МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

Таким чином, ми розглянули метод аналізу за допомогою переведення мережевої карти в нерозбірливий режим та метод розставляння сенсорів при пасивному мережевому аналізу. Виявлені деякі недоліки пасивного аналізу та запропоновано методи їх вирішення, а саме для вирішення проблеми аналізу загроз безпеці надаються методи використання нейронної мережі, як допоміжний інструмент у аналізі. Запропоновано використання ідентифікації користувачів мережі по заголовкам пакетів, що вони відправляють, для полегшення розслідувань та ідентифікації пристроїв з яких відбувалися неправомірні дії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Alexander J. Beecroft, Passive Fingerprinting of Computer Network Reconnaissance Tools, Monterey, CA 93943-5000, 2009, 89 p.
[2] A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral, Deep packet inspection as a service, 2014, p. 271.
[3]: Пассивный анализ сети. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.securitylab.ru/analytics/350448.php
[4] Исследование угроз безопасности и атак в сетях [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/ss7-vulnerability-2018/
[5] Colin J. Bennett, Andrew Clement, Kate Milberry, Introduction to Cyber-Surveillance. Cyber Surveillance in Everyday Life, 2012, 21 p.
[6] Network Intrusion Detection Signatures. [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-partfive.

УДК 004.738.5

АНАЛІЗ ХМАРНОЇ ТЕХНОЛОГІЇ GOOGLE DRIVE

РОМАНЮК О. Н., БОРИСОВА К. О., КАТЄЛЬНІКОВ Д. І. (*rom8591@gmail.com*)
Вінницький національний технічний університет

У статті розглянуто одне із найвідоміших хмарних сховищ даних та порівняно його з аналогічним продуктом від компанії Microsoft.

Хмарні сервіси [1-7], що дозволяють перенести обчислювальні ресурси й дані на віддалені інтернет-сервери, в останні роки стали одним з основних трендів розвитку IT-технологій. Щоб скористатися можливостями технологій, людині достатньо бути там, де є Інтернет, і мати пристрій, в якому є інтернет-браузер.

За даними аналітичного агентства *Research and Markets, очікується зростання глобального ринку хмарних обчислень від $371,4 млрд. у 2020 році до $832,1 млрд. у 2025 [1]. Необхідність у хмарних технологіях збільшилась внаслідок закриття офісів, шкіл і підприємств у зв'язку із пандемією COVID-19. Працівники використовують хмарні платформи для обміну даними та знаннями і спілкування протягом локдаунів.*

Одним із найпоширеніших подібних сервісів є хмарні сховища даних. *Хмарне сховище даних* – це модель зберігання цифрових даних в онлайновому просторі, що охоплює кілька серверів та місце розташувань, і зазвичай підтримується хостинг-компанією [2]. Таким чином, замість розміщення файлів на фізичних носіях пам'яті, здійснюється поступове перенесення інструментів і результатів роботи у хмарний простір задля підвищення їх доступності. Крім цього, втрата документа абсолютно виключена при хмарному зберіганні, коли копія документа завжди доступна на сервері та може бути легко знайдена засобами

пошуку з будь-якої точки планети, де є вихід в глобальну мережу, тоді як надмірна кількість зовнішніх накопичувачів може призвести до втрати важливих даних.

Хмарні сховища дозволяють синхронізувати дані між різними комп'ютерами та створювати резервні копії з комп'ютера у «хмару».

Розглянемо одне із найбільш використовуваних хмарних сховищ, а саме Google Drive.

Google Drive — сховище даних, яке належить компанії Google Inc., що дозволяє користувачам зберігати свої дані на серверах у хмарі та ділитися ними з іншими користувачами в Інтернеті [3].

Анонсований 24 квітня 2012 року, Google Drive дозволяє користувачам зберігати файли на своїх серверах, синхронізувати файли на різних пристроях і ділитися ними. Окрім веб-сайту, Google Drive пропонує додатки з автономними можливостями для комп'ютерів з ОС Windows і macOS, а також для смартфонів та планшетів Android і iOS. Станом на липень 2018, Google Drive мав понад 1 мільярд користувачів та понад 5 мільярдів завантажень.

Що стосується архітектури, Google Drive відображає типову модель клієнт-сервер. Процес, під час якого користувачі завантажують, зберігають та скачують файли, насправді є процесом кодування та декодування між веб-браузерами та окремими пристроями.

Для зберігання даних використовується Bigtable - високопродуктивна запатентована система, побудована на Google File System, Chubby Lock Service, SSTable (структурованому журналом сховищі, як LevelDB) та декількох інших технологіях Google [4]. Окрім цього, сервіс підтримується завдяки мовам програмування Python і Objective-C [3].

Для того, щоб зробити аналіз Google Drive більш об'єктивним, здійснимо коротке порівняння його з найбільшим конкурентом – OneDrive.

Google Drive ефективно працює з іншими програмами Google, такими як Google Docs та Google Sheets, тоді як OneDrive – це продукт Microsoft, тому він дуже добре поєднується з іншими програмами Microsoft.

Google Drive пропонує більший обсяг безкоштовного сховища (15 Гб порівяно з 5 Гб від OneDrive) та більший персональний варіант на 2 ТБ (максимальний об'єм пам'яті у персональному тарифі OneDrive – 1 Тб) [5]. OneDrive та Google Drive працюють однаково, коли йдеться про швидкість. Різниця стосується власних файлів Microsoft, і в цьому випадку block-level копіювання призводить до значно коротшого часу завантаження. Але за використання сервісів Google, block-level копіювання OneDrive не дає реальної переваги [6].

Платформи мають схожі користувацькі інтерфейси та протоколи управління файлами, але розширена функція пошуку Google Drive випереджає пошук OneDrive.

Google Drive дозволяє створювати резервні копії більшої кількості типів файлів, але OneDrive пропонує більше можливостей налаштування для резервного копіювання фотографій та відео.

З точки зору безпеки, жоден з постачальників не пропонує шифрування з нульовим розголошенням, що безумовно є недоліком з обох сторін [5].

Зваживши усі вищеперераховані факти, можна зазначити, що кожен із сервісів має свої переваги та недоліки, а вибір між ними залежить від того, продукти якої компанії – Miscrosoft чи Google – використовуються під час роботи.

Підсумовуючи вищесказане, можна стверджувати, що роль хмарних технологій зростатиме в наступні роки, прокладаючи шляхи для появи багатьох нових технологій. З появою хмарних сховищ даних значення зовнішніх носіїв та внутрішньої пам'яті пристрою зменшується. Послуги хмарного зберігання пропонують різноманітні опції, зручні для користувачів, як резервне копіювання даних, синхронізація, обмін та доступ до файлів на будь-яких пристроях в будь-якому місці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cloud Computing Market by Service Model – Global Forecast to 2025. Режим доступу: https://www.researchandmarkets.com/reports/5136796/cloud-computing-market-by-service-model
2. Siobhan Climer. What Is Cloud Storage Part 1: An Overview Of Cloud Computing Basics. Режим доступу: https://gomindsight.com/insights/blog/what-is-cloud-storage-overview-cloud-basics/
3. Google Drive. Режим доступу: https://uk.wikipedia.org/wiki/Google_Drive
4. Bigtable. Режим доступу: https://en.wikipedia.org/wiki/Bigtable
5. Dropbox vs Google Drive vs Onedrive: Comparing the Big Three in 2021. Режим доступу: https://www.cloudwards.net/dropbox-vs-google-drive-vs-onedrive/
6. Cloud Storage Showdown: OneDrive vs. Google Drive. Режим доступу: https://zapier.com/blog/onedrive-vs-google-drive/
7. Хошаба О. М. та О.Н. Романюк, «Деякі рішення проблем управління потоками даних у хмарних середовищах» Матеріали XV міжнародної конференції *"Контроль і управління в складних системах (КУСС-2020)*", м. Вінниця, 8-10 жовтня 2020 р. [Електронний ресурс]– Режим доступу: http://ir.lib.vntu.edu.ua//handle/123456789/30635.

УДК 004

АНАЛІЗ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

ТРОЩІЙ А.О. (*good180898@gmail.com*),
Харківський національний економічний університет імені Семена Кузнеця

Децентралізовані системи привернули широку увагу з появою технології блокчейн, яка використовуються в криптовалютах. Ці системи використовують властивості криптографії та ланцюгів для забезпечення консенсусу щодо фінансових транзакцій, які відбуваються в системі. Відкритий децентралізований характер системи робить її вразливою для критичних загроз і атак через присутність зловмисників. Загрози для децентралізованих систем стають критичними, оскільки відсутність централізованого управління ускладнює протидію цим загрозам і атакам. Тому важливо враховувати те, що потрібно досліджувати і забезпечити безпеку в децентралізованих системах.

Протягом останніх років децентралізовані системи активно просувалися, розвивалися і використовувались як взаємопов'язані інформаційні системи. В контексті обчислювальної техніки та інформаційних технологій децентралізовані системи зазвичай приймають форму мережевих комп'ютерів. У децентралізованій системі кожна сторона приймає локальні автономні рішення для досягнення своїх індивідуальних цілей, які можуть вступати в протиріччя з цілями інших сторін. Однорангові вузли безпосередньо взаємодіють один з одним і обмінюються інформацією або надають послуги іншим одноранговим вузлам.

Незважаючи на те, що децентралізовані системи надійніше централізованих, вони все одно схильні до збоїв, тому їх не можна назвати повністю надійними. Децентралізований характер системи робить її вразливою для загроз і атак. Наприклад, однією із загроз є відмова в обслуговуванні. Основна мета цієї атаки - відключити систему або унеможливити нормальну роботу. Але вихід з ладу однієї точки управління не призведе до падіння всієї системи.

Сучасні технології автентифікації, авторизації та шифрування дозволяють гарантувати зв'язок і захист від несанкціонованого доступу до даних, але з організаційної точки зору проблема безпеки даних не може бути вирішена. Децентралізоване зберігання даних в

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.