багатошарові огородження з м'якими прошарками (мінеральна вата).

Важливим технічним рішенням у забезпеченні виробничих умов є вдосконалення ручних віброінструментів. Для цього використовують віброгасіння, змінюють ударний вузол, проводять балансування частин, що обертаються.

Послаблення локальної вібрації і передачі вібрації на підлогу і сидіння досягається засобами віброізоляції і вібропоглинання, застосуванням пружинних і гумових амортизаторів, прокладок тощо. Для обмеження поширення вібрацій через ґрунт, між фундаментом і ґрунтом залишають повітряні проміжки, які називаються акустичними розривами.

В останні роки знаходять застосування динамічні віброгасники, в яких створюються вібрації, що співпадають по частоті і протилежні по фазі вібрації машини, коливання якої необхідно зменшити.

До організаційних заходів по боротьбі з шумом та вібрацією на виробництві відносяться: впровадження раціонального режиму праці і відпочинку, обмеження часу роботи при використанні ручного інструменту, який створює вібрацію.

Глушники звуку застосовуються для зменшення шуму аеродинамічних установок (вентиляторів, пневмоінструментів, газотурбінних, дизельних, компресорних установок). Вони поділяються на активні, які поглинають звукову енергію, що на них поступила, і реактивні, які відбивають цю енергію. Потужні джерела шуму як правило розміщують в окремих приміщеннях, які віддалені від постійних робочих місць.

Ізоляційні кабіни або екрани застосовують як екрани робочих місць для зменшення зовнішніх шумів.

Якщо не вдається зменшити рівень шуму і вібрації на робочому місці до нормативних значень та необхідно використовувати засоби індивідуального захисту: рукавиці, взуття, навушники, м'які шоломи, які зменшують рівень звукового тиску на 40-50 дБ.

У процесі виробництв, експлуатації і зберігання радіоелектронних засобів можуть виникати механічні і динамічні дії, що характеризуються широким діапазоном частот коливань, а також амплітудою, прискоренням і часом дії. Рівень механічних дій визначається умовами транспортування й експлуатації.

Необхідно розрізняти два види механічних дій: удари і вібрації. Удар виникає, коли апаратура отримує швидку зміну прискорення (піддаються удару входи кабелів, джгути, резистори, конденсатори, напівпровідникові діоди і тріоди, силові трансформатори, дроселі тощо). Вібрації – довготривалі знакозмінні процеси, які впливають на роботу апаратури при безпосередньому контакті з джерелом коливань або через повітряне середовище.

У результаті дії вібрацій і удару можуть бути наступні ушкодження апаратури: порушення герметичності через псування паяльних, зварних і клеєних швів і появи тріщин у метало-скляних спаях; повне руйнування корпусів або окремих їх частин через механічний резонанс або циклічну втому; обривання монтажних зв'язків, відшарування багатошарових друкованих плат, руйнування підставок; вихід з ладу електричних контактів; модуляція розмірів хвилеводних трактів; коаксіальних кабелів, конденсаторів змінної ємності, коливальних контурів, електровакуумних приладів, зміщення положення органів настроювання і управління.

Під впливом вібрацій може статись зміна параметрів напівпровідникових приладів, вольт амперних характеристик діодів, транзисторів. Все це призводить до руйнування конструкцій за рахунок явищ втоми.

Радіоелектронна апаратура (РЕА) повинна мати віброміцність, вібростійкість, ударостійкість.

Захист РЕА здійснюється наступними групами методів:

– зменшується інтенсивність джерел вібрації шляхом балансування, зменшення зазорів, віброізоляції джерела вібрацій;

– зменшується величина дій, що передається апаратом шляхом віброізоляції, демпфірування, виключення резонансів, активного віброзахисту за допомогою ексцентриків, маятників, гіроскопів;

– використання найбільш добротні і жорсткі компоненти і вузли;

– застосовуються амортизатори.

Захист часом, захист віддалю, усунення джерела тепловиділення, теплоізоляція, охолодження гарячої поверхні, забезпечення тепловіддачі тіла людини та індивідуальні засоби захисту.

Захист часом передбачає обмеження часу перебування робітника в зоні дії інфрачервоного випромінювання. Потужність випромінювання можна знизити за рахунок конструкторських і технологічних рішень (зміною нагрівання виробів у нагрівальних пічках індукційним нагріванням та ін.) і за рахунок покриття поверхні, яка нагрівається, тепло ізолювальним матеріалом.

Якщо теплоізоляція неможлива, тоді захист від прямої дії інфрачервоного випромінювання здійснюється екрануванням.

Екрани можуть бути прозорими, напівпрозорими і непрозорими.

У свою чергу вони поділяються на тепловідбивальні, тепловідвідні та теплопоглинальні; стаціонарні і нестаціонарні.

Застосовують також прозору водяну завісу у вигляді суцільної тонкої водяної плівки. Вода є активним поглиначем інфрачервоного випромінювання.

Перегрівання людини попереджують раціональним режимом пиття, режимом праці та гідро процедурами. Спецодяг виготовляється з незаймистого, стійкого до інфрачервоного випромінювання, м’якого і повітронепроникного

матеріалу (тканина з металевим покриттям відбиває 90 % інфрачервоного випромінювання).

Для захисту очей застосовують світлофільтри зі спеціального жовто-зеленого або синього скла.

Першочергові заходи – це конструкторські і технологічні рішення, які виключають генерацію або понижують інтенсивність випромінювання. Спеціальні засоби захисту (екранування джерел випромінювання, фарбування стін у світлі кольори) попереджують розповсюдження і знижують інтенсивність цих випромінювань у виробничих приміщеннях. Очі захищають окулярами або щитками зі склом – світлофільтром. Для захисту шкіри використовують мазі з речовинами – світлофільтрами для цих променів (салол, саліцилово-метиловий ефір та ін.), а також спецодяг з бавовняних тканин і грубововняного сукна. Руки захищають рукавицями.

ВИСНОВОК

Широке впровадження хмарних обчислень вимагає рішень безпеки та надійності, які підвищують довіру користувачів хмари до самої хмари та до її постачальників. Проблема забезпечення та перевірки безпеки загострюється тим фактом, що хмара надає багато функціональних можливостей, які підвищують гнучкість, продуктивність і надійність (наприклад, міграція, об'єднання, масштабованість, еластичність), які впливають на функціонування рішень безпеки та надійності для розподілених мереж.

Багато дослідників запропонували детальні рішення безпеки, які спрямовані на різні аспекти проблеми безпеки хмари. Незважаючи на те, що такі рішення можуть допомогти досвідченим користувачам захистити свої програми та дані в хмарі, вони роблять сценарій безпеки хмари громіздким для більшості клієнтів.

Можна стверджуквати, що самоспостереження, тобто здатність хмарного провайдера досліджувати та спостерігати за своїми внутрішніми процесами, не є єдиною концепцією, яка має значення при розгляді хмарної безпеки. Насправді, концепція аутроспекції, тобто надання клієнтам і постачальникам послуг можливості досліджувати та спостерігати за внутрішніми процесами хмари, що впливають на (безпеку) їх діяльності/додатків/даних, також має першочергове значення.

Правильне рішення безпеки в хмарі має охоплювати як самоаналіз постачальників хмари, так і зовнішню перевірку клієнтів хмари (загалом орендарів), збалансовуючи контроль безпеки та надійності між постачальниками та клієнтами, а також сприяючи повному прийняттю парадигми хмари також у критичних середовищах. Підвищена прозорість хмари може допомогти вирішити проблему керування безпекою, підтримуючи як самоаналіз, так і зовнішній аналіз. Прозорість може бути досягнута за допомогою стандартизованих інтерфейсів, незалежних від хмарного стеку, які надають

загальну точку доступу до подій і дій, що відбуваються в хмарному сервері. Наприклад, підтримку даної властивості безпеки можна перевірити, відстежувати та перевіряти шляхом збору даних щодо функціонування певного механізму безпеки (наприклад, механізму контролю доступу для авторизації).

Збираючи уніфіковані та однорідні дані про хмарну діяльність, ми також можемо збагатити рішення для оцінки відповідності та аудиту хмари, а також підходи, що підтримують динамічну адаптацію хмарної інфраструктури до змін, які вплинуть як на постачальника хмари (і його діяльність з управління), так і на клієнта. (і відповідні послуги). Крім того, стандартизований доступ до цих даних може надати клієнтам певні докази щодо поточного стану їхніх послуг і загальної безпеки, а також підтримувати управління життєвим циклом їхньої безпеки (і, загалом, нефункціональної) власності.

Хмарні серверні дані являють собою прихований цінний ресурс, на основі якого можна створювати нові служби та покращувати функціональність, безпеку та надійність хмари.

ПЕРЕЛІК ПОСИЛАНЬ

1. G. Ballabio. 2013. Security and availability techniques for cloud-based applications. Computer Fraud & Security 2013, 10 (October 2013), 5–7.
2. Bhadauria, Rohit, and Sugata Sanyal. "Survey on security issues in cloud computing and associated mitigation techniques." arXiv preprint arXiv:1204.0764 (2012). Retrieved from http://arxiv.org/ftp/arxiv/papers/1204/1204.0764.pdf.
3. M. Al Morsy, J. Grundy, and I. Muller. November-December 2010. An analysis of the cloud computing security¨ problem. In Proc. of APSEC-CLOUD 2010.
4. C. Irvine and T. Levin. December 1999. Toward a taxonomy and costing method for security services. In Proc. of ACSAC 1999.
5. N. Gruschka and L. L. Iacono. July 2009. Vulnerable cloud: SOAP message security validation revisited. In Proc. of IEEE ICWS 2009.
6. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono. July 2009. On technical security issues in cloud computing. In Proc. of IEEE CLOUD 2009.
7. A. Chonka, Y. Xiang, W. Zhou, and A. Bonti. 2011. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications 34, 4 (July 2011), 1097–1107.
8. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. November 2009. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In Proc. of ACM CCS 2009.
9. A. Aviram, S. Hu, B. Ford, and R. Gummadi. October 2010. Determinating timing channels in compute clouds. In Proc. of ACM CCSW 2010.
10. Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart. October 2012. Cross-VM side channels and their use to extract private keys. In Proc. of ACM CCS 2012.
11. M. Godfrey and M. Zulkernine. June 2013. A server-side solution to cache-based side-channel attacks in the cloud. In Proc. of IEEE CLOUD 2013.
12. H. Liu. October 2010. A new form of DOS attack in a cloud and its avoidance mechanism. In Proc. of ACM CCSW 2010.

13. F. Rocha and M. Correia. June 2011. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In Proc. of IEEE/IFIP DSN-W 2011.
14. S. Bleikertz, S. Bugiel, H. Ideler, S. Nurnberger,¨ and A.-R. Sadeghi. June 2013. Client-controlled cryptography-as-a-service in the cloud. In Proc. of ACNS 2013.
15. K. D. Bowers, A. Juels, and A. Oprea. November 2009. HAIL: A high-availability and integrity layer for cloud storage. In Proc. of ACM CCS 2009.
16. S. Pearson and A. Benameur. November-December 2010. Privacy, security and trust issues arising from cloud computing. In Proc. of IEEE CloudCom 2010.
17. M. Ahmed, Q. H. Vu, R. Asal, H. Al Muhairi, and C. Y. Yeun. July 2012. SECRESO: A secure storage model for cloud data based on reed-solomon code. In Proc. of AIM 2012.
18. H.-Y. Lin and W.-G. Tzeng. 2012. A secure erasure code-based cloud storage system with secure data forwarding. IEEE TPDS 23, 6 (June 2012), 995–1003.
19. D. Zissis and D. Lekkas. 2012. Addressing cloud computing security issues. Future Generation Computer Systems 28, 3 (March 2012), 583–592.
20. B. Libert and J.-J. Quisquater. 2011. Identity-based cryptosystems. In Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia (Eds.). Springer.
21. A. Juels and A. Oprea. 2013. New approaches to security and availability for cloud data. CACM 56, 2 (February 2013).
22. T. Jung, X.-Y. Li, and Z. Wan. April 2013. Privacy preserving cloud data access with multi-authorities. In Proc. of IEEE INFOCOM 2013.
23. E. Pattuk, M. Kantarcioglu, V. Khadilkar, H. Ulusoy, and S. Mehrotra. June 2013. BigSecret: A secure data management framework for key-value stores. In Proc. of IEEE CLOUD 2013.
24. P. K. Tysowski and M. A. Hasan. 2013. Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds. IEEE TCC 1, 2 (July 2013), 172–186.

25. L. Wei and M. K. Reiter. September 2013. Ensuring file authenticity in private DFA evaluation on encrypted files in the cloud. In Proc. of ESORICS 2013. Egham, UK.
26. A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket. October 2010. Venus: Verification for untrusted cloud storage. In Proc. of ACM CCSW 2010.
27. V. Attasena, N. Harbi, and J. Darmont. September 2013. Sharing-based privacy and availability of cloud data warehouses. In Proc. of EDA 2013.
28. Wang, N. Cao, K. Ren, and W. Lou. 2012. Enabling secure and efficient ranked keyword search overoutsourced cloud data. IEEE TPDS 23, 8 (August 2012), 1467–1479.
29. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A.V. Vasilakos. April 2014. Security and privacy for storage and computation in cloud computing. Information Sciences 258 (April April 2014), 371–386.
30. L. Xu, X. Cao, Y. Zhang, and W. Wu. 2013a. Software service signature (s3) for authentication in cloud computing. Cluster Computing 16, 4 (December 2013), 905–914.
31. U. Lang. November-December 2010. OpenPMF SCaaS: Authorization as a service for cloud & SOA applications. In Proc. of IEEE CloudCom 2010.
32. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman. 2012. Secure overlay cloud storage with access control and assured deletion. IEEE TDSC 9, 6 (November 2012), 903–916.
33. Y. Zhu, H. Hu, G.-J. Ahn, D. Huang, and S. Wang. March 2012. Towards temporal access control in cloud computing. In Proc. of IEEE INFOCOM 2012.
34. M. Raykova, H. Zhao, and S. M. Bellovin. February-March 2012. Privacy enhanced access control for outsourced data sharing. In Proc. of FC 2012.
35. Z. Wan, J. Liu, and R.-H. Deng. 2012. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE TIFS 7, 2 (April 2012), 743–754.

36. J. Bacon, D. Eyers, T. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch. 2014. Information flow control for secure cloud computing. IEEE TNSM (2014).
37. S. Ruj, M. Stojmenovic, and A. Nayak. 2014. Decentralized access control with anonymous authentication of data stored in clouds. IEEE TPDS 25, 2 (February 2014), 384–394.
38. Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masuoka. 2009. TrustCube: An infrastructure that builds trust in client. In Future of Trust in Computing, D. Gawrock, H. Reimer, A.-R. Sadeghi, and C. Vishik (Eds.). Vieweg+Teubner, 68–79.
39. S. A. Almulla and C. Y. Yeun. March-April 2010. Cloud computing security management. In Proc. of ICESMA 2010. Sharjah, UAE.
40. H. Li, Y. Dai, and B. Yang. 2011. Identity-based cryptography for cloud security. IACR Cryptology ePrint Archive 2011 (2011), 169.
41. U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli. September 2013. Cloud based secure and privacy enhanced authentication & authorization protocol. In Proc. of KES 2013.
42. F. J. Krautheim. June 2009. Private virtual infrastructure for cloud computing. In Proc. of HotCloud 2009. San Diego, CA, USA.
43. W. Ma, X. Li, Y. Shi, and Y. Guo. 2013. A virtual machine cloning approach based on trusted computing. TELKOMNIKA 11, 11 (November 2013), 6935–6942.
44. M. Li, W. Zang, K. Bai, M. Yu, and P. Liu. December 2013. MyCloud: Supporting user-configured privacy protection in cloud computing. In Proc. of ACSAC 2013.
45. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan. 2013b. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications 36, 1 (June 2013), 42–57.
46. M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni. November 2009. Cloud security is not (just) virtualization security. In Proc. of ACM CCSW 2009.

47.H. Li, Y. Dai, and B. Yang. 2011a. Identity-based cryptography for cloud security. IACR Cryptology ePrint Archive 2011 (2011), 169.

48.S. J. Stolfo, M. B. Salem, and A. D. Keromytis. May 2012. Fog computing: Mitigating insider data theft attacks in the cloud. In Proc. of IEEE SPW 2012.

49.S. Yu, Y. Tian, S. Guo, and D. Wu. 2013b. Can we beat DDoS attacks in clouds? IEEE TPDS (July 2013).

50.C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu. March-April 2014. On the management of cloud nonfunctional properties: The cloud transparency toolkit. In Proc. of IFIP NTMS 2014.

51.G. Spanoudakis, E. Damiani, and A. Mana. October 2012. Certifying services in cloud: The case for a hybrid,˜ incremental and multi-layer approach. In Proc. of IEEE HASE 2012.

52.. MacNeil and X. Li. 2006. “Comply or explain”: Market discipline and non-compliance with the Combined Code. Corporate Governance: An International Review 14, 5 (2006), 486–496.

53.C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu. March-April 2014. On the management of cloud nonfunctional properties: The cloud transparency toolkit. In Proc. of IFIP NTMS 2014.

54.ISTQB glossary. Testing. https://glossary.istqb.org/en_US/term/testing-9

55.K. Mahbub and G. Spanoudakis. 2007. Monitoring WS-agreements: An event calculusbased approach. In Test and Analysis of Web Services, L. Baresi and E. Di Nitto (Eds.). Springer, Berlin, 265–306.

56.L. Baresi and S. Guinea. December 2005. Dynamo: Dynamic monitoring of WS-BPEL processes. In Proc. of ICSOC 2005.

57.H.-L. Truong_c and T. Fahringer. 2004. SCALEA-G: A unified monitoring and performance analysis system for the grid. Scientific Programming 12, 4 (December 2004), 225–237.

58. C. Ghezzi and S. Guinea. 2007. Run-time monitoring in service-oriented architectures. In Test and Analysis of Web Services, L. Baresi and E. Di Nitto (Eds.). Springer, Berlin, 237–264.
59. M. Salifu, Yijun Yu, and B. Nuseibeh. October 2007. Specifying monitoring and switching problems in context.In Proc. of IEEE RE 2007.
60. J. Rao, Y. Wei, J. Gong, and C.-Z. Xu. 2013. QoS guarantees and service differentiation for dynamic cloud applications. IEEE TNSM 10, 1 (March 2013), 43–55.
61. E. Damiani, C. A. Ardagna, and N. El Ioini. 2009a. Open source systems security certification. Springer, New York.
62. B. Bertholon, S. Varrette, and P. Bouvry. July 2011. Certicloud: A novel TPM-based approach to ensure cloud IaaS security. In Proc. of IEEE CLOUD 2011.
63. F. Doelitzscher, T. Ruebsamen, T. Karbe, M. Knahl, C. Reich, and N. Clarke. 2013. Sun behind clouds - On automatic cloud security audits and a cloud audit policy language. International Journal on Advances in Networks and Services 6, 1–2 (2013), 1–16.
64. P. Wieder, J. M. Butler, W. Theilmann, and R. Yahyapour. 2011. Service Level Agreements for Cloud Computing. Springer.
65. R. Jhawar and V. Piuri. August 2013. Adaptive resource management for balancing availability and performance in cloud computing. In Proc. of SECRYPT 2013.
66. Zhao, Y. Ren, M. Li, and K. Sakurai. 2012. Flexible service selection with user-specific QoS supportin service-oriented architecture. Journal of Network and Computer Applications 35, 3 (March 2012), 962–973.
67. S. Sakr and A. Liu. June 2012. SLA-based and consumer-centric dynamic provisioning for cloud databases. In Proc. of IEEE CLOUD 2012.
68. A. Sulistio and C. Reich. September 2013. Towards a self-protecting cloud. In Proc. of OTM 2013.
69. Жидецький, В. Ц., Джигирей, В. С., & Мельников, О. В. (2000). Основи охорони праці. Львів: Афіша, 350, 132-136.

70.Навакатіян О.О., Кальниш В.В., Стрюков С.М. Охорона праці користувачів комп’ютерних відеодисплейних терміналів. - К.:1997. - 400с.