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.

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

хмарних системах повинна дати можливість усім сторонам самостійно вирішувати, які правила безпеки даних застосовуються до їх власними даними.

Оскільки злом даних продовжує відбуватися швидкими темпами, у майбутньому зростатиме попит на децентралізовані рішення, які дозволять людям захищати свої дані і конфіденційність [1]. Варіанти хмарного сховища значно поліпшили безпеку за останнє десятиліття, з різними рівнями безпеки для захисту даних як на рівні користувача, так і на рівні компанії. До них відносяться двофакторна автентифікація, наскрізне шифрування і багато іншого. Незважаючи на це, дані зазвичай як і раніше зберігаються на віддалених серверах, які можуть бути вразливими.

Забезпечення інформаційної безпеки - це процес, про який завжди повинні пам'ятати користувачі інформаційних систем. Жодна технологія і система не скасовує класичних методів забезпечення інформаційної безпеки [2].

Децентралізована система, зажадає розробки нових технологій інформаційної безпеки або переосмислення, аналізу та науково-технічного опрацювання застосування вже наявних. В силу розподіленого характеру систем необхідно врахувати можливі загрози, що відносяться не до конкретного користувача, а до системи в цілому, наприклад пов'язані з реалізацією комп'ютерних атак на інфраструктуру оператора, власника вузла або власника гаманця.

Завданнями забезпечення інформаційної безпеки залишаються забезпечення цілісності, доступності, конфіденційності інформації, підтвердження авторства, мінімізація ризиків технологічної залежності реалізованої інфраструктури від постачальників IT-послуг, продуктів і сервісів, забезпечення застосування довірених програмних і апаратних компонентів, а також протидія соціальної інженерії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Müller A. Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels [Електронний ресурс] / A. Müller, A. Ludwig, B. Franczyk. – 2017. – Режим доступу до ресурсу: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0082-3#ref-CR1.

2. Соколова Т. Н., Сыксин В. В. Управление децентрализованными системами с помощью технологии blockchain //Информационная безопасность регионов. – 2017. – №. 1 (26).

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.