ВІДГУК

офіційного опонента

Єсіна Віталія Івановича

на дисертаційну роботу Карпенка Андрія Сергійовича

на тему «Методи та засоби забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних з контрольованою узгодженістю», представлену на здобуття ступеня доктора філософії

в галузі знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

за спеціальністю 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Актуальність теми дисертаційної роботи

Забезпечення безпеки розподілених інформаційних систем є критично важливим завданням, оскільки ці системи активно використовуються у життєво важливих застосунках (системах зберігання банківських, медичних даних, системах системи військового призначення та інших важливих галузей життєдіяльності), відмови в яких можуть впливати на бізнес-процеси та життя людей. В епоху Великих Даних проблема забезпечення безпеки даних ще більше загострюється. За своєю природою глобально-розподілені системи, що працюють через публічну мережу Інтернет, особливо схильні до відмов компонентів і каналів зв'язку, а також кіберзагроз, спрямованих на порушення доступності та цілісності даних завдяки компрометації вузлів цих систем. У той час як сучасні інформаційні технології мають широкий спектр засобів криптографічного захисту, методів ідентифікації та автентифікації, які успішно вирішують завдання забезпечення конфіденційності даних, одночасне забезпечення доступності (готовності) та цілісності (узгодженості) даних – двох інших важливих властивостей інформаційної безпеки, у глобально-розподілених системах зберігання даних ускладнено через наявність існуючих протиріч між ними. А саме, традиційні механізми підвищення доступності в умовах інформаційних вторгнень, зокрема, резервування компонентів та реплікація даних, вимагають забезпечення синхронізації між репліками. Від цього також залежить і цілісність даних, яка на системному рівні перетворюється на необхідність забезпечення узгодженості між вузлами-репліками в умовах можливої компрометації деяких з них. Однак, для глобально-розподілених систем, компоненти яких знаходяться віддалено один від одного та об'єднані через глобальну мережу Інтернет, оновлення не можуть поширюватись миттєво. Це безумовно ускладнює забезпечення узгодженості між компонентами системи та підтримки доступності системи в цілому. Наприклад, очікування результату від усіх реплік для забезпечення сильної

узгодженості, особливо в умовах DDoS-атак може призвести до того, що відповідь від системи буде отримано лише після закінчення встановленого часу очікування (так званого тайм-ауту). Тобто, матиме місце порушення доступності. У той же час зниження рівня узгодженості підвищує ризик порушення цілісності інформації при компрометації окремих реплік. В цих умовах підвищення продуктивності системи та зниження часових затримок дозволить, з одного боку, підвищити її доступність та забезпечити більшу стійкість до DDoS-атак, а з іншого, – дає змогу збільшити рівень узгодженості без зниження доступності. Тому тема дисертаційної роботи, яка присвячена розробленню та удосконаленню методів та засобів забезпечення кібербезпеки глобально-розподілених реплікованих систем (ГРРС) зберігання даних й підвищення їхньої стійкості до загроз порушення доступності та узгодженості даних, є актуальною та своєчасною.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі, досягається аргументованим використанням відомих положень теорії ймовірності та математичної статистики, теорії систем масового обслуговування, методів математичного моделювання. Підтвердженням достовірності наукових результатів, поза сумнівом, є збіг результатів аналітичного та імітаційного моделювання при ідентичних структурах та параметрах глобально-розподілених реплікованих систем зберігання даних з результатами практичних випробувань та навантажувального тестування, а також позитивний досвід впровадження результатів роботи при проектуванні системи підтримки виконання асинхронних завдань, що підтверджується відповідними актами про впровадження.

Наукова новизна одержаних результатів

До основних нових наукових результатів дисертації слід віднести наступне:

– вперше запропоновано метод динамічного керування рівнем узгодженості ГРРС, який, на відміну від відомих, базується на побудові доменів змішаного робочого навантаження та дозволяє підвищити готовність системи, гарантуючи при цьому строгу узгодженість даних для підвищення стійкості до DDoS атак;

– удосконалено метод надлишкових читань ГРРС, який ґрунтується на використанні надлишковості щодо встановленого рівня узгодженості операцій читання та дозволяє зменшити екстремальні часові затримки та підвищити

готовність при встановленому обмеженні на час обслуговування або цілісність в умовах кіберзагроз порушення даних та відмов в обслуговуванні;

– розроблено комплекс нових та удосконалених моделей для глобально-розподілених систем зберігання даних, які забезпечують: деталізацію загроз кібербезпеки ГРРС та формалізацію опису патернів розгортання ГРРС у хмарному середовищі з урахуванням доменів готовності за допомогою апарату теоретико-множинного представлення, а також оцінювання готовності та зменшення часу обслуговування в умовах кібератак завдяки використанню механізму надлишкових читань за допомогою гібридного імітаційного підходу.

Повнота викладу основних наукових результатів у опублікованих працях

Основні отримані в роботі результати були апробовані і в належній мірі опубліковані у фахових виданнях. Відповідно до основного переліку робіт, за темою дисертаційної роботи було опубліковано 5 наукових праць, серед яких: 2 статті у наукових фахових виданнях України категорії Б; 2 статті у англомовних журналах категорії А, що індексовані у базі даних Scopus (квартіль Q3); 1 публікація в працях міжнародної конференції, матеріали якої включено у базу даних Scopus.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44.

Оцінка змісту дисертаційної роботи, її завершеність

Дисертаційна робота складається із вступу, чотирьох розділів, висновку, списку виконаних джерел і додатків. Загальний обсяг дисертації складає 172 сторінки, з яких анотація на 5 сторінках, зміст на 3 сторінках, перелік умовних позначень на 9 сторінках, основний текст на 133 сторінках, список використаних джерел із 100 найменувань на 10 сторінках, додатки на 39 сторінках. Робота містить 30 таблиць та 50 рисунків.

У вступі обґрунтовано актуальність дослідження, поставлену мету та визначено основні завдання дослідження, об’єкт та предмет дослідження. Викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Подано відомості про апробацію та опубліковані результати досліджень.

У першому розділі проаналізовано області використання і можливості систем зберігання даних. Розглянуто розвиток та проблеми архітектур систем

зберігання даних. Також проаналізовано моделі кібербезпеки ГРРС зберігання даних у частині забезпечення цілісності, доступності та конфіденційності, а також взаємозв’язок з моделлю гарантоздатності.

У другому розділі удосконалено модель загроз глобально-розподілених реплікованих систем зберігання даних, а також розроблено теоретико-множинну модель патернів розгортання ГРРС зберігання даних, спираючись на можливості її та провайдера хмарних послуг. Запропоновано та досліджено метод динамічного керування рівнем узгодженості, що дозволяє підвищити доступність системи та стійкість до DDoS атак.

У третьому розділі запропонована модель конфігурації надлишкових читань, що дозволяє описати взаємозв’язок між рівнем узгодженості, кількістю опитаних реплік та загальною кількістю реплік ГРРС зберігання даних. Виконано удосконалення методу надлишкових читань, який дозволяє підвищити доступність та цілісність. Виконано аналіз результатів використання методу надлишкових читання для підвищення доступності за допомогою розробленої гібридно імітаційної моделі.

Четвертий розділ дисертаційного дослідження є логічним продовженням попередніх розділів. У якому розроблено комплекс інформаційних технологій, яка дозволяє виконати розгортання, навантажувальне тестування, аналіз налаштувань та безперервний моніторинг глобально-розподіленого реплікованого кластеру. Також представлені результати впровадження дисертаційного дослідження.

Розділи дисертаційної роботи організовані за логічними блоками, прослідкується зв'язок між ними, що забезпечує достатньо наглядний перехід від одного аспекту дослідження до іншого. Простежується дотримання академічного стилю. Здобувач використовує наглядні приклади та ілюстрації, що допомагають усвідомити основні ідеї та результати досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних.

Академічна доброчесність

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено. Усі результати, які винесено автором на захист, містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Недоліки та зауваження до дисертаційної роботи

1. У розділі 1.7.1 зазначається, що засоби забезпечення конфіденційності досить розвинені, але не розглядаються окремо.
2. Результати експериментальних досліджень, які наведені у розділі 2.3 були отримані при використанні хмарного провайдеру AWS. Чи будуть вони відрізнятися, якщо в якості провайдера для розгортання ГРРС буде використовуватися інший хмарний провайдер?
3. Для дослідження продуктивності ГРРС в залежності від рівня узгодженості, використовується фреймворк YCSB з певними параметрами, які зазначені у розділі 2.3.3. Однак обрані параметри потребують більш ретельного обґрунтування, наприклад, чому саме використовується розмір пакету у 1000 байт?
4. У 3-му розділі запропонований метод надлишкових читань, який може використовуватися для підвищення цілісності ГРРС. Показана ефективність цього методу за умов порушення цілісності однієї з реплік. Однак на практиці атаки порушення цілісності можуть бути спрямовані на всі репліки одразу. Такий варіант у дисертації не розглядається.
5. В дисертації є ряд описок, орфографічних помилок, семантично некоректних подань окремих термінів та понять, наприклад: Зміст: с. 7 – «…дослідження. та», с. 8 – «глобально-розподілених репліційованих систем»; п. 1.2 (с. 18): є вимогі ACID або набір властивостей ACID, але не теорема ACID; у п. 1.7.1 с. 37 згадується деяка традиційна модель доступу, яка має дві категорії, насправді це дві відомі моделі доступу: модель вибіркового керування доступом (discretionary access control – DAC) та модель мандатного керування доступом (mandatory access control – MAC).

Однак означені недоліки суттєво не впливають на зміст та отримані науково-практичні результати дисертації.

Висновок про дисертаційну роботу

Дисертаційна робота Карпенка Андрія Сергійовича «Методи та засоби забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних з контрольованою узгодженістю» за своїм змістом відповідає спеціальності 125 Кібербезпека та захист інформації. Представлена робота виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеною науково-дослідною роботою, яка розв’язує актуальну науково-прикладну задачу розроблення та удосконалення методів та засобів для забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних. В результаті проведених досліджень отримані нові науково обґрунтовані результати.

Вважаю, що дисертаційна робота Карпенка А. С. відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44, а здобувач Карпенко Андрій Сергійович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент:
доктор технічних наук, професор,
професор кафедри безпеки
інформаційних систем і технологій
Харківського національного
університету імені В. Н. Каразіна Віталій Єсін

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу
кадрів

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА * КОД 02071205