МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра економічної кібернетики та інформатики

КОЛІНЕЦЬ Руслана Богданівна

Методи виявлення вразливостей аутентифікації в SaaS-сервісах / Methods for Detecting Authentication Vulnerabilities in SaaS Services

спеціальність: 124 – Системний аналіз

освітньо-професійна програма – Системний аналіз

Кваліфікаційна робота

Виконав студент групи
САм -21
Р.Б. Колінець

Науковий керівник
доктор економічних наук Л. М. Буяк

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2024 р.

Завідувач кафедри

_____ Л. М. Буяк

ТЕРНОПІЛЬ – 2024

Факультет комп'ютерних інформаційних технологій
Кафедра економічної кібернетики та інформатики
Освітній ступінь «магістр»
спеціальність: 124 – Системний аналіз
освітньо-професійна програма – Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Л. М. Буяк
«____» _____ 2022 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Колінець Руслані Богданівні
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Методи виявлення вразливостей аутентифікації в SaaS-сервісах / Methods for Detecting Authentication Vulnerabilities in SaaS Services
керівник роботи доктор економічних наук Л. М. Буяк

затверджені наказом по університету від 1 грудня 2023 року № _____

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- проаналізувати існуючих аутентифікаційних механізмів;
- провести аналіз потенційних загроз;
- розгляд нових методів виявлення вразливостей;
- провести аналіз MITRE ATT&CK для класифікації вразливостей;
- розробка рекомендацій та стратегій безпеки.

5. Перелік графічного матеріалу у роботі:
- захист SaaS – сервісів на основі матриці mitre att&ck
- шаблон атаки спамера
- проблеми безпеки в saas - сервісах
- етапи безпечного доступу до saas – сервісів

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз існуючих методів виявлення вразливостей аутентифікації в saas-сервісах	12.2023 р. – 03.2024 р.	
2	Використання mitre att&ck для класифікації та аналізу вразливостей аутентифікації в saas-сервісах	03.2024 р. – 05.2024 р.	
3	Запропонований метод захисту аутентифікації в saas- сервісах	05.2024 р. – 11.2024р.	

Студент _____ Колінець Р.Б.
(підпис)

Керівник роботи _____ доктор економічних наук Л. М. Буяк

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи виявлення вразливостей аутентифікації в SaaS-сервісах» на здобуття освітнього ступеня «Магістр» зі спеціальності 124 «Системний аналіз» освітньо-професійної програми «Системний аналіз» написана обсягом 76 сторінок і містить 9 ілюстрацій, 6 таблиць, 1 додаток та 31 джерело за переліком посилань.

Метою випускної кваліфікаційної роботи є покращенні безпеки SaaS-сервісів, що використовуються в різних сферах, забезпечуючи надійний захист конфіденційної інформації та даних користувачів.

Методи досліджень. Для розв'язання поставлених задач у магістерській роботі використано методи: аналізу, виявлення загроз, використання MITRE ATT&CK для класифікацій вразливостей, розробка рекомендацій, стратегії безпеки.

Результати дослідження: аналіз відомих вразливостей аутентифікації в SaaS – сервісах, аналіз вразливостей з використанням матриці MITRE ATT&CK, рекомендації

Результати роботи можуть бути корисні у різних аспектах, сприяючи покращенню роботи та розвитку аутентифікації в SaaS-сервісах.

Орієнтовні напрямки розвитку досліджень: сформульовані та обґрунтовані висновки цього дослідження можуть бути базою для подальших наукових пошуків у галузі хмарних сервісів та роботи з ними.

Ключові слова: SAAS, MITRE ATT&CK, АУТЕНТИФІКАЦІЯ, SAAS-СЕРВІСИ, МЕТОДИ АУТЕНТИФІКАЦІЇ.

ABSTRACT

Final qualification work with the topic «The algorithms for detecting botnets in the Internet of Things» from the specialty 124 «System analysis» was wrote on 76 pages volume and contains 9 illustrations, 6 tables, 1 application and 31 sources for references.

The aim of the graduation qualification work is to enhance the security of SaaS services used in various domains, ensuring reliable protection of confidential information and user data.

Research Methods. To address the set tasks in the master's thesis, the following methods were employed: analysis, threat detection, the use of MITRE ATT&CK for vulnerability classification, development of recommendations, and security strategies.

The results: The research outcomes include the analysis of known authentication vulnerabilities in SaaS services, vulnerability analysis using the MITRE ATT&CK matrix, and recommendations.

The results of the work can be beneficial in various aspects, contributing to the improvement and development of authentication in SaaS services.

The formulated and justified conclusions of this research can serve as a foundation for further scientific exploration in the field of cloud services and their authentication processes.

Keywords: SAAS, MITRE ATT&CK, AUTHENTICATION, SAAS SERVICES, AUTHENTICATION METHODS.

ЗМІСТ

ВСТУП

Актуальність теми. У час активного розвитку хмарних технологій та широкого впровадження SaaS-платформ, питання надійної аутентифікації користувачів набуває особливої актуальності. Оскільки такі сервіси оперують важливими даними та забезпечують доступ до критичних функцій, системи перевірки автентичності повинні відповідати найвищим стандартам захисту.

Сучасні тенденції демонструють постійне збільшення спроб несанкціонованого доступу через компрометацію облікових записів, включаючи соціальну інженерію та інші методи зламу систем автентифікації. Це створює нагальну потребу у поглибленому аналізі та модернізації підходів до виявлення потенційних вразливостей у механізмах аутентифікації SaaS-платформ.

Впровадження інноваційних методик пошуку слабких місць у системах аутентифікації хмарних сервісів сприятиме значному посиленню їх захищеності, мінімізації ризиків витоку персональних даних та зміцненню репутації сервісів серед користувачів. Такі дослідження є ключовим елементом у забезпеченні належного рівня захисту інформації, що обробляється та зберігається у SaaS-системах.

Мета і завдання дослідження. Метою дослідження є підвищення рівня безпеки хмарних сервісів, що застосовуються в різних професійних середовищах, через створення надійних механізмів захисту конфіденційної інформації та персональних даних користувачів.

Зазначена мета передбачає вирішення таких завдань дослідження:

- Аналіз існуючих аутентифікаційних механізмів.
- Виявлення потенційних загроз.
- Розгляд нових методів виявлення вразливостей.
- Використання MITRE ATT&CK для класифікації вразливостей
- Розробка рекомендацій та стратегій безпеки.

Об’єктом дослідження виступають системи ідентифікації та верифікації користувачів, механізми контролю доступу, протокольні рішення безпеки та стратегії протидії соціальної інженерії в середовищі хмарних платформ (SaaS).

Предметом дослідження служать конкретні процедури та алгоритми ідентифікації користувачів, реалізовані в структурах сучасних хмарних платформ (SaaS).

Методи дослідження. Аналіз існуючих аутентифікаційних механізмів, аналіз відомих вразливостей в SaaS-сервісах, систематизація вразливостей за допомогою методології MITRE ATT&CK, формування рекомендацій та стратегічних рішень безпеки кіберпростору.

Наукова новизна отриманих результатів полягає в тому, що робота є комплексним дослідженням ідентифікації та верифікації користувачів у середовищі хмарних платформ.

Практичне значення дослідження полягає в розроблених концепціях та методологічних підходах, які створюють теоретичне підґрунтя для подальших наукових досліджень у сфері безпеки та функціонування хмарних середовищ.

Публікації та апробація.

1. Колінець Р.Б.. Аналіз поширених вразливостей у веб застосунках. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції "Актуальні проблеми комп’ютерних наук АПКН-2024", Хмельницький, 2024. С. 282 - 288.

1. ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ АУТЕНТИФІКАЦІЇ В SAAS-СЕРВІСАХ

Сучасні веб-технології породили новий напрям - хмарні обчислення, які представляють собою комплексне рішення для надання різноманітних IT-послуг через мережу Інтернет. Цей підхід трансформує традиційні бізнес-процеси, забезпечуючи гнучкий доступ до спільних обчислювальних ресурсів, програмного забезпечення та інформаційних сервісів за запитом.

Архітектура хмарних обчислень базується на трьох ключових компонентах: чотирьох варіантах розгортання, трьох сервісних моделях та п'яти фундаментальних характеристиках, що визначають її функціональність.

Щодо варіантів розгортання, виділяють публічні хмари, доступні широкому загалу, приватні хмари для окремих організацій, гібридні рішення, що поєднують обидва підходи, та хмари спільноти, створені для певних груп користувачів. У сфері хмарних обчислень виділяють три основні сервісні моделі: програмне забезпечення як сервіс (SaaS), платформа як сервіс (PaaS) та інфраструктура як сервіс (IaaS). Успішна реалізація хмарних обчислень базується на декількох ключових технологіях.

Фундаментальні технологічні складові хмарних обчислень включають:

Веб-застосунки та сервіси становлять фундамент для SaaS та PaaS рішень. Це пояснюється тим, що веб-застосунки фактично є SaaS-пропозиціями, для яких PaaS забезпечує середовище розробки та виконання. У контексті IaaS, веб-технології застосовуються для створення програмних інтерфейсів та споріднених сервісів [1].

Віртуалізація в IaaS відіграє визначальну роль у реалізації хмарних обчислень. Її значення поширюється також на PaaS та SaaS моделі, оскільки вони зазвичай функціонують на базі IaaS-інфраструктури.

Методи криптографії виявилися незамінними для забезпечення безпеки хмарних обчислень. З розвитком та вдосконаленням хмарних технологій очікується розширення переліку базових технологій.

Ключові характеристики хмарних обчислень, визначені Національним інститутом стандартів і технологій США (NIST), включають [2]:

Автоматизоване самообслуговування: клієнти хмарних сервісів можуть самостійно управляти обчислювальними ресурсами без прямої взаємодії з провайдером.

Мережева доступність: хмарні сервіси доступні через інтернет або приватні мережі з використанням стандартизованих протоколів.

Спільне використання ресурсів: обчислювальні ресурси об'єднуються в загальний пул, з якого здійснюється розподіл між користувачами сервісів.

Гнучке масштабування: можливість оперативно змінювати обсяг використовуваних ресурсів як у більшу, так і в меншу сторону.

Вимірюваність послуг: використання ресурсів постійно відстежується, а оплата нараховується відповідно до обсягу споживання.

Розвиток та впровадження хмарних технологій, з їх численними характеристиками та моделями обслуговування, супроводжується зростаючою вразливістю до різноманітних загроз безпеки [3]. Щоденні новини висвітлюють проблеми безпеки хмарних обчислень, які стали основним бар'єром для їх широкого впровадження. Тому важливо дослідити вплив хмарних технологій на існуючі проблеми безпеки, де ключовим фактором є вразливості системи. Традиційні вразливості мережевої безпеки набувають нового значення в контексті хмарних обчислень, які також створюють додаткові ризики. Стандарт ISO 27005 визначає ризик як потенційну можливість використання вразливостей активу загрозами, що може завдати шкоди організації, враховуючи ймовірність події та її наслідки. За таксономією ризиків Open Group, оцінка базується на двох ключових факторах: частоті виникнення шкідливих подій та масштабі потенційних втрат. Успішна експлуатація вразливості залежить від частоти спроб зловмисника та його рівня доступу до цілей безпеки. Також важливим є співвідношення між потенціалом атаки та захисними можливостями системи. Open Group визначає вразливість як ймовірність нездатності активу протистояти діям зловмисника. Цей другий фактор веде нас до потужного визначення

вразливість [4]. Згідно з визначенням таксономії ризиків Open Group, вразливість представляє собою ймовірність нездатності активу чинити опір діям зловмисника.

Вразливість виникає у випадках, коли існує невідповідність між потенціалом атакуючої сторони та можливостями системи протидіяти цьому потенціалу. Відповідно, вразливість завжди характеризується через призму протистояння або спроможності системи витримати різні види атак. Можна простежити тісну взаємозалежність між вразливостями та ризиками у хмарному середовищі, проаналізувавши структуру факторів ризику, починаючи з правої частини.

З точки зору користувача хмарних послуг, перехід до хмарних обчислень не має суттєвого впливу на праву частину дерева, яка відображає потенційний масштаб майбутніх втрат. Однак ліва частина, що стосується частоти виникнення втрат, зазнає значних змін при впровадженні хмарних технологій. Міграція від традиційної IT-інфраструктури до хмарної може суттєво вплинути на рівень доступу потенційного зловмисника, його мотивацію, а також на необхідні зусилля та ризики, пов'язані з атакою (рисунок 1).

Рисунок 1 – Програмне забезпечення як сервіс.

Після розгляду абстрактної моделі хмарних обчислень та аналізу концепції вразливості, можемо сформулювати точне визначення специфічних хмарних вразливостей. Під хмарними вразливостями розуміються слабкі місця, що виникають внаслідок впровадження різноманітних хмарних сервісів та їх особливостей. У широкому контексті такі вразливості характеризуються чотирма основними показниками.Уразливість відповідає критеріям бути специфічним для хмари, якщо це так:

а) є природним для основної хмари або є місцевим у ній обчислювальна техніка;

б) має головну причину в одній із п’яти основні характеристики хмари;

в) виникає при хмарних інноваціях, основні обчислювальні технології роблять реалізація різних засобів безпеки засоби керування громіздкі або неможливі;

г) є звичайним для різних сучасних технологій хмарних пропозицій.

Тепер кожен із цих чотирьох покажчиків є специфічним для хмари вразливість обговорюється нижче.

Далі розглянемо вразливі хмарні технології. Ключові технологічні рішення в хмарних середовищах мають слабкі місця в різних формах свого прояву. Це означає, що вразливі можуть бути притаманні самій технології або виникати через особливості сучасних реалізацій. Раніше ми вже називали основні технологічні компоненти хмарної інфраструктури, зокрема веб-додатки, служби, рішення з віртуалізації IaaS та криптографічні механізми.

Серед типових прикладів вразливостей - проблеми з управлінням сеансами та їх викраденням у веб-додатках, вихід за межі віртуальної машини внаслідок особливостей віртуалізації, а також недосконала або застаріла криптографія.

Природа віртуалізації створює передумови для певної втечі зловмисника з віртуалізованого середовища. Відтак вразливість віртуальної втечі визнана невід'ємною характеристикою віртуалізації та críticos значною для хмарних обчислень.

Веб-технології вимагають підтримки стану сеансу, однак протокол HTTP є ефективним такої властивості. За наявності чисельних методів реалізації сесійного управління, основні підходи залишаються вразливими до викрадання сеансів. Отже, проблеми управління та безпеки сеансів є актуальними для хмарних обчислень. Крім того, постійний розвиток криптоаналізу призводить до виявлення нових методів злому криптографічних алгоритмів, що робить їх менш захищеними. Таким чином, криптографічні вразливості набувають дедалі більшого значення в хмарних обчисленнях, оскільки використання криптографічного захисту є практично незначним для забезпечення конфіденційності та цілісності даних у хмарному середовищі [5].

Вразливості базових характеристик хмарних обчислень. У попередньому обговоренні були розглянуті п'ять ключових характеристик хмарних обчислень, визначених NIST. Розглянемо вразливості, що виникають внаслідок цих фундаментальних особливостей:

Вразливості розподіленої природи: Розподілена архітектура хмарних обчислень підвищує ризик несанкціонованого доступу та порушень безпеки.

Проблеми стандартизації на різних рівнях: Забезпечення належної гнучкості хмарних обчислень становить серйозну проблему. Це призводить до зростання залежності клієнтів від конкретного постачальника послуг, підвищуючи ризик "хмарного полону" та загальну вразливість. Вразливості при відновленні даних: Особливості об'єднання ресурсів та еластичності дозволяють різним користувачам використовувати одні й ті ж ресурси в різний час. При використанні ресурсів для зберігання даних виникає можливість доступу та відновлення інформації попередніх користувачів.

Вразливості багатокористувацького адміністрування: Характеристика "самообслуговування на вимогу" передбачає наявність інтерфейсу управління, доступного користувачам хмарних сервісів. На відміну від традиційних систем, де доступ до адміністративних функцій мають лише окремі адміністратори, в хмарі ризик несанкціонованого доступу значно вищий. Таким чином,

багатокористувацька адміністративна інфраструктура є суттєвою вразливістю хмарних систем.

Визначення хмарних обчислень NIST забезпечує надійну основу для аналізу проблем безпеки. Недоліки в існуючих механізмах безпеки, коли хмарні інновації ускладнюють впровадження стандартних заходів захисту, створюють специфічні хмарні вразливості, які також називають "проблемами контролю". Розглянемо деякі приклади:

Віртуалізовані мережі мають обмежені можливості контролю. Традиційне мережеве зонування на основі IP-адрес стає неефективним. Управління ключами безпеки та їх зберігання потребують спеціальної інфраструктури в хмарному середовищі. Через відсутність фіксованої апаратної інфраструктури та географічну розподіленість, застосування стандартних механізмів контролю ключів ускладнюється.

Крім того, традиційні показники безпеки не пристосовані до хмарних інфраструктур. Відсутність стандартизованих метрик безпеки не дозволяє користувачам ефективно моніторити стан захищеності своїх ресурсів у хмарі. До створення та впровадження таких стандартів реалізація механізмів оцінки безпеки, аудиту та звітності залишається складною, витратною або навіть неможливою.

Розглянемо типові вразливості сучасних хмарних середовищ. на відносну молодість ринку, хмарні пропозиції вже демонструють значне різноманіття. Вразливості, характерні для хмарних технологій, здебільшого пов'язані з особливостями найсучасніших сервісних рішень. Серед розширених проблем безпеки виділяються ін'єкційні вразливості та недосконалі схеми автентифікації. таким чином, ін’єкційні атаки здійснюються через маніпулювання вхідними даними служб або добавок всупереч первинному задуму розробників. Найтиповіші приклади включають SQL-ін'єкції, команди та міжсайтові сценарії, коли шкідливі вхідні дані неправильно працюють на рівнях бази даних, операційної системи або браузера користувача. Не менш критичною проблемою є слабкі механізми автентифікації. Розглянемо традиційну схему входу за

допомогою імені користувача та пароля. Основні фактори вразливості такої системи, пов'язані з двома аспектами:

По-перше, це небажана поведінка користувачів - вибір простих паролів, їх повторне використання та інші ризиковані практики.

По-друге, впровадження однофакторних механізмів автентифікації, які не забезпечують належного рівня захисту. Таким успішним кроком у підвищенні безпеки є впровадження багатофакторної аутентифікації. Такий підхід дозволяє створити більш надійний бар'єр для несанкціонованого доступу та мінімізувати ризики компрометації облікових записів.

1.1 Недоліки та переваги існуючих методів виявлення вразливостей аутентифікації в SaaS-сервісах

В умовах стрімкої еволюції технологій питання безпеки набуває першочергового значення, особливо у контексті систем аутентифікації SaaS-платформ. Для ефективного захисту користувацьких та корпоративних даних необхідно провести ґрунтовний аналіз сильних та слабких сторін сучасних методологій ідентифікації вразливостей у механізмах аутентифікації SaaS-рішень (таблиця 1) [7].

Таблиця 1 – Аналіз існуючих методів виявлення вразливостей аутентифікації в SaaS-сервісах

Метод виявлення вразливостей	Опис методу	Переваги	Недоліки	Приклад успішного використання
Аудит безпеки	Проведення систематичного перегляду	Дозволяє виявити	Висока витратність	Зменшення кількості

	безпеки для виявлення слабких місць.	потенційні вразливості.	часу і ресурсів.	несанкціонованих доступів.
Сканування вразливостей	Використання інструментів для автоматизованого виявлення вразливостей.	Швидка і ефективна ідентифікація проблем.	Може давати помилкові позитиви.	Забезпечення відповідності стандартам безпеки.
Пентестинг (тестування на проникнення)	Спроби емулювати атаку для оцінки безпеки системи.	Моделює реальні атаки та вразливості.	Вимагає кваліфікованих фахівців.	Виявлення вразливостей, недоступних іншим методам.
Аналіз журналів	Систематичний перегляд журналів подій для виявлення аномалій.	Виявлення непередбачуваних активностей.	Може потребувати значних обчислювальних ресурсів.	Виявлення несанкціонованого доступу через аналіз активності
Використання машинного навчання	Використання алгоритмів для виявлення змін та аномалій у поведінці системи.	Здатність виявляти нові та розуміти складні атаки.	Вимагає великого обсягу даних для навчання моделі.	Адаптація до еволюції загроз та виявлення навіть хитрих атак.

При дослідженні механізмів аутентифікації-вразливостей у SaaS-середовищах стає очевидним, що не існує уніфікованого підходу. Найбільш результативною стратегією може стати інтегрована методика, яка поєднує в собі найефективніші практики та технологічні рішення. Визначальним фактором

забезпечення кібербезпеки є усвідомлення її безперервної природи. Тільки багатовекторний підхід, що включає глибоке розуміння сучасних загроз, впровадження інноваційних технологій та постійне навчання користувачів, передбачено створення дієвого захисного механізму в мінімальному технологічному просторі. Жоден окремий метод не може гарантувати абсолютну безпеку. Натомість, комплексне поєднання різних стратегій, превентивних заходів та безперервного моніторингу формує надійний фундамент захисту інформаційних систем [8].

1.2 Приклади вразливостей аутентифікації, що були виявлені в різних SaaS-сервісах

Хмарне обчислення пропонує значні переваги для сучасного IT-середовища завдяки унікальним сервісним моделям. Однак вони не відображають потенційних ризиків та викликів у сфері інформаційної безпеки, притаманних будь-яким комунікаційним технологіям. Подібні безпекові питання суттєво впливають на загальну ефективність хмарної інфраструктури.

Відповідальність для забезпечення належного рівня захисту системи та даних розміщується на провайдерах хмарних послуг. Керівництво сервісів змушене впроваджувати чіткі політики та процедури подолання наявних загроз, зокрема через використання технологій віртуалізації, вдосконалення механізмів аутентифікації та криптографічного захисту. Водночас сучасні реалізації цих технологічних рішень мають певні вразливості, які потребують постійної уваги та вдосконалення. Критичним місцем є проведення глибокого аналізу та ідентифікації певних ризиків, а також регулярне впровадження системи моніторингу та аудиту хмарного середовища. Розуміння, оцінка та мінімізація безпекових ризиків є визначальним кроком у забезпеченні надійності та стійкості хмарних обчислювальних інфраструктур [9]. При розміщенні даних, веб-застосунків та сервісів у хмарному середовищі клієнти втрачають безпосередній

контроль над ними, що породжує низку проблем, пов'язаних із захистом інформації та іншими аспектами безпеки.

Оскільки хмарна інфраструктура є спільною, необхідно мінімізувати потенційні ризики несанкціонованого доступу до даних. Це включає вирішення питань конфіденційності інформації, управління ідентифікацією, процедур автентифікації, відповідності нормативним вимогам, забезпечення цілісності та доступності даних, впровадження шифрування та усунення вразливостей мережевих протоколів. Додаткової уваги потребують такі аспекти як: умови угод про рівень обслуговування (SLA) між провайдером та споживачем послуг, взаємодія з третіми сторонами, показники продуктивності, ризики віртуалізації, відсутність єдиних стандартів, процедури аудиту та дотримання законодавчих норм [10].

Існує кілька серйозних ризиків, пов’язаних із безпекою в хмарі (Рисунок 2). Цифри представляють пріоритет відповідно до їх випадків від 1 до 10.

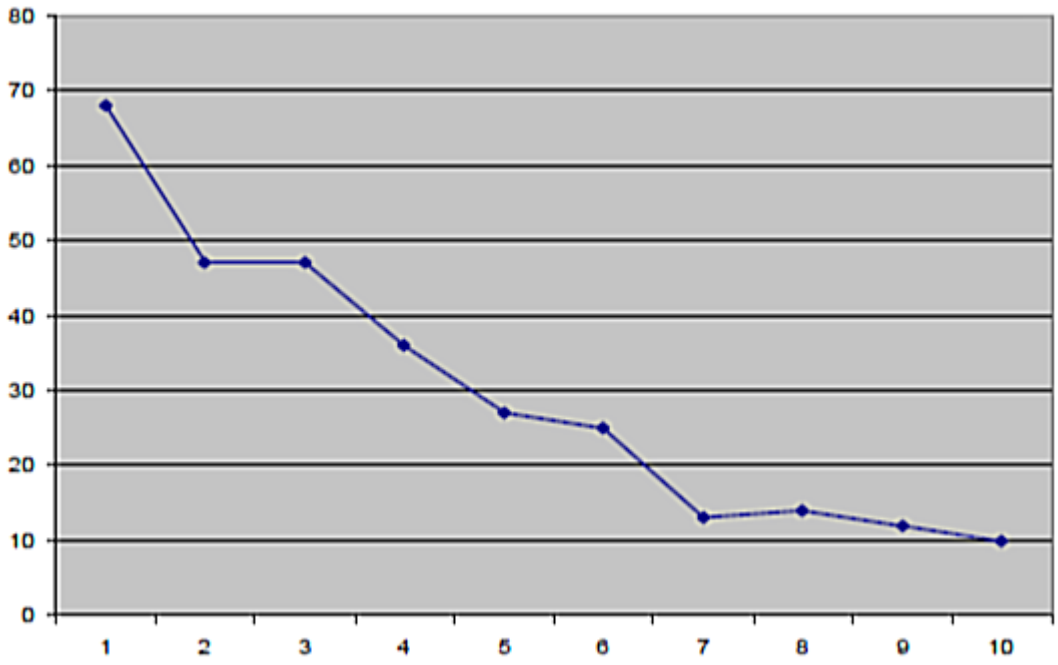

Рисунок 2 - Ризики хмарних обчислень

Розвиток SaaS-технологій докорінно змінив бізнес-ландшафт та щоденні практики користувачів, однак поширення цих сервісів супроводжується

зростанням потенційних ризиків у сфері інформаційної безпеки, особливо в контексті автентифікаційних механізмів.

Дослідження різноманітних інцидентів дозволяє виявити типові вразливості та зрозуміти передумови їх виникнення. Зокрема, критичну загрозу становлять проблеми, пов'язані з безпекою автентифікаційних токенів. Показовим прикладом є масштабний інцидент 2018 року з платформою Facebook, коли внаслідок успішної кібератаки зловмисники отримали несанкціонований доступ до автентифікаційних токенів. Це дозволило порушникам здійснити широкомасштабне викрадення персональних даних користувачів та повністю скомпрометувати механізми інформаційної безпеки соціальної мережі.

Подібні випадки демонструють критичну важливість постійного вдосконалення та моніторингу систем автентифікації в сучасних SaaS-сервісах для запобігання потенційним атакам та витокам конфіденційної інформації. Заходи безпеки: · Впровадити надійну систему шифрування для зберігання токенів автентифікації. · Запровадити систему двоетапної верифікації (2FA) як додатковий рівень захисту.

1. Ненадійні паролі. У 2019 році було виявлено значну вразливість у системі Dropbox через недостатньо суворі вимоги до паролів [11]. Представники сервісу підтвердили, що деякі користувацькі акаунти опинились під загрозою через використання занадто простих комбінацій.

Заходи безпеки: · Встановити обов'язкові вимоги щодо складності паролів. · Впровадити автоматизовані системи аналізу надійності паролів для виявлення поширених та слабких комбінацій.

2. Фішингові атаки. У 2020 році на Salesforce було здійснено фішингову атаку, під час якої зловмисники намагались отримати доступ до конфіденційних даних користувачів через методи соціальної інженерії.

Заходи безпеки: · Проводити регулярні навчання користувачів щодо розпізнавання фішингових загроз. · Впровадити системи виявлення аномальної активності та поведінкового аналізу.

3. Неефективна обробка помилок автентифікації. Деякі SaaS-платформи надають надмірно детальну інформацію про помилки входу, що може сприяти проведенню атак методом перебору. Наприклад, повідомлення "логін вірний, але пароль невірний" спрощує процес злому.

Заходи безпеки: · Використовувати уніфіковані повідомлення про помилки для всіх випадків невдалої автентифікації. · Інтегрувати CAPTCHA та інші механізми захисту від автоматизованих атак.

4. Слабкі механізми відновлення паролів. Неправильно реалізовані процедури відновлення доступу можуть призвести до несанкціонованого доступу [12].

Приклад: · При відновленні паролю через електронну пошту існує ризик перехоплення доступу через скомпрометовану поштову скриньку.

Заходи безпеки: · Застосовувати надійні методи верифікації, такі як надсилання одноразових кодів на верифіковані мобільні номери.

5. Недостатній захист від захоплення сесії. Вразливості у передачі автентифікаційних даних можуть призвести до перехоплення користувацьких сесій.

Заходи безпеки: · Забезпечити захищене з'єднання через SSL/TLS протоколи. · Впровадити ефективну систему управління токенами та сесіями.

6. Небезпечне зберігання паролів. Зберігання паролів у незахищеному або слабко захищеному форматі створює серйозні ризики безпеки.

Заходи безпеки: · Забезпечити надійне хешування всіх паролів. · Використовувати сучасні криптографічні алгоритми для хешування.

Всі ці приклади демонструють, що забезпечення безпеки автентифікації вимагає постійної уваги та комплексного підходу, включаючи активну взаємодію з користувачами [13]. Систематичний моніторинг та оновлення систем безпеки є критично важливими для підтримки належного рівня захисту SaaS-сервісів від сучасних кіберзагроз.

У сучасному цифровому середовищі постійно з'являються нові види загроз та методи атак, тому організаціям необхідно регулярно проводити аудит своїх систем безпеки та оновлювати політики автентифікації. Впровадження багаторівневого захисту, постійний моніторинг підозрілої активності та навчання персоналу щодо найкращих практик кібербезпеки допоможуть значно знизити ризики несанкціонованого доступу до корпоративних ресурсів. Крім того, важливо підтримувати баланс між надійністю захисту та зручністю використання систем для кінцевих користувачів, оскільки занадто складні механізми безпеки можуть призвести до того, що користувачі шукатимуть шляхи їх обходу.

2. ВИКОРИСТАННЯ MITRE ATT&CK ДЛЯ ІДЕНТИФІКАЦІЇ ТА АНАЛІЗУ ВРАЗЛИВОСТЕЙ АУТЕНТИФІКАЦІЇ В SAAS-СЕРВІСАХ

MITER ATT&CK є комплексним фреймворком кібербезпеки, що складається з впорядкованої колекції методів та стратегій, які деталізують поведінку кіберзловмисників упродовж різних стадій атаки. Розроблений на базі практичних спостережень, цей ресурс надає структуровану класифікацію тактичних прийомів, технік та процедур (TTP), які слугують фундаментальним інструментом для створення моделей та методологій аналізу кіберзагроз у різних інформаційних середовищах [14].

Стратегія розкриває потенційний намір противника провести напад, а методологія детально розкриває механізми реалізації цього наміру. Регламенти висвітлюють поглиблені підходи з точними технічними деталями. Інформаційний масив є легкодоступним для будь-якого користувача незалежно від його соціального контексту. Більше того, він постійно оновлюється завдяки актуальним подіям у сфері безпеки та вдосконаленню розуміння новітніх атакувальних прийомів (рисунок 3).

Рисунок 3 - Захист SaaS – сервісів на основі матриці MITRE ATT&CK

Використання фреймворку MITRE ATT&CK для ідентифікації вразливостей у протоколах автентифікації користувачів у хмарних сервісах передбачає такі етапи [15]:

1. Формування цілей. Компанія окреслює пріоритети щодо забезпечення безпеки автентифікаційних процесів у власних онлайн-сервісах. Мета може включати виявлення потенційних атак, протидію неправомірному використанню прав доступу, гарантування цілісності облікових записів тощо.

2. Дослідження загроз. Організація ретельно вивчає матрицю MITRE ATT&CK, концентруючись на специфічних тактиках і методиках, пов'язаних з механізмами входу в систему. Проводиться комплексний аналіз потенційних ризиків та уразливостей.

3. Розробка захисних механізмів. Компанія формує та реалізує стратегію протидії вразливостям автентифікаційних систем. До захисних заходів можуть входити системи моніторингу, інструменти реагування на інциденти, аналітичні платформи тощо.

4. Спостереження та діагностика. Впроваджуються інструменти контролю для виявлення нестандартної або підозрілої активності в контексті користувацької автентифікації. Зокрема, аналізуються спроби неправомірного використання привілеїв, недозволеного доступу, використання некоректних автентифікаційних даних.

5. Реагування на інциденти. За умови виявлення підозрілої активності або атаки на систему автентифікації, організація негайно вживає заходів для припинення загрози, відновлення системної безпеки та превенції подібних інцидентів у майбутньому.

6. Аналітика та вдосконалення. Компанія проводить ретроспективний аналіз результатів виявлення вразливостей та послідовно покращує власні безпекові практики. Це може включати оновлення внутрішніх політик безпеки, впровадження новітніх технологічних рішень, проведення освітніх програм для користувачів.

Використання методології MITER ATT&CK дозволяє компаніям здійснити глибокий аналіз вразливостей системи автентифікації в хмарних додатках, що

дає детальне виявлення про можливості ризиків та разом розробити цільові стратегії посилення захисту облікових механізмів.

Ідентифікація наявних вразливостей системи автентифікації в хмарних сервісах є ключовим аспектом захисту інформаційних активів та протидії неправомірному входу. Організації мають у своєму арсеналі низку методологій для діагностики та мінімізації ризиків безпеки. У додатку представлена порівняльна характеристика різних стратегій виявлення недоліків механізмів аутентифікації в SaaS-платформах з детальним аналізом їх сильних та слабких сторінок.

Таблиця 2 - Підходи до виявлення недоліків у механізмах аутентифікації в SaaS сервісах

Назва підходу	Опис підходу	Переваги	Недоліки
Аналіз журналів та моніторинг	Цей підхід полягає в аналізі журналів активності та моніторингу подій, пов'язаних з аутентифікацією.	Можливість виявлення підозрілої активності, нестандартних аутентифікаційних звернень або намагань несанкціонованого доступу.	Велика кількість згенерованих подій, що потребують ефективного моніторингу та аналізу.
Перевірка наявності актуальних патчів та вразливостей	Цей підхід передбачає оцінку наявності актуальних патчів і визначення потенційних вразливостей у	Дозволяє виявити відомі недоліки та вирішити їх шляхом встановлення патчів або розробки	Складність виявлення нових невідомих вразливостей та залежність від постачальників SaaS-сервісів для вирішення проблем безпеки

	механізмах аутентифікації	відповідних заходів безпеки.	
Тестування проникнення	Цей підхід полягає в проведенні спеціалізованих тестів проникнення для ідентифікації слабких місць у механізмах аутентифікації.	Виявлення потенційних проблем та використання реалістичних сценаріїв атак.	Висока вартість та потреба у висококваліфікованих спеціалістах для проведення тестування.
Аналіз вразливостей з використанням інструментів автоматичного сканування	Цей підхід використовує спеціалізовані інструменти для автоматичного сканування системи з метою виявлення вразливостей у механізмах аутентифікації.	Виявляє низькорівневі проблеми та надає широкий огляд стану безпеки системи.	Висока кількість фальшиво-позитивних результатів та потреба додаткової перевірки та підтвердження виявлених вразливостей.

Фреймворк ATT&CK слугує фундаментальним джерелом для формування спеціалізованих підходів до аналізу кіберзагроз, охоплюючи інтереси комерційних організацій, державних структур та професійної спільноти розробників рішень у сфері інформаційної безпеки.

Фреймворк MITRE ATT&CK представлений трьома різноспрямованими матрицями: Enterprise, Mobile та PRE-ATT&CK. Кожна з матриць містить унікальний набір тактик і технік, специфічних для свого контексту.

● Матриця Enterprise охоплює методики та стратегії, призначені для операційних систем Windows, Linux і MacOS.

● Mobile фокусується на тактиках та прийомах, релевантних для мобільних екосистем і пристроїв.

● PRE-ATT&CK деталізує тактику та підходи, що передують безпосередній спробі вторгнення в конкретну мережеву інфраструктуру або системний простір.

Розробляючи ATT&CK, організація MITRE реалізує власну місію створення більш безпечного світового кіберсередовища, консолідуючи професійні спільноти для розвитку ефективних стратегій кібербезпеки. Фреймворк ATT&CK є повністю відкритим та безкоштовним для використання будь-якими фізичними та юридичними особами [16].

За минуле п’ятнадцятиріччя технологічний ландшафт зазнав кардинальних змін: від локальних серверів і стаціонарних робочих станцій до гнучких хмарних середовищ з міграцією між високими платформами та одночасним використанням хмарних додатків. Незалежно від архітектурної складності інфраструктури, сучасні системи пропонують універсальне програмне забезпечення, здатні підтримувати роботу різноманітних операційних систем. Водночас кожен вразливий компонент створює точку входження для кіберзловмісників, тому фахівцям з інформаційної безпеки необхідно забезпечити постійний моніторинг та оперативне оновлення всього інсталяційного ресурсу.

2.1 Аналіз механізмів аутентифікації користувачів в SaaS-сервісах

Автентифікація становить складову підсистему інформаційної безпеки. Подібно до загальної безпекової концепції, механізми автентифікації значною мірою ґрунтуються на критичних принципах конфіденційності, цілісності та

доступності; ці параметри перетворюються на ключові критерії при розробці захищених інформаційних систем.

Легкість взаємодії: cloud-сервіси можуть бути вразливими для маніпуляцій зловмисників через надмірно спрощену процедуру реєстрації, де для верифікації достатньо мати єдиний дійсний платіжний інструмент [17].

Безпечність інформаційного обміну: комунікація між користувачами та хмарними сервісами повинна здійснюватися через криптографічно захищені канали зв'язку.

Вразливості програмних інтерфейсів: хмарні сервіси надають доступ до своїх функцій через API, доступні через інтернет. Це створює потенційні ризики, оскільки зловмисники можуть використати такі інтерфейси для компрометації даних корпоративних користувачів.

Внутрішні загрози: персонал провайдера хмарних послуг потенційно має доступ до всіх корпоративних ресурсів клієнтів.

Виклики спільного використання технологій: провайдери хмарних сервісів (SaaS/PaaS/IaaS) застосовують єдину масштабовану інфраструктуру, яка обслуговує множину користувачів одночасно.

За останній період було здійснено значний прогрес у розробці та впровадженні механізмів автентифікації та захисту для мінімізації ризиків втрати чи пошкодження інформації.

Дослідники представили децентралізовану систему на основі реплікації, розроблену для забезпечення захисту від випадкових збоїв компонентів. Візантійські алгоритми стійкості до відмов мають справлятися з такими збоями, продовжуючи виконувати свої функції, проте основні складнощі виникають через помилки виконання та навмисне спотворення даних.

У дослідженні [18] презентовано хмарну інформаційну платформу під назвою «CHARON». Це система зберігання даних, спроможна безпечно та результативно акумулювати й трансферувати інформацію через мультихмарну інфраструктуру задля дотримання юридичних стандартів щодо конфіденційних персональних даних. CHARON реалізує три принципові функціональні

характеристики: (1) не потребує абсолютної довіри до будь-якого учасника системи, (2) не вимагає клієнтського адміністрування серверів, та (3) ефективно опрацьовує великі інформаційні масиви в географічно диверсифікованому середовищі зберігання. Система містить орієнтований на дані протокол лізингу з надійним byzantine-стійким механізмом. Водночас застосування byzantine-резильєнтної технології в хмарному середовищі передбачає збільшення часу затримки порівняно з уніфікованою хмарою. Для оптимізації рішення перспективним убачається впровадження біометричної автентифікації, яка надає додаткові переваги в контексті безпеки, функціональності, контролю та верифікації. Розроблена система представляє захищену віртуальну інфраструктуру з використанням декількох хмар. Вона включає grid-механізм, що функціонує поверх мультихмарної архітектури для оптимального розподілу задач між обчислювальними вузлами. Ці вузли отримують ресурси з різних хмарних платформ, що забезпечує економічну ефективність та високу доступність системи. Для координації задач використовується Oracle Grid Engine, де робочі вузли (як локальні, так і хмарні) виступають у ролі приймачів завдань від головного вузла. Користувачі можуть надсилати завдання через grid-систему після проходження автентифікації. Особлива увага приділяється контролю доступу через загрозу хакерських атак, причому потенційним зловмисником може виявитися особа з легітимним доступом до хмарної інфраструктури.

Для захисту даних пропонується система автентифікації, що базується на двох ключових протоколах: шифруванні на основі атрибутів (ABE) для захисту інформації та підписах на основі атрибутів (ABS) для верифікації користувачів. Комбінація цих протоколів забезпечує анонімність користувачів при роботі з хмарними сховищами. Управління атрибутами здійснюється децентралізовано. Однак, враховуючи виявлені вразливості в DES та впровадження лавинного ефекту в нових алгоритмах шифрування, ці методи потребують оновлення.

Система включає довірений клієнтський компонент та мінімум три хмарні сервіси, що надають послуги баз даних. Хоча провайдери забезпечують надійне

зберігання та управління даними, вони не мають доступу до конфіденційної інформації. Клієнтська частина не зберігає постійних даних, але містить таблицю мапування фрагментів даних та їх розташування.

Досліджується можливість залучення множинних CSP (провайдерів хмарних послуг) для колективного зберігання та підтримки клієнтських даних [19]. Додатково для валідації цілісності та доступності інформації, що зберігається в CSP, застосовується кооперативна модель верифікації даних (cooperative PDP). Послідовність перевірки виглядає наступним чином: спочатку клієнт (власник інформаційного масиву) використовує приватний ключ для первинної обробки файлу, що складається з n блоків. Генерується набір публічної верифікаційної інформації, яка акумулюється в TTP (довірених посередниках), потім файл і відповідні перевірочні мітки передаються CSP з подальшим видаленням локальної копії. Запропонована архітектура спроможна забезпечити специфічні функції зберігання та управління даними, однак такий підхід підвищує складність адміністрування сховища. Зокрема, можливі сценарії перетину блоків даних та наявності інформаційних лакун. Запропоноване рішення щодо захисту геолокаційних даних базується на створенні ієрархічного дерева запитів до бази даних. Це дерево відображає взаємозв'язок між географічними даними та частотою звернень до них. Система додає випадкові шуми до вузлів дерева і генерує модифікований запит як результат, що підвищує рівень захисту інформації про місцезнаходження.

Розроблено також механізм збору даних із підтримкою конфіденційності для бездротових сенсорних мереж (WSN). Основне завдання - забезпечити приватність даних датчиків шляхом унеможливлення аналізу мережевого трафіку та відстеження потоків у WSN. Застосування гомоморфного шифрування (HEF) при зборі компресованих даних перешкоджає аналізу трафіку та гарантує конфіденційність. Проте система захищає лише від внутрішніх загроз, залишаючись вразливою до зовнішніх атак через можливість компрометації проміжних сенсорних вузлів.

Дослідники розробили трикомпонентну систему, що включає вибіркове шифрування HEVC-відео, вбудовування даних у зашифрований відеопотік та їх подальше вилучення. Спершу власник контенту застосовує потокове шифрування до HEVC-потоку перед відправкою в кеш. Подальша система кешування впроваджує приховані комунікативні блоки в зашифроване відео через модуляцію коефіцієнтів. На етапі прийому процедури вилучення та декодування інформації реалізовані паралельно, що надає можливість працювати як з зашифрованими, так і з розшифрованими масивами даних. Водночас, дієвість запропонованого підходу досі не була апробована в складних мультихмарних інфраструктурах.

Дослідники здійснили компаративний аналіз означених систем (рисунок 4), маючи на меті більш структуровано систематизувати проблематику автентифікації та ідентифікувати різноманітні методологічні підходи й технічні рішення, запропоновані науковцями для забезпечення безпеки в багатохмарних середовищах.

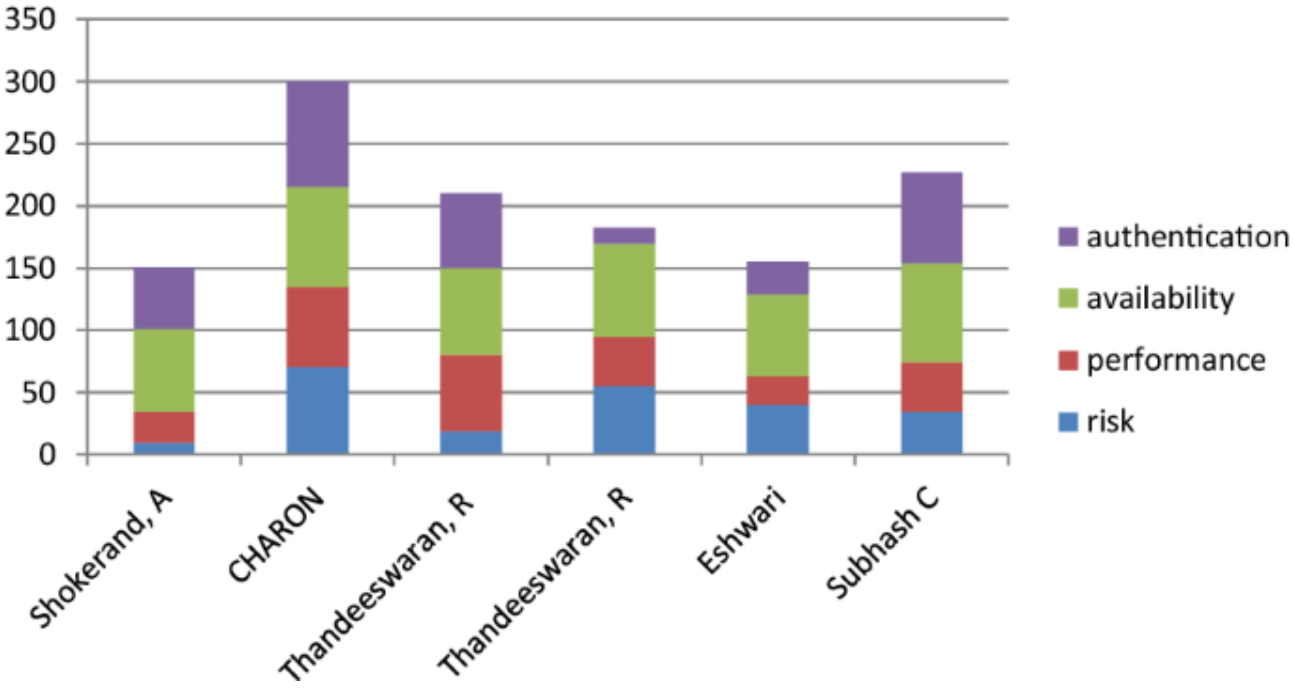

Рисунок 4 - Результати ступеня виконання порівняльних характеристик системи

Попри наявні наукові напрацювання та дослідження в цій галузі, проблема інформаційної безпеки залишається критично актуальною, і користувачі продовжують відчувати занепокоєння щодо потенційної втрати або неправомірного розголошення персональних даних. Як засвідчують дослідження, близько 80% таких інцидентів спричиняються діями кіберзловмисників. Приміром, зловмисник може здійснити привласнення особистості легітимного користувача та в подальшому заволодіти його обліковим записом (рисунок 5). Оскільки порушник системи зазвичай не реагує на верифікаційні повідомлення автентифікаційного сервера (наприклад, на секретні запитання, відомі винятково законному користувачеві), система може filtрувати користувачів на підставі аналізу їхньої поведінки. Однак такого підходу виявляється недостатньо для забезпечення абсолютної безпеки у відкритих та розподілених інформаційних системах.

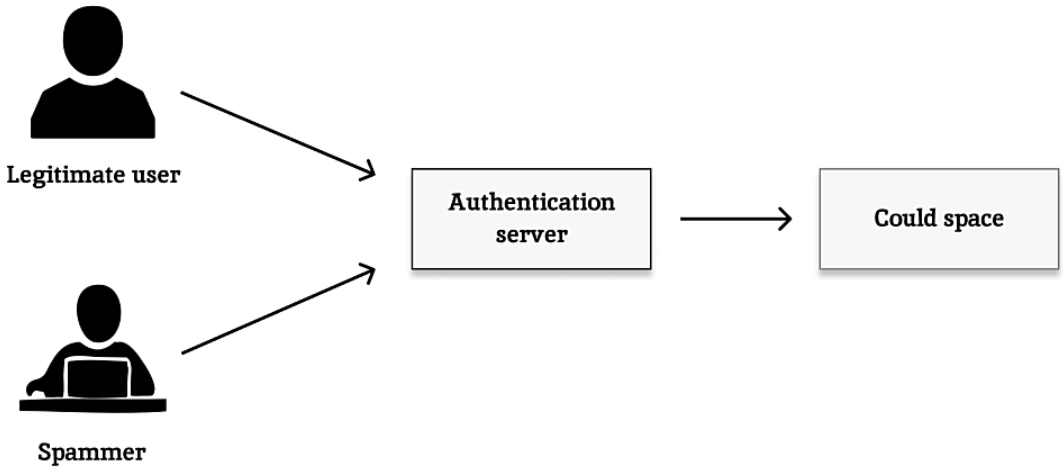

Рисунок 5 – Атака спамера

У публікації [20] дослідники презентують авторську методику забезпечення безпечного доступу до програмних додатків і сервісів у мультихмарному середовищі. Запропонована концепція включає три ключові технологічні підходи: по-перше, передбачається формування віртуальної приватної мережі (VPN) між клієнтом та провайдером; це дозволяє мінімізувати

ризики втрати інформації під час її транспортування та редукує потенціал несанкціонованих вторгнень, забезпечуючи високоякісний захисний механізм.

По-друге, планується застосування асиметричного криптографічного алгоритму RSA для гарантування високого рівня захисту інформаційних масивів у процесі передачі. І, нарешті, передбачено відновлення інформації з множинних джерел (хмарних середовищ), що забезпечує верифікацію цілісності даних через механізм хешування (рисунок 6).

Рисунок 6 – Етапи безпечного доступу до SaaS - сервісів

2.2 Основні концепції та структура MITRE ATT&CK

У 2011 році компанія Lockheed Martin запропонувала концепцію Cyber Kill Chain - модель, яка описує послідовні етапи кібератаки на організацію. Ця модель демонструє поступовий процес від початкової розвідки через застосування шкідливих інструментів до встановлення контролю над цільовою системою. Знання цієї структури допомагає фахівцям з кібербезпеки ефективніше розміщувати захисні механізми та впроваджувати заходи протидії.

Після впровадження концепції Kill Chain організація MITRE провела дослідження методів кіберзловмисників і створила загальнодоступну систематизацію. MITRE - це неприбуткова організація, що керує федеральними дослідницькими центрами (FFRDC). Ці центри надають підтримку різним державним структурам США у сферах авіації, оборони, медицини, національної та кібербезпеки. База знань MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) представляє собою систематизовану структуру для моніторингу дій кіберзловмисників, що охоплює різні стадії атаки. Перший варіант ATT&CK, розроблений у 2013 році, містив вісім тактичних категорій та приблизно 70 технік атак [21]. Модель еволюціонувала, охоплюючи дедалі більше джерел і технологічних рішень. Десята версія матриці включає 14 тактик та понад 500 інтегрованих технік і підтехнік (Strom et al., 2020). Порівняно з фреймворком Lockheed Martin Cyber Kill Chain, MITRE ATT&CK пропонує більш деталізований інструментарій, що надає захисникам розширений рівень абстракції для демонстрації 19 варіантів поведінки супротивника. Архітектура MITRE ATT&CK постійно вдосконалюється завдяки активній підтримці професійної спільноти.

Структура ATT&CK деталізує механізми первинного проникнення зловмисників в організаційні системи, їхнє подальше переміщення, ескалацію привілеїв та стратегії уникнення захисту. Цей інструментарій дозволяє ідентифікувати специфічні методи, які використовуються при цілеспрямованих атаках. ATT&CK систематизує протиправну поведінку через набір тактик,

прийомів і підтехнік, застосовуваних супротивниками в різних категоріях. Фреймворк має універсальне призначення – може використовуватися як в наступальному, так і в оборонному контексті (Strom et al., 2017). У своєму магістерському дослідженні Холлберг продемонстрував валідну реалізацію застосування MITRE ATT&CK для візуалізації та детекції вторгнень.

У структурі ATT&CK тактичний рівень представляє найвищий ступінь узагальнення. Тактики відображають мотивацію та цілі зловмисника, тоді як методи та їх підвиди розкривають конкретні способи реалізації цих намірів. Актуальна версія 10 матриці MITER ATT&CK для корпоративного середовища включає 14 різних тактичних категорій. Кожна тактика має свій унікальний ідентифікатор, що особливо важливо при програмній інтеграції фреймворку [22].

Розглянемо випадок, коли кінцевою метою зловмисника є отримання викупу через ransomware-атаку. Така стратегічна ціль класифікується як TA0040 (Impact). Для досягнення цієї мети зловмисник має виконати серію проміжних тактичних завдань. Типова атака починається з проникнення в мережу організації (TA0001 - Initial Access). Після проникнення зловмисник проводить розвідку для визначення шляху до цілі (TA0007 - Discovery). Подальше просування вимагає підвищення привілеїв (TA0004 - Privilege Escalation) та латерального руху мережею (TA0008 - Lateral Movement). Під час цих дій зловмисник застосовує різні техніки обходу систем захисту (TA0005 - Defense Evasion), включаючи виконання шкідливого коду для подолання захисних механізмів (TA002 - Execution). Важливо відзначити, що послідовність виконання цих проміжних завдань може варіюватися.

Таблиця 3 - Тактика ATT&CK v10 матриці підприємства

ID	Назва	Опис
TA0043	Розвідка	Противник намагається зібрати інформацію для планування майбутніх операцій.

TA0042	Ресурс Розвиток	Противник намагається встановити ресурси, їх можна використовувати для підтримки операцій.
TA0001	Початковий доступ	Зловмисник намагається проникнути у вашу мережу.
TA0002	Виконання	Зловмисник намагається запустити шкідливий код.
TA0003	Наполегливість	Противник намагається втриматися.
TA0004	Підвищення привілеїв	Противник намагається отримати вищий рівень дозволів.
TA0005	Ухилення від захисту	Противник намагається уникнути виявлення.
TA0006	Обліковий доступ	Зловмисник намагається викрасти імена облікових записів і паролі.
TA0007	Відкриття	Противник намагається з'ясувати ваше навколишнє середовище.
TA0008	Бічний рух	Противник намагається пройти через ваше навколишнє середовище.
TA0009	Колекція	Зловмисник намагається зібрати цікаві для нього дані, для власної мети.
TA0011	Команда і контроль	Противник намагається зв’язатися з скомпрометованими системами для їх контролю.
TA0010	Ексфільтрація	Зловмисник намагається викрасти дані.
TA0040	Вплив	Противник намагається маніпулювати, переривати або знищити ваші системи та дані.

Під час кібератаки зловмисник не завжди потребує використання всього арсеналу тактичних прийомів для реалізації стратегічного задуму (за даними Cybersecurity and Infrastructure Security Agency, 2021).

Фреймворк MITRE ATT&CK розкриває механізми досягнення супротивниками тактичних цілей через специфічні дії. Ці методи фокусуються на поясненні «яким чином» та частково на «що» отримує зловмисник після виконання певної дії. Оскільки існує множинність підходів для реалізації тактичних завдань, кожна категорія тактики містить декілька технік. Десята версія матриці MITRE ATT&CK налічує 188 технік, а відмінності між тактиками [23], техніками та підтехніками проілюстровано частковим представленням матриці на рисунку 7.

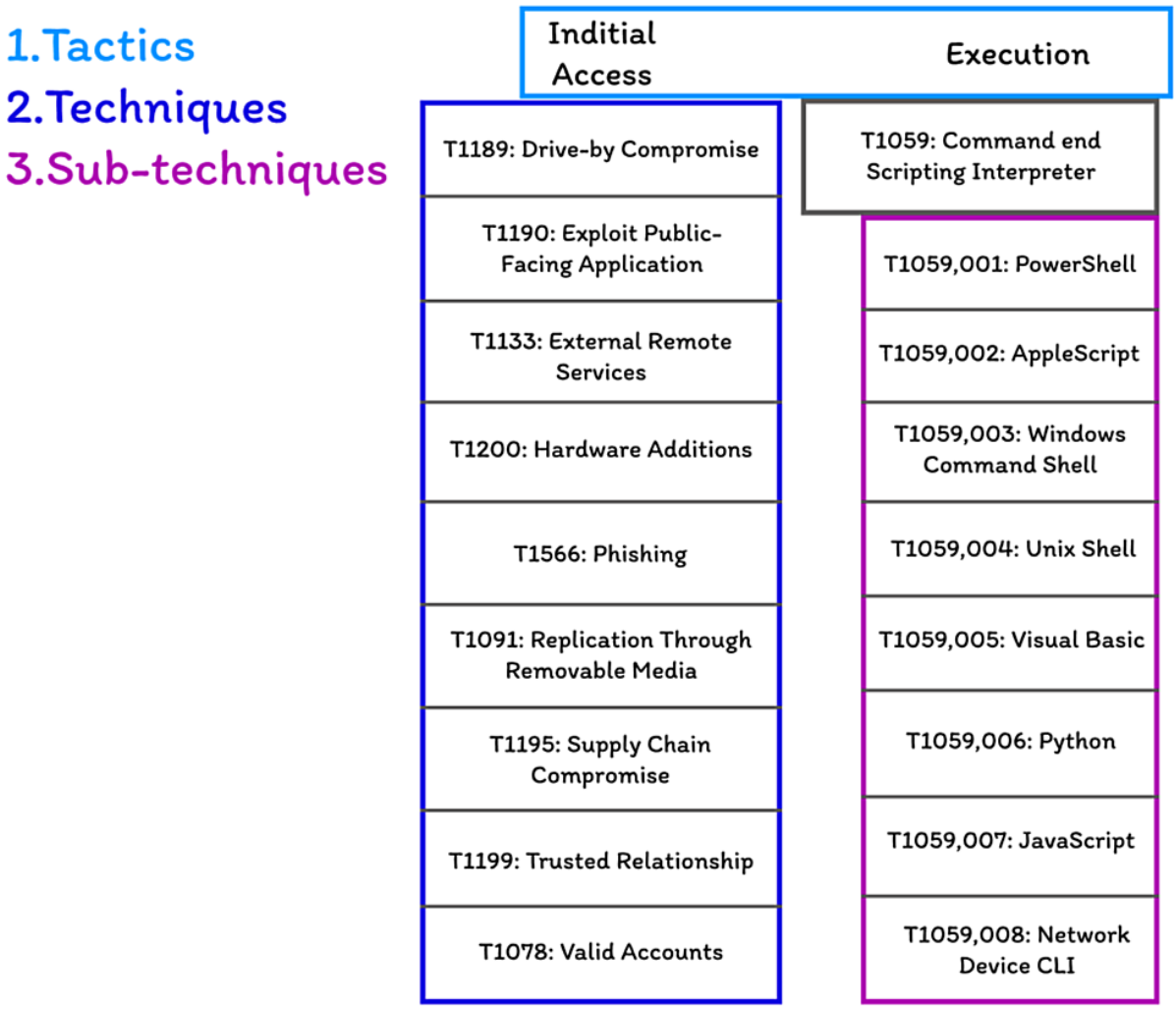

Рисунок 7 - Тактика, техніка та підтехніка MITRE ATT&CK

Методологія MITER ATT&CK Enterprise дозволяє співвідносити одну атакуючу дію з кількома технічними прийомами. Наприклад, якщо атакуючий використовує шкідливе програмне забезпечення, що містить обфусковані VBA макроси, які запускають cmd.exe для виконання шкідливого PowerShell-скрипта, така операція відповідає одразу декільком технікам ATT&CK: використання скриптів (T1064), застосування командного рядка (T1059) та експлуатація PowerShell (T1086).

У кіберзахисті трапляється, що одна конкретна техніка може бути інструментом для реалізації різних стратегій нападу. Розглянемо техніку T1078 про використання легітимних облікових записів – вона задіяна одночасно в чотирьох тактичних напрямках: ухиленні від захисту, закріпленні в системі, розширенні повноважень і встановленні первинного контролю. За даними дослідження Mandiant (2022), кіберзлочинці зосереджуються на пошуку адміністративних профілів саме на етапі первинного проникнення. Після успішного отримання доступу зловмисники використовують захоплені облікові записи для горизонтального переміщення в інфраструктурі, збереження присутності та реалізації кінцевої мети атаки.

Субтехніки надають найдетальнішу характеристику способів реалізації супротивниками тактичних завдань. Вони пропонують більш глибокий технічний опис дій порівняно зі стандартними техніками. Як правило, такі підходи орієнтовані на специфічні операційні середовища, зокрема Linux або Windows. (за матеріалами Strom та колег, 2020) Десята версія матриці ATT&CK налічує 379 субтехнік.

Приміром, Техніка T1222 – Модифікація прав доступу до файлових об'єктів та директорій розподілена на два субметоди, представлені на відповідній ілюстрації. Ідентифікація субметодів здійснюється через додавання чисельного номера після базового ідентифікатора техніки (.001).

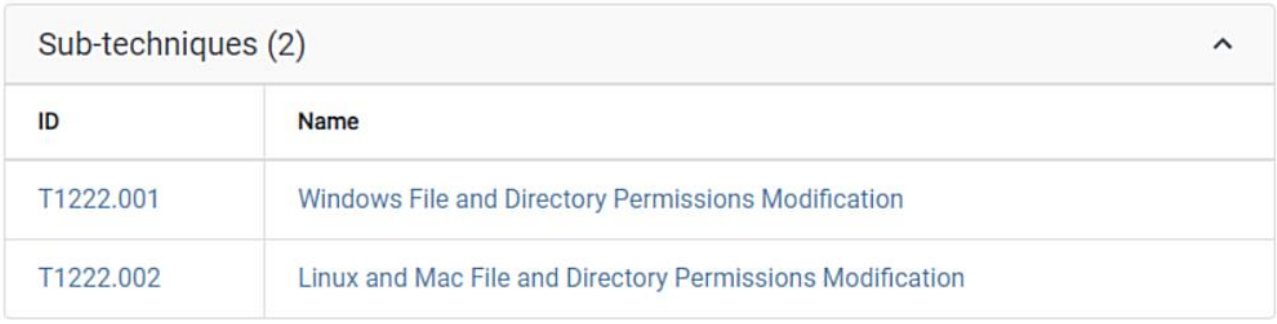

Рисунок 8 – Допоміжні методи модифікації дозволів на файли та каталоги

Процедури висвітлюють практичну реалізацію того, що зловмисники застосовують для конкретних Технік або Допоміжних технік. Вони слугують для деталізації використання технічних прийомів у реальних сценаріях, паралельно демонструючи різноманітні варіанти поведінки під час їхнього виконання. Процедури здатні ідентифікувати специфічні інструментальні засоби, які супротивники використовують для досягнення власних тактичних цілей. Методологія ATT&CK передбачає використання інформаційних джерел. Під джерелами даних розуміють технічні засоби та програмні комплекси, здатні забезпечувати інформаційні сліди та журнали для дослідження конкретних технік або підтехнік кібератак. На сьогодні організація MITRE пропонує каталог з 38 різноманітних інформаційних джерел. Серед найпоширеніших джерел можна виділити, наприклад, систему автентифікації Active Directory, мережеві екрани та системний реєстр операційної системи Windows. (The MITER Corporation, n.d.) У наступному розділі дослідження буде представлено перелік додаткових джерел даних, що виходять за межі стандартного набору MITRE ATT&CK [25].

3. ЗАПРОПОНОВАНИЙ ПІДХІД ДЛЯ ЗАХИСТУ АУТЕНТИФІКАЦІЇ В SAAS- СЕРВІСАХ

Модель програмного забезпечення як послуги (SaaS) є інноваційним підходом до розповсюдження додатків, де програмні рішення та пов'язані бази даних розміщуються в хмарному середовищі. Специфіка SaaS та хмарних технологій, за яких інформація та обчислювальні процеси перебувають поза безпосереднім контролем користувача, актуалізує питання захисту персональних даних. Дослідження галузі демонструють, що безпека та конфіденційність є визначальними викликами при впровадженні хмарних рішень. У багатокористувацьких SaaS-системах клієнти мають серйозні побоювання щодо збереження приватності власних даних через спільне використання інфраструктури.

Постають критичні питання: як гарантувати доступ до інформації виключно авторизованим користувачам? Яким чином унеможливити несанкціонований доступ до чужорідних даних? Для вирішення цих викликів пропонується технологія SignedQuery – механізм забезпечення захисту інформації в хмарному середовищі. Технічне рішення гарантує конфіденційність даних, перешкоджаючи випадковому або навмисному доступу до інформації сторонніх клієнтів без порушення функціональності системи. SignedQuery реалізує підхід цифрового підписування клієнтських запитів, що дозволяє серверу ідентифікувати джерело звернення та перевірити належність запитуваних даних. Механізм перехоплює HTTP-об'єкти в інфраструктурі клієнта, генерує цифровий підпис, інтегрує його до заголовків запиту та передає SaaS-провайдеру для автентифікації.

Забезпечення безпеки програмних сервісів, що функціонують у мережі Інтернет, завжди було наскрізною нефункціональною вимогою надзвичайно критичного характеру. Еволюція та стрімке впровадження концепції хмарних обчислень зумовили виникнення комплексу принципово нових викликів у домені кібербезпеки.

Це спровокувало появу концепції "Безпека як послуга" (SecaaS), яка передбачає створення багаторазових програмних рішень, здатних інтегруватися зі стандартними хмарними службами для надання відповідного захисту. У сучасних реаліях постає нагальна необхідність розроблення методик та інструментарію для моделювання потенційних загроз безпеці, а також впровадження технік оцінювання, що дозволяють порівнювати різні проектні рішення та аналізувати їхній вплив на функціональність нових сервісів до безпосередньої реалізації. Традиційні механізми автентифікації забезпечують базовий рівень захисту, проте в умовах постійної еволюції кіберзагроз виникає об'єктивна потреба в удосконаленні систем протидії новітнім атакам. Наша дослідницька група розробила інноваційний підхід до посилення безпеки автентифікації в SaaS-сервісах, якийґрунтується на комплексному аналізі контекстної поведінки користувачів.

Класичні підходи до автентифікації, включаючи паролі та біометричні механізми, демонструють обмежену ефективність перед сучасними витонченими техніками соціальної інженерії та фішингу. Основне завдання розробників - гарантувати максимальний рівень захисту, мінімізувати надмірну технічну складність та водночас зберегти зручність використання для кінцевих споживачів (таблиця 4) [27].

Таблиця 4 - Основні принципи безпеки для хмарних обчислень

№ з/п	Принципи	Коротка характеристика принципів
1.	Прозорість	Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність.
2.	Обмеження за сферами використання	Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників.

3.	Розкриття	Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство.
4.	Система управління безпекою	Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002).
5.	Додаткові можливості у сфері безпеки	Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних.
6.	Розміщення даних	Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані.
7.	Повідомлення про витоки інформації	Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних.
8.	Аудит	Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам відповідних стандартів.
9.	Переносимість даних	Компанії надають замовникам можливість вивантаження даних у стандартному форматі, придатному для передавання через Інтернет.
10.	Звітність	Компанії співпрацюють із замовниками в адекватному розподілі обов'язків під час

		складання звітності «Про приватність і безпеку».

Попри наявні пропозиції, які наразі не здобули широкої підтримки в галузі, існує висока вірогідність формування уніфікованих правил – спочатку в США та Європі, а згодом і в інших державах. Такий підхід сприятиме збалансуванню інтересів користувачів і провайдерів хмарних послуг. Українське законодавство наразі приділяє недостатньо уваги хмарним технологіям, зокрема бракує комплексного договору між споживачем та постачальником хмарних потужностей, тоді як у європейських країнах процес оновлення нормативної бази відбувається досить динамічно.

Концепція доступних комп'ютерних послуг трансформується в реальність. Хмарні технології надають змогу ефективно розв'язувати бізнес-завдання та скорочувати терміни обслуговування. Центри обробки даних отримують можливість розширення клієнтської бази, а розробники можуть концентруватися на створенні інноваційних продуктів.

Експерти прогнозують, що повномасштабної міграції комерційних структур до публічних хмар не відбудеться. Не очікується й повної відмови від власних дата-центрів – натомість dominant стане гібридна модель, яка поєднуватиме традиційні та хмарні інфраструктурні рішення.

Програмні застосунки майбутнього матимуть два компоненти: локальний на комп'ютері користувача та хмарний.Cloud-складова повинна забезпечувати гнучке масштабування – від роботи на одній віртуальній машині до взаємодії з тисячами серверів за потреби.

Необхідно розробити інтелектуальні системи керування енергоспоживанням, які дозволять оптимізувати роботу серверів, пам'яті та мережевої інфраструктури в режимі енергозбереження. Це також важливий аспект інформаційної безпеки.

Наступним кроком має стати не лише юридичне врегулювання технології, а й створення збалансованої моделі взаємовідносин між користувачами та

постачальниками. Питання інформаційної безпеки хмарних сервісів потребують комплексного вдосконалення та розроблення принципово нових підходів.

Базові принципи захисту даних ґрунтуються на трьох ключових складових: конфіденційності, цілісності та доступності. Конфіденційність передбачає максимальний захист інформації та є найсуворішою вимогою інформаційної безпеки. У контексті хмарних обчислень, де дані концентруються в центрах обробки, питання безпеки набувають особливої значущості. Цілісність даних гарантує захист від несанкціонованого втручання, видалення або модифікації. Доступність забезпечує можливість ефективного використання даних з урахуванням потенціалу хмарних технологій.

У представленій моделі застосовується тришарова захисна архітектура системи, де кожен рівень має унікальні функції забезпечення захисту даних у середовищі хмарних обчислень.

· Перший рівень здійснює автентифікацію користувачів через цифрові сертифікати, емітовані уповноваженими органами; здійснює адміністрування кодів доступу користувачів.

· Другий рівень відповідає за криптографічний захист даних користувача та забезпечення конфіденційності певними механізмами.

· Третій рівень призначений для відновлення даних користувача максимально швидким способом.

Підсумковий захист усієї системи становить завершальний бар'єр захисту користувацьких даних. Трирівнева структура дозволяє реалізувати багатофакторну автентифікацію для гарантування цілісності інформації. У випадку нелегітимного втручання в систему автентифікації, коли порушник отримує доступ, наступні рівні шифрування та конфіденційності створюють додатковий захисний механізм.

На цьому етапі відбувається шифрування файлів у разі неправомірного введення ключа доступу. Механізми захисту конфіденційності унеможливлюють повний доступ зловмисника до інформації, що критично важливо для збереження комерційних таємниць ділових користувачів у

хмарному середовищі. Прикінцевий рівень забезпечує швидке відновлення файлів через спеціальні алгоритми, що дає змогу відновлювати дані навіть за умов значних пошкоджень.

Впровадження хмарних технологій висуває принципово нові вимоги до якості інтернет-послуг, які стають критично важливими. Найбільш прогресивними в цьому напрямку є американські телекомунікаційні компанії. У США прийнята практика публічного оприлюднення детальних зобов'язань щодо якості обслуговування, які закріплюються в угодах про рівень сервісу (Service Level Agreements). У разі недотримання провайдером встановлених зобов'язань, передбачається фінансова відповідальність. Не викликає сумніву, що хмарні обчислення докорінно трансформували комунікаційні процеси, цифрову економіку, соціальну взаємодію та розважальну індустрію. Водночас спостерігається стрімке зростання попиту на інтернет-орієнтовані додатки. Практично всі сфери життєдіяльності – від підприємств і розважальних пристроїв до складних технічних систем (авіаційні комплекси, системи управління польотами), критично важливих безпекових та медичних систем, пристроїв Інтернету речей – мають мережеве підключення з різноманітних причин: онлайн-оновлення, розподілені додатки, колективні проекти та взаємодія з серверами.

Внаслідок цього постійно зростає потреба в захищених додатках та довірчих комунікаціях. Кіберзагрози набувають дедалі витонченіших форм – від елементарного спаму та фішингу до масштабних атак, пов'язаних з викраденням персональних даних, відмиванням коштів і кібертероризмом. Існує реальний ризик того, що масштабна кібератака може паралізувати системи управління, вивести з ладу електромережі, несанкціоновано впливати на інженерні споруди, порушити комунікаційні та транспортні мережі, провокуючи масову паніку. Такі загрози становлять серйозну небезпеку, оскільки сучасні особи, державні інституції, комерційні структури та бізнес-організації значною мірою залежать від комп'ютерних та мобільних технологій у процесах комунікації та керування. Кожна потенційна кібератака може слугувати передвісником масштабної

терористичної або військової агресії, що актуалізує питання кібербезпеки на глобальному рівні.

Спостерігається стрімке зростання різноманітних хмарних служб, зокрема у сферах охорони здоров'я, електронного навчання та цифрового виробництва. Дослідники Kostoska, Gusev та Ristov (2014) презентували інноваційну платформу стійкості (PaaS), яка забезпечує автоматичну інтеграцію та обмін між різними хмарними середовищами. Han et al. (2016) запропонували алгоритм консолідації віртуальних машин з урахуванням залишкового використання ресурсів. Xu (2013) розробив інтерактивну хмарну виробничу систему (ICMS), що дозволяє об'єднувати виробничі та бізнес-можливості в єдиний ресурсний пул. Срівастава та колеги (2015) висвітлили потенціал технологій електронної медицини, які завдяки хмарним сервісам та Інтернету речей уможливлюють низьковартісні консультації експертів worldwide для проведення складних медичних маніпуляцій. Дослідження також акцентує на необхідності інтеграції різноманітних технологічних рішень.

Представлена стаття пропонує концепцію розвитку безпеки програмного забезпечення як окремої послуги, спрямованої на розроблення інструментарію та методик у сфері забезпечення безпекових вимог, проектування, розробки, аналізу вразливостей та тестування програмних продуктів.

На ринку хмарних технологій домінують відомі гіганти: Amazon EC2, IBM, HP, Google та Microsoft Azure. Водночас з'являються нові гравці, як-от 2nd Watch, що співпрацює з AWS та пропонує послуги хмарної міграції, керування навантаженням і обслуговує понад 75 000 клієнтських екземплярів. BetterCloud пропонує комплексне автоматизоване управління та захист інформації для хмарних офісних платформ, охоплюючи Google Apps і Microsoft Office 365.

Дослідники Хсу та Ченг (2015) презентували концепцію Semantic Agent as a Service (SAaaS), спроможну акумулювати та інтерпретувати семантичну інформацію через взаємодію з провідними хмарними сервісами: SaaS, PaaS та IaaS. Провайдери хмарних технологій одноголосно визнають критичну

необхідність розвитку захищених хмарних сервісів та забезпечення надійної міграції бізнес-процесів.

Розробка програмного забезпечення (SE) сформувала низку прийомів, методик та технологій протягом останніх двох десятиліть. SE також надає різноманітні інструменти та підходи до моделювання вимог щодо програмного забезпечення, проектування, розробки, тестування, управління конфігурацією та показниками. Водночас проблеми безпеки виступають безпосередніми атрибутами різноманітного програмного інструментарію, включаючи додатки, інтерфейси користувача, мережеві компоненти, системи розповсюдження, транзакційні процеси з інтенсивним використанням даних, комунікаційні інструменти тощо.

У сучасну епоху хмарних технологій спостерігається впровадження інноваційних методик у традиційних (фінанси, медицина, освіта, розробка програмного забезпечення, кібербезпека) та нових галузях (мобільні додатки, соціальні мережі, метеорологічна візуалізація, опрацювання великих даних). Попередні дослідження колективу включали розробку низки унікальних хмарних застосунків як сервісної послуги (Chang, Ramachandran, Wills, Walters, Kantere та Li, 2015).

Розвиток методологій безпечної розробки програмного забезпечення сприяв усвідомленню критичної важливості інтеграції захисних механізмів на всіх етапах життєвого циклу. Oueslati та співавтори (2016) розглядають проблематику створення захищених програмних продуктів з використанням адаптивних методологій. Водночас наявні методики аналізу вимог здебільшого концентруються на трансформації вимог, не приділяючи достатньої уваги безпековій компоненті еволюції проектних завдань.

Останніми роками спостерігається стрімке зростання впровадження моделі "Software as a Service" (SaaS). Найпоширенішим механізмом надання SaaS є API веб-сервісів провідних технологічних компаній (Google, Amazon, Yahoo, Facebook, Twitter). Подібні інтерфейси перетворюються на критично важливі

складники додатків, побудованих на монолітних багаторівневих або мікросервісних архітектурних рішеннях.

Користувачі застосовують API хмарних сервісів (передусім RESTful) через веб-браузери або в поєднанні з альтернативними системами для розширення функціональних можливостей мобільних додатків, екосистем Інтернету речей та цифрової робочої інфраструктури. Сучасні технологічні рішення значно оптимізують процеси розробки та надання послуг, забезпечуючи гнучкість, доступність та масштабованість SaaS-додатків. Водночас вражаючі переваги технологічної трансформації можуть супроводжуватися потенційними ризиками для інформаційної безпеки.

У контексті стрімкого розвитку SaaS-технологій постають серйозні виклики інформаційної безпеки. Для споживачів ключовим питанням є забезпечення повної конфіденційності та цілісності даних в середовищі, яке контролюється зовнішніми постачальниками. Провайдери, своєю чергою, змушені розробляти ефективні стратегії захисту своїх додатків від потенційних кібератак.

Головними загрозами інформаційній безпеці в SaaS-середовищі вважаються вразливості додатків, незахищені API та інтерфейси. Хмарні веб-сервіси створюють зовнішній периметр, який може бути легко атакований зловмисниками, надаючи додаткові можливості для несанкціонованого втручання. Найпоширенішими методами атак є маніпуляції з інформаційними потоками: SQL-ін'єкції, XML Path-ін'єкції, міжсайтові скриптинги та ін'єкції команд. Основною причиною таких вразливостей є неналежна перевірка та очищення вхідних даних. Успішна реалізація атаки може призвести не лише до компрометації даних окремого користувача, але й спричинити широкомасштабні порушення безпеки в системі. Дослідники останніх років зосередили свою увагу на розробці систем захисту та аналізу забруднень. Проте існуючі підходи мають значні обмеження. Системи на основі Taint концентруються переважно на статичній перевірці відкритих інформаційних потоків, ігноруючи приховані

канали передачі даних. Це суттєво знижує їхню ефективність у забезпеченні надійного захисту інформації.

Новіші методи орієнтовані на відстеження потоку даних під час виконання програми. Однак вони мають суттєві недоліки: виявлення порушень відбуваєтьсяpost-factum, вони вимагають модифікації базового середовища, спричиняють значне навантаження на продуктивність і можуть бути легко обійдені адаптивними атаками. Незважаючи на прогрес у статичному аналізі веб- та мобільних додатків, досі бракує комплексної моделі, здатної ефективно протидіяти складним викликам безпеки в SaaS-середовищі.

Альтернативні методології передбачають застосування різних підходів, зокрема механізмів виявлення вторгнень та тестування на проникнення для ідентифікації порушень інформаційної безпеки в хмарному середовищі. Інструменти виявлення вторгнень не спроможні забезпечити повномасштабну перевірку безпеки [29]. Тестування на проникнення розглядає досліджувану програму як закриту систему, внаслідок чого практично не гарантує захищеність програмного забезпечення від потенційних кібератак.

3.1 Рекомендації для вирішення проблем з аутентифікацією в сервісах

Технологія хмарних обчислень широко обговорюється серед професіоналів IT-галузі, бізнес-лідерів та незалежних експертів. Думки щодо цієї технології розходяться: одні вважають її революційним кроком в еволюції інтернет-технологій, інші сприймають як черговий маркетинговий трюк, щоґрунтується на вже існуючих обчислювальних рішеннях. З perspective користувача, хмарні обчислення – це спосіб отримання комп'ютерних послуг без глибокого занурення в технологічні деталі. Для організацій це означає спрощене надання сервісів, які масштабуються відповідно до потреб споживачів, підтримуючи швидкі інновації та прийняття рішень.

За визначенням Gartner, хмарні обчислення – це модель, де масштабовані IT-можливості надаються як послуга через інтернет-технології. Експерти

Секкомба та Національного інституту стандартів і технологій виділяють чотири моделі розгортання: приватну, спільну, публічну та гібридну, а також три моделі доставки послуг.
Основні моделі доставки включають:

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

Ці моделі характеризуються ключовими атрибутами: самообслуговуванням на вимогу, широким мережевим доступом, об'єднанням ресурсів, вимірюваним обслуговуванням та швидкою еластичністю. Особливу увагу привертає модель SaaS – найпоширеніша гілка хмарних обчислень.Ця модель передбачає розміщення додатків у центрах обробки даних провайдера з оплатою за передплатою та доступом через веб-браузер. Її суть полягає в наданні клієнтам ліцензій на використання програмного забезпечення як послуги на вимогу. Яскравим прикладом SaaS є CRM-система Salesforce.com, яка демонструє типову архітектуру та переваги такого підходу до надання програмних рішень.

У моделі Software as a Service (SaaS) клієнт цілковито покладається на постачальника послуг щодо забезпечення інформаційної безпеки. Критичним аспектом є гарантування ізоляції даних різних користувачів та забезпечення конфіденційності інформації. Для замовника стає принципово важливим переконатися в надійності системи захисту та її стабільному функціонуванні. Впровадження SaaS передбачає поступову заміну застарілих програмних рішень сучасними додатками. Основний фокус зміщується з технічної переносимості на збереження та вдосконалення безпекових механізмів, успішну міграцію корпоративних даних. Постачальники SaaS мають два варіанти розгортання додатків: на власних приватних серверах або з використанням хмарної інфраструктури провідних провайдерів, як-от Amazon чи Google. Модель "плата

за використання" дозволяє мінімізувати інфраструктурні витрати та сконцентруватися на наданні якісного сервісу.

Сучасні підприємства розглядають власні бізнес-дані як стратегічний актив, запроваджуючи жорсткі механізми контролю доступу та дотримання корпоративних політик. Водночас у SaaS-моделі інформація зберігається в центрах обробки даних провайдера поруч з даними інших організацій, що створює додаткові ризики. За умови використання публічних хмарних сервісів, корпоративні дані можуть співіснувати з інформацією інших, не пов'язаних між собою додатків. Більше того, хмарні провайдери часто реплікують дані в різних географічних локаціях для забезпечення відмовостійкості та доступності.

На відміну від класичної моделі локальних систем, де інформація перебуває під повним контролем організації, SaaS висуває принципово нові виклики інформаційної безпеки. Постачальникам необхідно вирішувати традиційні проблеми кібербезпеки, властиві класичним комунікаційним системам, та водночас опановувати специфічні загрози, притаманні хмарним технологіям. Для зручності аналізу всі проблеми безпеки SaaS можна розділити на дві категорії: традиційні виклики інформаційної безпеки та нові ризики, безпосередньо пов'язані з парадигмою хмарних обчислень. На рисунку 9 показано різні проблеми безпеки в моделі SaaS, які обговоюрються в статті [30].

Попри те, що питання інформаційної безпеки притаманні й класичним комунікаційним системам, cloud-технології створюють додаткові канали для потенційних кіберзагроз, які раніше були або складнішими, або неможливими для реалізації. Нижче розглянуто деякі традиційні виклики безпеці, характерні також для моделі SaaS.

· Автентифікація та авторизація. Може виникнути необхідність модифікації наявних механізмів автентифікації та авторизації корпоративних систем для забезпечення сумісності з безпечним cloud-середовищем. Forensic-дослідження ускладнюються через відсутність безпосереднього фізичного доступу до апаратних компонентів. Концепція, запропонована дослідником Прата Мурукутлою, дає змогу використовувати уніфіковану систему

ідентифікації. Автор пропонує рішення на базі стандартів Open Authorization, де функціонує незалежний аудитор довіреної сторони, який акумулює облікові записи, а cloud-провайдер отримує можливість диференціювати користувачів. Модель реалізує багатофакторну автентифікацію через поєднання класичного паролю, смарт-карток та позасмугових методів (тобто створює потужний двофакторний захист). Додатково схема забезпечує взаємну ідентифікацію, керування обліковими записами, генерацію унікальних сесійних ключів, гарантує конфіденційність та протидіє багатьом популярним атакам, хоча формальна верифікація безпеки залишається не до кінця опрацьованою (рисунок 9).

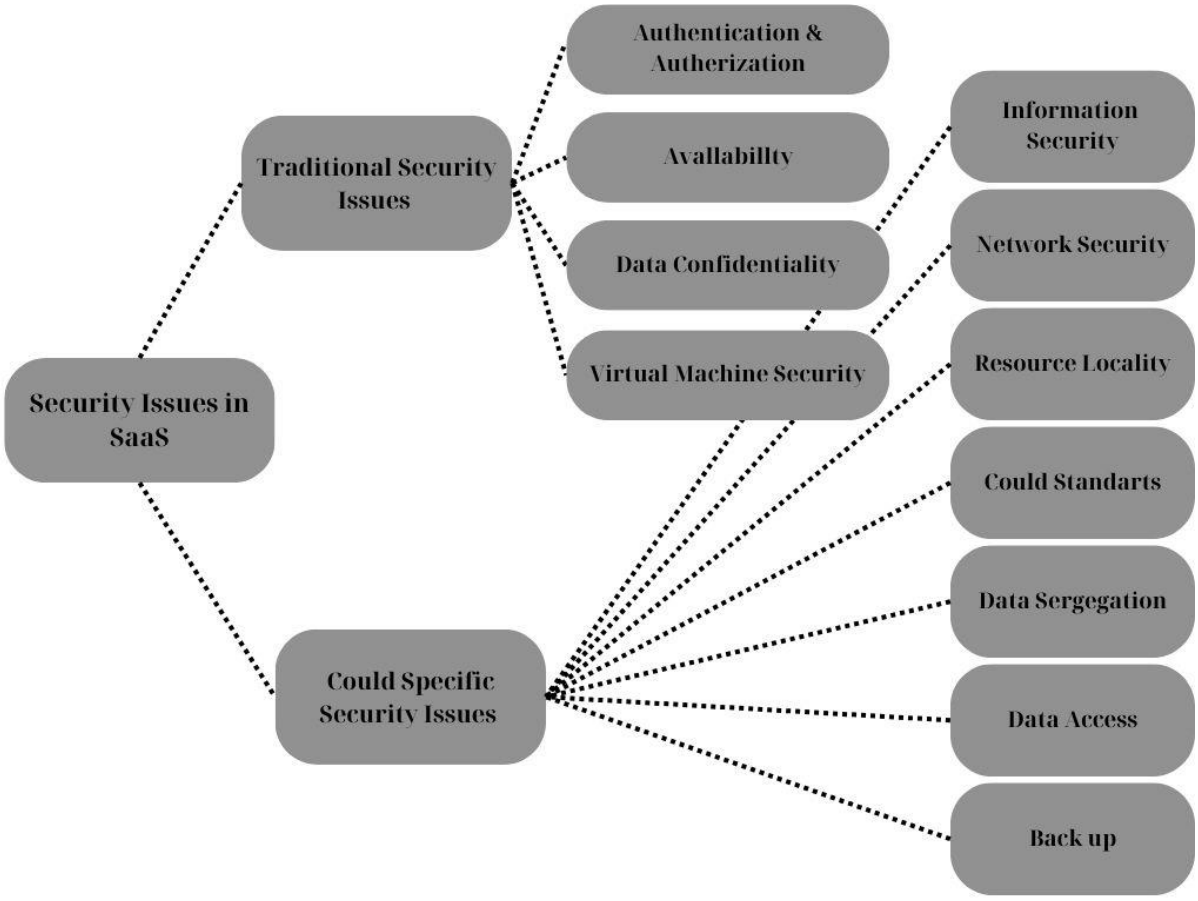

Рисунок 9 - Проблеми безпеки в SaaS - сервісах

Доступність у хмарних обчисленнях передбачає забезпечення надійного та своєчасного доступу до даних та ресурсів для авторизованого персоналу.

Особливе занепокоєння викликає стабільність роботи провайдерів хмарних послуг, оскільки будь-який збій може мати масштабніші наслідки порівняно з традиційними IT-моделями.

Промовистим прикладом такої вразливості став інцидент з Amazon у 2011 році, коли технічні проблеми призвели до припинення роботи низки популярних веб-сервісів, включаючи Reddit, Foursquare та Quora. Постачальники SaaS-додатків змушені гарантувати максимально безперервну роботу систем та цілодобову підтримку клієнтів. Досягнення високої доступності вимагає фундаментальних архітектурних змін як на рівні додатків, так і інфраструктури.

Необхідно закласти механізми стійкості до технічних збоїв та потенційних атак на працездатність системи ще на етапі розроблення.

Критично важливим є формування комплексного плану забезпечення безперервності бізнесу та аварійного відновлення. Це дозволяє мінімізувати ризики втрати корпоративних даних та скоротити час простою в критичних ситуаціях. Провідні хмарні провайдери впроваджують передові методи захисту. Приміром, Amazon Web Services використовує інфраструктуру світового рівня, ідентичну тій, що підтримує роздрібну онлайн-торгівлю компанії. Серед застосованих технік – використання синхронних файлів cookie, обмеження підключень та створення внутрішніх потужностей, які перевищують пропускну здатність інтернет-каналів.

Стандартні методи протидії розподіленим атакам (DDoS) включають:

- Синхронізацію файлів cookie
- Контроль мережевих підключень
- Резервування комунікаційної інфраструктури

Метою таких рішень є забезпечення максимальної стійкості хмарних сервісів та захист від потенційних збоїв і кіберзагроз. Постійне вдосконалення архітектури та механізмів безпеки стає визначальним фактором конкурентоспроможності провайдерів хмарних послуг.

Захист інформації передбачає унеможливлення навмисного або ненавмисного неавторизованого розкриття даних. Приватність у cloud-

середовищі пов'язана з правовими аспектами інтелектуальної власності, латентними каналами комунікації, трафік-аналізом, криптографічними методами та аналітичними висновками. Cloud-технології передбачають обмін або зберігання інформаційних масивів на віддалених серверах, що належать або контролюються третіми сторонами, з доступом через інтернет-мережу чи інші комунікаційні канали. Сервіси cloud-обчислень представлені широким спектром додатків, включаючи платформи для зберігання даних, відеохостинги, сервіси податкової звітності, електронні медичні картки та інші інформаційні ресурси. Увесь контент пристроїв користувача може зберігатися як в одного постачальника cloud-послуг, так і розподілятися між кількома провайдерами. Щоразу, коли фізична особа, комерційна організація, державна установа чи будь-який інший суб'єкт передає інформацію в cloud-простір, актуалізуються питання забезпечення конфіденційності та приватності. Незважаючи на відносно нещодавнє глобальне впровадження віртуалізації, пов'язані з нею кіберзагрози еволюціонують надзвичайно динамічно. Гіпервізори та віртуальні машини, що використовуються хмарними провайдерами, мають власні вразливості, особливо критичні в мультиклієнтських середовищах, де компрометація однієї віртуальної машини може створити ризики для всіх користувачів фізичного сервера. Віртуалізація є ключовим компонентом хмарних технологій, проте водночас генерує значні ризики інформаційної безпеки. Основне завдання – забезпечення повної ізоляції різних екземплярів на одному фізичному обладнанні, яке наразі реалізується не повною мірою. Суттєвою проблемою залишається контроль адміністратора вhost-guest операційних системах.

Монітори віртуальних машин (VMM) не гарантують абсолютної ізоляції. У провідних VMM виявлено численні вразливості, що дозволяють здійснювати несанкціонований доступ. Практично в усьому програмному забезпеченні віртуалізації існують вразливості, які можуть бути використані локальними користувачами для обходу захисних механізмів. Прикладом такої вразливості є проблеми в Microsoft Virtual PC та Virtual Server, які потенційно дозволяють виконувати код на хості або інших гостьових системах з підвищенням привілеїв.

Це змушує постачальників хмарних послуг переосмислювати традиційні підходи до забезпечення кібербезпеки.

У сфері хмарної безпеки активно працюють декілька впливових організацій:

- Cloud Security Alliance (CSA) об'єднує постачальників рішень для обговорення кращих практик захисту
- Cloud Standards координує розроблення галузевих стандартів
- Open Web Application Security Project підтримує актуальний перелік уразливостей SaaS-моделей
- Open Grid Forum публікує специфікації безпеки для дослідників

Експерти пропонують різні стратегії підвищення безпеки: від розроблення жорсткої архітектурної моделі до ізоляції обчислювальних ресурсів. Зокрема, пропонуються методи ізоляції кешу процесора у віртуальних машинах та захисту від втручання гіпервізора.

Для британських компаній одним з найпростіших рішень вважається використання власних приватних хмар. Водночас експерти наголошують на браку прозорості, що перешкоджає повноцінному використанню потенціалу хмарних технологій [31].

З метою забезпечення ефективного управління ідентифікацією та контролю доступу в SaaS-системах розроблено спеціалізовану методичну документацію, яка містить перелік рекомендованих інноваційних практик для реалізації надійної ідентифікації та безпечного адміністрування доступу (таблиця 5). Територіальне розташування ресурсів та ізоляція інформаційних масивів становлять два критичні аспекти кібербезпеки, висвітленню яких в існуючих наукових джерелах приділено недостатньо уваги, що обумовлює необхідність проведення подальших поглиблених досліджень у цій сфері.

Таблиця 5 - Доступні поточні рішення для захисту SaaS

№	Зони безпеки	Поточні/можливі рішення

1	Автентифікація та авторизація	• Відкрити авторизацію • Двофакторна автентифікація • OAuth
2	Доступність	• Розпорошення даних
3	Конфіденційність даних	•Повторне шифрування проксі на основі атрибутів
4	Безпека віртуальної машини	•Реконфігурована розподілена віртуальна машина •Опитування щодо безпеки віртуальної машини
5	Інформаційна безпека	•Структура управління ризиками інформаційної безпеки
6	Безпека мережі	• Безпека мережі для віртуальних машин • Пісочниця безпеки мережі
7	Хмарні стандарти	• IEEE Cloud Computing Standard Study Group • Фокус-група ITU Cloud Computing • Cloud Security Alliance (CSA)
8	Доступ до даних	• Політики багатокористувацького доступу • Керування доступом до даних
9	Безпека веб-додатків	• Сканери веб-додатків
10	Порушення даних	• Шифрування даних • Двофакторна аутентифікація • Регулярне оновлення та патчі • Моніторинг та аналіз журналів
11	Резервне копіювання	•Безагентний метод резервного копіювання та відновлення даних
12	Керування ідентифікацією та процес входу	•Інструкції CSA щодо керування ідентифікацією та доступом

3.2 Заходи щодо покращення безпеки аутентифікації користувачів

Модель Software as a Service (SaaS) презентує низку значущих переваг, передусім у контексті оптимізації фінансових витрат, однак її впровадження вимагає надзвичайно виваженого та детального підходу для запобігання потенційним ризикам інформаційної безпеки. Представлений аналіз фокусується на дослідженні безпекових аспектів різних архітектурних рішень у сфері SaaS – від класичних багатокористувацьких моделей до складних сервісів з елементами аутсорсингу та віртуалізації. Розглядаючи еволюцію SaaS-архітектур, ми маємо на меті комплексно оцінити наявні підходи до забезпечення кібербезпеки, виокремити найбільш вразливі компоненти та запропонувати стратегії мінімізації ризиків при впровадженні хмарних сервісів. Ключовим завданням є не лише демонстрація потенційних переваг SaaS-технологій, але й критичний аналіз можливих загроз та механізмів їх нейтралізації в різних контекстах використання.

Спершу ми здійснюємо детальний аналіз характерних загроз у SaaS-середовищі [32], далі розглядаємо комплекс провідних стратегій для нівелювання виявлених ризиків та, зрештою, презентуємо концептуальну модель формалізації безпекових вимог, релевантних контексту SaaS-платформ. Наше дослідження орієнтоване на підтримку споживачів SaaS-послуг у глибинному розумінні складних аспектів інформаційної безпеки та розробці дієвих механізмів мінімізації потенційних кіберзагроз.

Ключова перевага Software as a Service полягає в передачі постачальникові послуг усіх завдань з управління апаратними засобами, програмними ліцензіями та конфігураційними налаштуваннями. Економічна модель передбачає розподіл витрат між різними клієнтами для забезпечення рентабельності. Впровадження SaaS суттєво трансформує традиційні підходи до кібербезпеки, генеруючи низку специфічних викликів. Для малих організацій це унікальна можливість отримати потужні рішення інформаційної безпеки, які були б недоступні через високу

вартість. Водночас клієнти змушені частково втрачати безпосередній контроль над власними інформаційними системами.

Спільне використання ресурсів різними орендарями створює додаткові ризики. Тому постачальник SaaS зобов'язаний запропонувати переконливі механізми захисту, які забезпечують:

- Надійний захист служб від зовнішніх загроз
- Ефективну ізоляцію клієнтських екземплярів
- Можливість перевірки дотримання договірних умов

У дослідженні ми послідовно:

- Проаналізуємо потенційні загрози безпеці в SaaS-середовищі
- Запропонуємо адекватні механізми контролю
- Розробимо методологію оцінки інформаційної безпеки
- Визначимо межі відповідальності замовника та постачальника в разі потенційних інцидентів

Наша мета – створити комплексний підхід до убезпечення хмарних сервісів, який дозволить клієнтам мінімізувати ризики та максимізувати ефективність використання SaaS-технологій.

SaaS передбачає взаємодію декількох учасників, а саме споживачів та постачальників: перші використовують прикладні сервіси, що надаються останніми [33]. Типовий клієнт SaaS застосовує багаторівневу / багатокомпонентну модель інформаційної безпеки для дистанційного підключення до сервісу. Приміром, в організації різні співробітники отримують диференційований доступ до програмного забезпечення з відмінними рівнями привілеїв. Конкретний SaaS-сервіс може бути призначений для поодинокого замовника, однак здебільшого розробляється з мультиклієнтською архітектурою, де один сервіс обслуговує водночас кількох споживачів. Попри зовнішню монолітність, SaaS-додаток може мати складну багатокомпонентну архітектуру з різними постачальниками. Провайдер має альтернативні стратегії розміщення: від повного самостійного обслуговування власними потужностями до часткового використання ресурсів сторонніх центрів обробки даних.

Наприклад, постачальник може орендувати апаратні ресурси – обчислювальні потужності або системи зберігання даних – у зовнішніх операторів. Це ускладнює традиційні моделі забезпечення інформаційної безпеки та вимагає комплексного підходу до аналізу потенційних ризиків.

Під час вивчення безпеки SaaS-сервісів необхідно враховувати чотири магістральні вектори потенційних загроз:

1. Взаємодія між клієнтом та постачальником
2. Міжклієнтські інтеракції в середовищі одного провайдера
3. Комунікації між SaaS-постачальником та субпровайдерами
4. Зовнішні кіберзагрози, спрямовані на будь-які компоненти служби

Усі ідентифіковані загрози можна систематизувати за двома принциповими категоріями:

- Ризики, генеровані безпосередньо провайдером
- Загрози, породжені архітектурними особливостями SaaS-моделі

Такий структурований підхід дозволяє всебічно оцінити потенційні вразливості та розробити ефективні механізми захисту інформаційних активів.

Важливо підкреслити, що ми не розглядаємо універсальні кіберзагрози, котрі можуть вплинути на будь-яке програмне забезпечення незалежно від його SaaS-специфіки (як-от випадки, коли зловмисник використовує вразливість системи для неправомірного підвищення власних привілеїв), натомість зосереджуємося на ситуаціях, де безпосередньо SaaS-парадигма впливає на ймовірність реалізації або масштаб потенційних ризиків. У світі хмарних сервісів існують різноманітні ризики, які можуть виникати через дії постачальника SaaS, викликані як навмисними, так і ненавмисними факторами. Загрози безпеці даних клієнта являють собою серйозну проблему. Оскільки інформація додатку зберігається та контролюється постачальником, він має потенційну можливість здійснювати несанкціоновані маніпуляції. Це може включати неправомірний доступ до даних, їх неавторизовану зміну, фальсифікацію або повне видалення. Подібно до інших форм зовнішнього сервісу, SaaS вимагаєретельного вибору

надійного постачальника та розробки комплексної стратегії захисту інформації для мінімізації потенційних ризиків.

Проблема недостовірних обчислень також становить значну загрозу. Постачальник може навмисно або ненавмисно модифікувати алгоритми та надавати клієнтові викривлені послуги. Більше того, він спроможний виконувати несанкціоновані дії під виглядом клієнта. Розглянемо приклад з маркетинговою аналітикою: зловмисний постачальник може вступити в змову з конкурентом і маніпулювати результатами, надаючи неповну або спотворену інформацію на користь третьої сторони.

Подібний сценарій може включати службу, яка виконує розробки, корисні для аналізу прототипу (таблиця 6).

Таблиця 6 - Заходи щодо покращення безпеки аутентифікації користувачів

Захід	Опис	Вигоди
Впровадження двофакторної аутентифікації	Вимагання введення додаткового елемента, окрім пароля (наприклад, SMS-код або аплікація для генерації одноразових кодів).	Збільшення рівня безпеки. - Захист від атак брутфорсу та витоків паролів.
Використання біометричних методів	Впровадження систем розпізнавання обличчя, відбитків пальців, голосу тощо.	Зручність для користувачів. Унікальність біометричних даних. Важкість підробки.
Застосування аналізу ризиків	Використання алгоритмів для визначення рівня ризику на основі поведінкових	Динамічне адаптування безпеки до змінних умов. Виявлення незвичайних активностей.

	та контекстуальних факторів.	
Мультифакторна аутентифікація (MFA)	Використання комбінації різних факторів, таких як пароль, код з SMS і біометричні дані.	Захист від викрадення одного фактора. Зменшення ризику компрометації облікового запису.
Використання блокування після помилок	Тимчасове блокування облікового запису після визначеної кількості невдалих спроб входу.	Ускладнення атак брутфорсу. Зменшення ризику вгадування пароля.
Регулярна зміна паролів	Вимагання від користувачів періодично змінювати свої паролі.	Зменшення часу, протягом якого можуть використовуватися викрадені паролі. Підвищення рівня безпеки.
Аудит безпеки та моніторинг	Постійний моніторинг діяльності та аудит безпеки для виявлення ненормальних або підозрілих активностей.	Реагування на потенційні загрози в реальному часі. Можливість проведення вчасних заходів безпеки.
Забезпечення надійних каналів зв'язку	Використання зашифрованих протоколів та безпеки на рівні транспортного шару для захисту обміну інформацією.	Запобігання перехопленню чутливої інформації. Захист від атак "человік посередині".

У сучасному цифровому середовищі інформаційні системи дедалі більше покладаються на бази даних як основний механізм збереження критично важливої інформації. Визначальним аспектом структурованих масивів даних є зберігання облікових записів, які слугують для ідентифікації користувачів та забезпечення диференційованого доступу до персональних даних. Системи автентифікації часто стають мішенню для кіберзлочинців, оскільки можуть слугувати вхідною точкою для подальших протиправних дій.

Незважаючи на наявність галузевих рекомендацій від авторитетних організацій, таких як OWASP, PCI-SSC, IETF та IEEE, практична реалізація заходів безпеки залишається далекою від досконалості. Непослідовність та недоліки впровадження created середовище підвищеної вразливості баз даних автентифікації. Показовим прикладом став масштабний витік даних компанії Yahoo у 2016 році, коли зловмисники отримали доступ до облікових записів приблизно мільярда користувачів через застарілі механізми захисту паролів.

Застарілі підходи до зберігання автентифікаційних даних становлять серйозну загрозу інформаційній безпеці, роблячи їх легкою здобиччю для потенційних зловмисників. Існує сучасний метод підвищення захисту, який передбачає використання криптографічних технік: додавання унікальної солі, застосування одностороннього хешування та багаторівневого шифрування як для існуючих, так і для нових паролів. Такий підхід може бути реалізований на серверному рівні з мінімальними змінами в інфраструктурі та без втручання користувачів, що створює потенціал для суттєвого посилення системної безпеки та захисту персональних даних.

ВИСНОВКИ

Технологія хмарних обчислень перебуває в стані безперервної динамічної еволюції. Разом з розширенням функціональних можливостей та зручності використання, вона стає більш вразливою до диверсифікованих атак на інформаційну безпеку. З дозріванням технології цілком очікувано, що деякі специфічні вразливості будуть з'являтися, водночас попередні поступово втрачатимуть свою критичність. Ці уразливості становлять суттєву перешкоду як для провайдерів хмарних послуг, так і для їхніх споживачів у процесі надання та використання сервісів. Відповідні інституції усвідомлюють важливість мінімізації ризиків, що допоможе здійснювати більш виважені інвестиційні стратегії.

Для попередження потенційних загроз експерти пропонують низку рекомендацій:

- Систематичне проведення аудитів безпеки з метою виявлення можливих вразливостей
- Впровадження багатофакторної автентифікації для підвищення рівня захисту
- Формування суворої політики паролів з акцентом на складність та унікальність
- Підготовка користувачів шляхом навчання безпековим практикам
- Застосування динамічних систем моніторингу та ідентифікації аномалій

Наведені рекомендації підкреслюють критичну важливість приділяти максимальну увагу питанням безпеки автентифікації в SaaS-середовищі та вживати випереджувальних заходів для редукції ризиків.

Аналіз механізмів автентифікації в SaaS-сервісах демонструє, що убезпечення облікових записів є не лише технічним викликом, але й фундаментальним компонентом довіри в цифровому просторі. При дослідженні

різноманітних методів – від традиційних до інноваційних біометричних рішень – необхідно враховувати їхні переваги та потенційні вразливості.

Класична парольна автентифікація залишається вразливою до зовнішніх атак. Багатофакторні методи забезпечують вищий рівень захисту, проте важливо зважати на етичні та фізичні аспекти біометричних технологій.

Тенденції аналізу ризиків та інноваційні підходи стають ключовими драйверами вдосконалення систем безпеки. Водночас ускладнення механізмів захисту супроводжується зростанням потенційних загроз фішингових та брутфорс-атак.

Статистичні дослідження демонструють, що вибір оптимального механізму автентифікації має базуватися на збалансованому підході між рівнем захищеності та зручністю використання. Кожен метод має власні переваги та обмеження, тому crucial розуміти контекст застосування.

Забезпечення безпеки облікових записів – це комплексне завдання, яке виходить за межі суто технічних аспектів. Від розробників до кінцевих користувачів усі учасники мають бути залучені в процес підвищення обізнаності, впровадження сучасних технологій та перманентного вдосконалення стратегій автентифікації.

Розробка програмного забезпечення безпеки передбачає впровадження найкращих практик для створення стійких та стабільних систем. Принципово важливо, щоб безпека була вбудованою на всіх етапах розроблення, а не додавалася post-factum.

Незважаючи на революційний потенціал хмарних обчислень, існує низка невирішених питань у сфері сервісних угод, безпеки, конфіденційності та енергоефективності. Поки не буде сформовано комплексний модуль безпеки, який враховуватиме всі можливі ризики, технологія не зможе повною мірою реалізувати свій потенціал.

Підсумовуючи, забезпечення надійного захисту в хмарному середовищі потребує системного підходу, постійної уваги та готовності до адаптації в умовах динамічних технологічних змін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. Goel, M. Garuba and A. Girma, "Cloud Computing Vulnerability: DDoS as Its Main Security Threat, and Analysis of IDS as a Solution Model," 2014 11th International Conference on Information Technology: New Generations, Las Vegas, NV, 2014, pp. 307-312.

2. B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011.

A. M. Al Zadjali, A. H. Al-Badi and S. Ali, "An Analysis of the Security Threats and Vulnerabilities of Cloud Computing in Oman," 2015 International Conference on Intelligent Networking and Collaborative Systems, Taipei, 2015, pp. 423-428.

A. Gkortzis, S. Rizou and D. Spinellis, "An Empirical Analysis of Vulnerabilities in Virtualization Technologies," 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg City, 2016, pp. 533-538.

3. Madria, Sanjay K. "Security And Risk Assessment In The Cloud". Computer 49.9 (2016): 110-113. Web.

4. M. Derfouf, A. Mimouni and M. Eleuldj, "Vulnerabilities and storage security in cloud computing," 2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech, 2015, pp. 1-5.

A. Girma, M. Garuba and J. Li, "Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics," 2015 12th International Conference on Information Technology – New Generations, Las Vegas, NV, 2015, pp. 206-211.

5. L. Krishnakumar and N. M. Varughese, "High speed classification of vulnerabilities in cloud computing using collaborative network security management," 2013 International Conference on Advanced Computing and Communication Systems, Coimbatore, 2013, pp. 1-6.

6. Sameena Naaz, Firdoos Ahmad Badroo, “Investigating DHCP and DNS Protocols using Wireshark”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p- ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 01-08

7. Sameena Naaz, Faizan Ahmad Siddiqui, “Comparative Study of Cloud Forensics Tools”, Communications on Applied Electronics (CAE) ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 5 – No.3, June 2016, page 24-30.

8. F. Zhou, M. Goel, P. Desnoyers and R.Sundaram, "Scheduler Vulnerabilities and Coordinated Attacks in Cloud Computing," 2011 IEEE 10th International Symposium on Network Computing and Applications, Cambridge, MA, 2011, pp. 123-130.

9. Rohlmann S, Mladenov V, Mainka C, Hirschberger D and Schwenk J. Every signature is broken. Proceedings of the 32nd USENIX Conference on Security Symposium. (7411-7428). URL: /doi/10.5555/3620237.3620652

10. Engelbertz N, Erinola N, Herring D, Somorovsky J, Mladenov V and Schwenk J. Security analysis of eIDAS - the cross-country authentication scheme in europe. Proceedings of the 12th USENIX Conference on Offensive Technologies. (15-15). URL: /doi/10.5555/3307423.3307438

11. The MITRE Corporation. “MITRE ATT&CK®”, The MITRE Corporation. 2023. [Електронний ресурс]. Режим доступу: https://attack.MITRE.org/.

12. The MITRE Corporation. “MITRE ATT&CK®”, The MITRE Corporation for SaaS platform. 2023. [Електронний ресурс]. Режим доступу: https://attack.MITRE.org/matrices/enterprise/cloud/saas/.

B. Strom and A. Robertson, "The MITRE Corporation," 3 March 2020. [Електронний ресурс]. Режим доступу: https://medium.com/MITRE-attack/2020-attack-roadmap-4820d30b38ba.

13. Megouache L, Zitouni A, Djoudi M (2018) A new framework of authentication over cloud computing. In: Silhavy R, Silhavy P, Prokopova Z (eds)

Cybernetics approaches in intelligent systems. CoMeSySo 2017. Advances in intelligent systems and computing, vol 661. Springer, Cham, pp 262–270

14. Thandeeswaran R, Subhashini S, Jeyanthi N, Saleem Durai MA (2012) Secured multi-cloud virtual infrastructure with improved performance. J Cybern Inf Technol 12(2):11–22

15. Venkat RK, Avala AR (2013) Data integrity in multi-cloud storage international. J Sci Eng Adv Technol 1(7):219–223

16. Long M, Peng F, Li HY (2018) Separable reversible data hiding and encryption for HEVC video. J Real-Time Image Process 14(1):171–182

17. Chow, E. (2021, June 27). *Lockheed Martin Cyber Kill Chain vs. MITRE ATTACK Framework.* Retrieved January 29, 2022, from eric-chow.medium.com: https://eric-chow.medium.com/lockheed-martin-cyber-kill-chain-vs-mitre-attack-framework-64f8f3bf1e58

18. CISA. (2021, June). *us-cert.cisa.gov.* Retrieved October 17, 2021, from Best Practices for MITRE ATT&CK® Mapping: https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisa-releases-best-practices-mapping-mitre-attckr

19. Cybersecurity Insiders. (2021). *Industry Report: The State of MITRE ATT&CK® Threat-Informed Defense in 2021.* Retrieved January 29, 2022, from mitre-engenuity.org: https://mitre-engenuity.org/mad/state_of_attack_report_2021/

20. Kwon, R. A. (2020). Cyber Threat Dictionary Using MITRE ATT&CK Matix and NIST Cybersecurity Framework Mapping. Pacific Northwest National Laboratory. doi:10.1109/RWS50334.2020.9241271

21. MITRE ATT&CK : Design and Philosophy. https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf

22. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. NIST Special Publication 800-30 (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

23. Stallings, W.: Cryptography and Network Security, 4th edn. Prentice Hall, Englewood Cliffs (2005)

24. Miller, E.L., Freeman, W.E., Long, D.D.E., Reed, B.C.: Strong security for network-attached storage. In: USENIX Conference on File and Storage Technologies (FAST), pp. 1–14 (January 2002)

25. Ferrie, P.: Attacks on more virtual machine emulators. Symantec Advanced Threat Research (2008)

26. Бондар Є. С. Хмарні обчислення та їх застосування / Є. С. Бондар, М. М. Глибовець, С. С. Гороховський // Вісник КНУ ім. Т. Шевченка. – Вип. № 1. – К.: КНУ, 2011. – С. 74–82.

27. Гриджук Г. С. Систематизація методів інформаційної безпеки підприємства / Г. С. Гриджук. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

28. Pratap Murukutla, K.C. Shet (2012).Single Sign On for Cloud .In: International Conference on Computing Sciences,2012 IEEE DOI 10.1109/ICCS.2012.66

29. Amazon Web Services: Overview of Security Processes http://aws.amazon.com/security Accessed:[January 2013]

30. Berre AJ, Roman D, Landre E, Heuvel WVD, Skar LA, Udnaes M, et al. Towards best practices in designing for the cloud. In: Proceedings of the 24th ACM

31. Колінець Р.Б.. Аналіз поширених вразливостей у веб застосунках. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції "Актуальні проблеми комп’ютерних наук АПКН-2024", Хмельницький, 2024. С. 282 - 288.

ДОДАТОК А Копія публікації результатів дослідження

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2024»

15-16 листопада 2024

Хмельницький 2024

УДК 004.056.5

Колінець Р.Б.

Західноукраїнський національний університет

АНАЛІЗ ПОШИРЕНИХ ВРАЗЛИВОСТЕЙ У ВЕБ-ЗАСТОСУНКАХ

У даній статті ми розглянемо деякі з найпоширеніших вразливостей у веб-застосунках, а також запропонуємо рекомендації щодо їх попередження та захисту. Це допоможе розробникам та адміністраторам веб-застосунків забезпечити надійний рівень безпеки та захисту для своїх користувачів. Одним із способів запобігти веб-загрозам є аналіз поширених вразливостей у веб-застосунках. Цей процес дозволяє ідентифікувати потенційні проблеми безпеки та розробити стратегії їх усунення.

In this article, we will examine some of the most common vulnerabilities in web applications and provide recommendations for their prevention and protection. This will help web application developers and administrators ensure a reliable level of security and protection for their users. One way to prevent web threats is to analyze common vulnerabilities in web applications. This process allows identifying potential security issues and developing strategies to address them.

Веб-застосунки займають все більш важливе місце в нашому цифровому світі, надаючи різноманітні сервіси та сприяючи комунікації. Однак, разом зі зростанням їх популярності, збільшується ймовірність виявлення вразливостей, які можуть бути вживані зловмисниками. Тому важливо проводити аналіз та виявляти такі уразливості, щоб забезпечити надійність та безпеку веб-застосунків.

Одна з найпоширеніших вразливостей, яка часто зустрічається в веб-застосунках, – це SQL-ін'єкція. Ця вразливість дозволяє зловмиснику виконати шкідливий SQL-код через веб-форми або параметри URL-адреси, що може призвести до незаконного доступу до бази даних та втрати конфіденційної інформації. Щоб запобігти SQL-ін'єкції, розробники повинні використовувати параметризовані запити та перевіряти вхідні дані перед їх використанням в SQL-запитах.

Ще одна поширена вразливість – це міжсайтовий скриптинг (XSS). Зловмисники вставляють шкідливий код у веб-сторінки, який потім виконується в браузері користувача. Це може призвести до крадіжки сесійних файлів, перенаправлення на шахрайські сайти або виконання шкідливих дій в контексті аутентифікованого користувача. Для запобігання XSS-атакам рекомендується екранувати та валідувати всі вхідні дані, а також використовувати заголовки безпеки, такі як Content Security Policy (CSP).

Крім того, важливо захистити веб-застосунки від аутентифікаційних та авторизаційних атак. Недостатній контроль доступу може дозволити зловмиснику зламати облікові записи користувачів або отримати привілеї адміністратора. Для попередження таких атак необхідно застосовувати сильні паролі, використовувати двофакторну аутентифікацію та перевіряти права доступу на всіх рівнях системи.

Також слід звернути увагу на вразливості, пов'язані з некоректною обробкою файлів, перенаправленням та збереженням даних. Зловмисники можуть використовувати такі уразливості для завантаження шкідливих файлів на сервер, здійснення фішинг-атак або отримання неприпустимого доступу до конфіденційних даних. Правильна перевірка та обробка вхідних файлів, належне збереження та перенаправлення даних допоможуть запобігти таким вразливостям. [1]

Загалом, проведення аналізу поширених вразливостей у веб-застосунках є критичним етапом у процесі розробки та утримання безпечних програмних продуктів (Таблиця 1). Застосування належних методів тестування на вразливості, таких як динамічний аналіз коду та пенетраційне тестування, дозволить виявити та виправити уразливості до їх використання зловмисниками.

Таблиця 1 – Аналіз поширених вразливостей у веб застосунках

Вразливість	**Наслідки**
SQL-ін'єкція	Незаконне отримання даних, порушення БД
Cross-Site Scripting (XSS)	Крадіжка сесій, зловживання користувачів
Cross-Site Request Forgery (CSRF)	Порушення конфіденційності, втрата даних
Недостатні перевірки доступу	Незаконне отримання даних, порушення БД
Незахищені сесії	Підроблення ідентифікації, зловживання
Вразливості файлового завантаження	Входження шкідливого коду, компрометація

Захист веб-застосунків від вразливостей є невід'ємною складовою розробки та експлуатації безпечних програмних продуктів. Окрім аналізу і виявлення уразливостей, необхідно приймати активні заходи для їх попередження та мінімізації ризиків. Нижче розглянемо деякі важливі кроки та рекомендації з метою запобігання поширеним вразливостям у веб-застосунках.

1. Навчання розробників: Ключовим елементом є належне навчання розробників про безпеку веб-застосунків. Розробники повинні мати глибокі знання про вразливості, методи їх використання та ефективні способи запобігання. Включення безпеки як основної складової процесу розробки допоможе створити свідомість про безпеку серед всіх учасників проекту.

2. Використання безпечних бібліотек та фреймворків: Використання вже перевірених та безпечних бібліотек та фреймворків може допомогти уникнути багатьох вразливостей. Ці рішення вже мають вбудовані механізми безпеки, такі як захист від SQL-ін'єкцій, XSS та інших атак. При розробці власних компонентів важливо дотримуватись найкращих практик безпеки.

3. Регулярні оновлення та патчі: Важливо відстежувати оновлення та патчі для всіх використовуваних компонентів, включаючи бібліотеки, фреймворки та серверне програмне забезпечення. Вразливості часто виявляються після випуску продукту, тому розробники повинні бути готові вносити виправлення та оновлення з метою підтримки безпеки веб-застосунків.

4. Тестування на вразливості: Проведення регулярних тестів на вразливості є невід'ємною складовою процесу розробки. Використання автоматичних сканерів вразливостей, пенетраційного тестування та аудиту коду допомагає виявити потенційні проблеми та уразливості до їх використання зловмисниками.

5. Захист сесій та куки: Для забезпечення безпеки аутентифікації та авторизації веб-застосунків необхідно правильно налаштувати та захищати сесії користувачів. Використання безпечних механізмів сесій, таких як зміна ідентифікаторів сесій, використання SSL / TLS та обмеження часу сесій, допоможе запобігти атакам типу сесійного викрадення.

Ці кроки і рекомендації є лише початком для забезпечення безпеки веб-застосунків. Важливо постійно оновлювати свої знання про нові види атак та вразливості, а також впроваджувати найкращі практики безпеки в усіх етапах життєвого циклу розробки веб-застосунків.

Аналіз поширених вразливостей у веб-застосунках виявив, що безпека цих систем є критичним аспектом. Розробники та адміністратори повинні усвідомлювати потенційні загрози та вживати відповідних заходів для їх попередження та захисту. Використання надійних бібліотек та фреймворків, навчання розробників про безпеку, регулярне оновлення та тестування на вразливості - це лише деякі з рекомендацій, які можуть допомогти уникнути серйозних наслідків. Забезпечення безпеки веб-застосунків має бути постійним процесом, що вимагає уваги та відповідального підходу. Лише тоді можна забезпечити захищеність і довіру користувачів до цих важливих інтернет-ресурсів. [2]

Існуючі методи виявлення вразливостей у сервісах SaaS мають низку переваг і недоліків. Переваги включають такі можливості, як постійний моніторинг, аналіз загроз у реальному часі та автоматизоване керування виправленнями. З іншого боку, ці методи можуть становити проблеми, такі як потенційна ресурсомісткість, складність впровадження та потреба в постійних оновленнях, щоб залишатися ефективними.

Програма як послуга (англ. Software as a service, SaaS) — модель поширення програм споживачам, при якій постачальник розробляє вебпрограму, розміщує її й керує нею (самостійно або через третіх осіб) з метою використання її замовниками через інтернет. Замовники платять не за володіння програмами як такими, а за їх використання (через API, що доступне через веб і яке часто використовують вебслужби). Близьким до терміну SaaS є термін «On-Demand» (за запитом). SaaS також відомий як «програмне забезпечення на вимогу» та програмне забезпечення на базі/вебхостинг.

Принциповою відмінністю моделі SaaS від попередніх (Hosted Applications та Application Service Provider (ASP)) є те, що отримується саме послуга та інтерфейс (призначений для користувача або програми), тобто деяка функціональність без жорсткої прив'язки до способу її реалізації.

SaaS вважається частиною хмарних обчислень разом з інфраструктурою як послугою (IaaS), платформою як послугою (PaaS), настільним комп'ютером як послугою (DaaS), керованим програмним забезпеченням як послугою (MSaaS), мобільним бекендом як послугою (MBaaS), центр обробки даних як послуга (DCaaS), інтеграційна платформа як послуга (iPaaS) та управління інформаційними технологіями як послуга (ITMaaS).

До програм SaaS зазвичай звертаються користувачі за допомогою тонкого клієнта, наприклад, через веббраузер. SaaS став загальною моделлю доставки для багатьох бізнес-додатків, включаючи офісне програмне забезпечення, програмне забезпечення для обміну повідомленнями, програмне забезпечення для обробки заробітної плати, програмне забезпечення СУБД, програмне забезпечення для управління, програмне забезпечення CAD , програмне забезпечення для розробки, гейміфікацію, віртуалізацію, бухгалтерський облік, співпрацю, управління відносинами з клієнтами (CRM)), інформаційні системи управління (MIC), планування ресурсів підприємства (ERP), виставлення рахунків, управління польовими послугами, управління людськими ресурсами (HRM), залучення талантів, системи управління навчанням, управління контентом (CM), географічні інформаційні системи (GIS) та управління службою обслуговування.

В сучасному цифровому світі SaaS-сервіси (Software as a Service) здобули широку популярність, надаючи зручність та доступність програмного забезпечення через хмарні технології. Однак, разом із зростанням популярності цих сервісів, збільшується і ризик зазнати атак на системи аутентифікації.

Методи фішингу та соціальної інженерії: зараз, атаки фішингу та соціальної інженерії стають все більш вдосконаленими. Атакувальники використовують не тільки електронну пошту, але і соціальні мережі та месенджери для того, щоб вивести користувачів з рівноваги та змусити надавати свої дані для аутентифікації.

Брутфорс атаки та словникові атаки: за допомогою програм для брутфорс атак, зловмисники намагаються вгадати паролі, спробувавши безліч можливих комбінацій. Сполучені зі словниковими атаками, які використовують популярні паролі та їх комбінації, ці методи можуть бути дуже ефективними. [3]

Атаки з використанням витоку даних: ще однією серйозною загрозою є виток особистих даних. Здобувши доступ до баз даних, зловмисники можуть використовувати витікнуту інформацію для атак на аутентифікацію, зокрема шляхом перевірки отриманих паролів та інших конфіденційних даних.

Мультифакторна аутентифікація (MFA) як відповідь на загрози: з урахуванням цих тенденцій, компанії та користувачі стають більш обізнаними і приймають заходи для забезпечення вищого рівня безпеки. Мультифакторна аутентифікація, що включає в себе не лише пароль, але і додатковий фактор, такий як OTP (одноразовий код), біометричні дані чи інші, стає стандартом для забезпечення захисту від атак.

Штучний інтелект та аналітика для виявлення аномалій: важливим напрямком розвитку є використання штучного інтелекту та аналітики для виявлення аномалій у поведінці користувачів. Системи можуть автоматично визначати незвичайні патерни, що можуть бути індикаторами атаки на аутентифікацію.

Загрози атак на аутентифікацію в SaaS-сервісах стають все складнішими та вдосконаленими. Захист від таких атак стає важливою частиною стратегії інформаційної безпеки. Розуміння та використання сучасних технологій, таких як мультифакторна аутентифікація та аналітика на основі штучного інтелекту, дозволяє підняти бар'єри перед потенційними загрозами та забезпечити безпеку для користувачів і компаній, які використовують SaaS-сервіси.

Таблиця 2 – Тенденції розвитку атак на аутентифікацію в SaaS-сервісах

Тенденція атаки	**Опис**	**Приклади заходів протидії**
Фішинг та соціальна інженерія	Зловмисники використовують маніпуляції та обман, щоб отримати конфіденційні дані користувачів.	Навчання користувачів впізнавати фішингові спроби, використання антиспам фільтрів.
Брутфорс та словникові атаки	Атакувальники спробують вгадати паролі шляхом спроб брутфорсу та використання популярних паролів.	Встановлення обмежень на кількість спроб введення пароля, використання сильних паролів.
Атаки з використанням витоку даних	Використання витоків даних для отримання конфіденційної інформації та подальшої атаки.	Шифрування конфіденційних даних, моніторинг витоків та інші заходи безпеки.
Мультифакторна аутентифікація (MFA)	Використання додаткових шарів аутентифікації, таких як OTP або біометричні дані.	Впровадження MFA для всіх користувачів, використання різних факторів аутентифікації.
Використання штучного інтелекту	Використання аналітики та штучного інтелекту для виявлення аномалій у поведінці користувачів.	Впровадження систем моніторингу та аналізу аномальної поведінки, використання машинного навчання для прогнозування атак.

Ця таблиця надає огляд основних тенденцій атак на аутентифікацію в SaaS-сервісах та пропонує приклади заходів для протидії цим загрозам. У реальних умовах важливо поєднувати різні стратегії безпеки для ефективного захисту від різноманітних атак.

Аналізуючи переваги та недоліки існуючих методів виявлення вразливостей аутентифікації в SaaS-сервісах, стає очевидним, що безпека має вирішальне значення в цифрову епоху, де доступ до інформації визначається швидкістю та ефективністю. Кожен метод, незалежно від своєї ефективності, має свої обмеження, і важливо приймати збалансований підхід до захисту.

Переваги сучасних методів, таких як мультифакторна аутентифікація та використання штучного інтелекту для виявлення аномалій, дозволяють створювати міцні бар'єри перед загрозами. Водночас, недоліки та вразливості деяких методів наголошують на необхідності постійного вдосконалення і вдосконалення стратегій безпеки. [4]

Здатність здійснювати ефективний моніторинг, реагувати на аномалії та розвивати та вдосконалювати заходи безпеки — це критичні аспекти успішного захисту аутентифікації в SaaS-сервісах. І хоча неможливо досягти абсолютної безпеки, збалансована стратегія, поєднана з освітою користувачів та постійним вдосконаленням, може значно зменшити ризики та забезпечити безпеку в еру високотехнологічних викликів.

Однак, незважаючи на всі виклики, ключовим аспектом є свідомість та сприйняття загроз з боку усіх учасників цифрового екосистеми. Тільки через спільний зусилля розробників, безпекових експертів та користувачів можна досягти ефективного та надійного захисту аутентифікації в SaaS-сервісах і забезпечити стійкість у світі, де безпека — це ключовий фактор успіху.

Суттєві характеристики. П'ять основних характеристик хмарних обчислень, які були визначені Національним інститутом США стандартів і технологій (NIST) стали де-факто стандарт для його визначення. Вони є:

– Самообслуговування на вимогу: - Це означає, що різні клієнти хмарних сервісів (зазвичай організації) можуть легко запросити, замовити або керувати власними обчислювальними ресурсами без будь-якого втручання або взаємодії з постачальники хмарних послуг.

– Повсюдний або широкий доступ до мережі: - Є різні послуги, які пропонує хмара отримати доступ через мережу (інтернет або інші приватні мережі). Він використовує певний стандарт механізми та протоколи.

– Об’єднання ресурсів: це означає об’єднання ресурсів різні необхідні обчислювальні ресурси для надання хмарних послуг організовано в однорідній спільній формі, яка називається пулом ресурсів з якого всі черпають ресурси користувачів або клієнтів послуг.

– Швидка еластичність: - Використання хмарних обчислень горизонтальне та вертикальне масштабування для збільшення та швидко скоротити доступ до різних ресурсів пружно.

– Вимірювані послуги: усі хмарні ресурси/послуги використання постійно вимірюється і клієнтів виставляються відповідні рахунки [5].

Всі атрибути, моделі обслуговування та інші характеристики хмарних обчислень призвели до його величезний розвиток, а також досягли цього вразливі до різних типів атак безпеки.

Перелік посилань

1. Nedeljković N., Vugdelija N., Kojić N. USE OF "OWASP TOP 10" IN WEB APPLICATION SECURITY. Fourth International Scientific Conference ITEMA Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture. 2020. URL: https://doi.org/10.31410/itema.2020.25.
2. Idris M., Syarif I., Winarno I. Development of Vulnerable Web Application Based on OWASP API Security Risks. 2021 International Electronics Symposium (IES), Surabaya, Indonesia, 29–30 September 2021. 2021. URL: https://doi.org/10.1109/ies53407.2021.9593934.
3. Yaworski P. How to Make Money Hacking Ethically. Web Hacking 101 : Kindle Edition. 2019.
4. Zalewski M. A Guide to Securing Modern Web Applications. The Tangled Web : Book, Poland, September 2011.
5. Scott D., Sharp R. Abstracting application-level web security. the eleventh international conference, Honolulu, Hawaii, USA, 7–11 May 2002. New York, New York, USA, 2002. URL: https://doi.org/10.1145/511446.511498.