Рішення разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Разова спеціалізована вчена рада Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» Міністерства освіти і науки України, м. Харків прийняла рішення про присудження ступеня доктора філософії
у галузі знань 12 Інформаційні технології
на підставі публічного захисту дисертації на тему
«Методи та засоби забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних з контрольованою узгодженістю»
за спеціальністю 125 Кібербезпека та захист інформації
"7" березня 2024 року.

Карпенко Андрій Сергійович 1995 року народження, громадянин України, освіта вища: закінчив у 2018 році Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут» за спеціальністю Кібербезпека.

Працює асистентом кафедри комп'ютерних систем, мереж і кібербезпеки у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут», Міністерства освіти і науки України, м. Харків з 2023 року до цього часу.

Дисертацію виконано у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут», Міністерства освіти і науки України, м. Харків.

Науковий керівник Горбенко Анатолій Вікторович, доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

Здобувач має 4 наукових публікацій за темою дисертації, з них 2 статей у наукових фахових виданнях України, 2 статей у періодичних наукових виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

1. А. Карпенко, О. Тарасюк, і А. Горбенко, «Дослідження узгодженості та продуктивності у нереляційних реплікованих баз даних», Сучасні інформаційні системи, т. 5, №3, pp. 66-75, 2021. DOI: doi.org/10.20998/2522-9052.2021.3.09

2. A. Gorbenko, A. Karpenko, and O. Tarasyuk, «Performance evaluation of various deployment scenarios of the 3-replicated Cassandra NoSQL cluster on AWS», Radioelectronic and computer systems, no. 4 (100), pp. 157-165, 2021. DOI: 10.32620/reks.2021.4.13

3. J. Ahmed, A. Karpenko, O. Tarasyuk, A. Gorbenko, and A. Sheikh-Akbari «Consistency issue and related trade-offs in distributed replicated systems and databases: a review», Radioelectronic and computer systems, no. 2 (106), pp. 171-179, 2023. DOI: 10.32620/reks.2023.2.14

4. О. Тарасюк, А. Горбенко, і А. Карпенко, «Розвиток архітектур, теорем та моделей властивостей розподілених систем зберігання даних», Вимірювальна та обчислювальна техніка в технологічних процесах, №2, pp. 5-13, 2022. DOI: 10.31891/2219-9365-2022-70-2-1

У дискусії взяли участь голова і члени спеціалізованої вченої ради та присутні на захисті фахівці:

1. Голова разової спеціалізованої вченої ради Лукін В. В., д.т.н., проф., завідувач кафедри інформаційно-комунікаційних технологій ім. О.О. Зеленського Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

Зауваги:

— хто ініціював дослідження в обраному напрямку – це була Ваша ініціатива чи Вашого наукового керівника?

— яке співвідношення між кібербезпекою та гарантоздатністю? В чому полягає різниця?

— чи є недоліки у запропонованих Вами рішень? Якщо так, то в чому вони полягають?

— у четвертому розділі здобувач наводить стисло приклад реалізації наукових результатів, але не зрозуміло можливості цієї системи та які функції на неї покладені.

2. Рецензент Пєвнєв В.Я., д.т.н., доц., професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

Зауваги:

— не зрозуміло, чому здобувач вводить поняття готовності до інформаційної безпеки замість традиційного поняття доступності, ставлячи їх до одного ряду (стор. 12). При цьому визначення готовності (стор. 39, 41) практично не відрізняється від визначення доступності (НД ТЗІ 1.1-003-99).

— не зрозуміло, як працює метод динамічного керування, який представлений на рис. 2.16.

— при оцінки ефективності методу динамічного керування рівнем узгодженості не визначено критерія ефективності.

— дисертаційна робота має зауваження щодо оформлення: багато неповних сторінок (стор. 17, 20, 23 та ін.), порушено порядок посилань на рисунки (стор. 52), невірно оформлені розриви таблиць (табл. 2.1, 2.2), помилки під рисунками (2.7, 2.9в, 2.13).

3. Рецензент Фесенко Г.В., д.т.н., проф., професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

Зауваги:

— у розділі 1 автором розглядається модель загроз глобально-розподілених реплікованих систем зберігання даних з урахуванням теореми CAP, яка пов'язує такі властивості як узгодженість (consistency), готовність (availability) та стійкість до розділів (partition tolerance). Але, розподіл системи в явному вигляді не розглядається як окрема загроза кібербезпеки глобально- розподіленої реплікованої системи зберігання даних;

— у розділі 2.3 відсутнє обґрунтування доцільності вибору для використання у дослідженнях хмарного провайдера AWS;

— з огляду на погану екстраполяцію, незрозумілим є обрання у пункті 2.4.2 поліноміальної функції регресії четвертого порядку для опису поведінки експериментальних даних;

— дисертаційна робота має зауваження стилістичного характеру.

4. Офіційний опонент Єсін В.І., д.т.н., проф., професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна.

Зауваги:

— у розділі 1.7.1 зазначається, що засоби забезпечення конфіденційності досить розвинені, але не розглядаються окремо;

— 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?

— 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?

— 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;

— у 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).

5. Офіційний опонент Смірнов О.А., д.т.н., проф., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Зауваги:

— у розділі 2.1 використовується метод оцінки загроз STRIDE без порівняння з іншими аналогічними методами. Чому застосовується саме STRIDE методологія?

— у розділі 2.3.2 виконується порівняння тестових фреймворків, які дозволяють виконати навантажувальне тестування. Обраний YCSB фреймворк має велику кількість параметрів не всі з яких були застосовані під час досліджень;

— у роботі зазначено «протиріччя між властивостями узгодженості та готовності», але задача оптимізації не була поставлена у формальному вигляді, а також не наведено обґрунтування методу оптимізації, що використовувався;

— у розділі 3 для оцінки ефективності запропонованого методу надлишкових читань для підвищення готовності й цілісності була розроблена та використовувалася імітаційна модель. Чи не доцільно було б для вирішення цієї задачі використовувати теорію масового обслуговування?

— під час оцінки підвищення готовності глобально-розподілених реплікованих систем зберігання даних при використанні методу динамічного керування рівнем узгодженості та методу надлишкових читань, які запропоновані у розділах 2 та 3 дисертаційної роботи відповідно, не враховується базовий рівень готовності хмарного провайдеру, що надається у Service-level agreement (SLA) та інших чинників, що можуть впливати на кібербезпеку.

На зауваги Здобувач дав такі відповіді:

1. Відповіді на зауваги Голови ради Лукіна В.В.:

— у 2018 році я закінчив магістратуру за спеціальністю кібербезпека і вже мав досвід роботи з хмарними обчисленнями та розподіленими системами. В результаті, ми з науковим керівником дійшли висновку, що гарною темою для роботи може бути дослідження властивостей та протиріч розподілених систем у розрізі інформаційної безпеки;

— як відомо, модель кібербезпеки характеризується властивостями готовності, цілісності та конфіденційності. У свою чергу модель гарантоздатності включає ці властивості окрім конфіденційності;

— так дійсно, недоліки є. У методі надлишкових читань для підвищення цілісності використовується припущення, що тільки одна репліка у кластері може бути зі спотвореними даними, однак на практиці може бути дві та більше реплік. Також недоліком методу динамічного керування рівнем узгодженості може слугувати те, що при зміні фізичної інфраструктури необхідно виконувати повторне навантажувальне тестування;

— так дійсно, наукові результати, які були отримані у дисертаційному дослідженні, а саме метод динамічного керування рівнем узгодженості та метод надлишкових читань для підвищення готовності були впроваджені у e-commerce систему. Дана система має дворівневу архітектуру, де компоненти бізнес-логіки розташовані у системі оркестрації Kubernetes та глобально-розподіленою системою зберігання даних. Основною метою даної системи є підтримка процесу виконання асинхронних завдань;

— з іншими зауваги погоджуюсь.

2. Відповіді на зауваги рецензента Пєвнєв В.Я.:

— дійсно, з точки зору кібербезпеки та моделі CIA (конфіденційність, цілісність та доступність) у стандартах та законах, які регулюють інформаційну сферу зазначається термін доступність. На системному рівні це трактується, як готовність системи. Тому у роботі зосереджено увагу на системний рівень в цілому. Крім того, у роботі розглядається готовність системи, як необхідна умова доступності інформаційних ресурсів;

— метод динамічного керування рівнем узгодженості, який представлений у другому розділі, складається з двох етапів. На першому етапі виконується: формування вимог до системи, безпосереднє розгортання, навантажувальне тестування та пошук кращих налаштувань узгодженості. На другому етапі виконується безперервний моніторинг навантаження та корекція налаштувань. Перший етап може бути безпосередньо виконаний на етапі проектування системи, а другий етап повинен безпосередньо виконуватися під час реального навантаження;

— у роботі критерієм ефективності методу динамічного керування рівнем узгодженості є мінімізація затримки, яка напряму зв'язана з готовністю системи та атаками типу «відмова в обслуговуванні»;

— з іншими зауваги погоджуюсь.

3. Відповіді на зауваги рецензента Фесенка Г.В.:

— дійсно, у роботі розглядаються розділ, як аспект готовності;

— дійсно, існують різні хмарні провайдери, але більш вживаним є AWS. Крім того, AWS має більш розвинену мережу обчислювальних центрів обробки даних, що дає можливість дослідити різні конфігурації глобально-розподіленого кластеру;

— дійсно, поліноміальні функції, особливо великих порядків треба обережно використовувати для передбачення. Однак, вони добре підходять до інтерполяції. У роботі ми змінювали діапазон навантаження системи встановленим технічним завданням. Ці функції не були використані для екстраполяції;

— з іншими зауваги погоджуюсь.

4. Відповіді на зауваги опонента Єсіна В.І.:

— так дійсно, однією з важливих властивостей кібербезпеки є конфіденційність. Для глобально-розподілених реплікованих систем зберігання даних, широко використовуються криптографічні примітиви. Для захисту даних, які передаються та зберігаються використовується криптографічні алгоритми та протоколи. Здебільшого, механізми захисту від несанкціонованого доступу вже інтегровані у мережеві протоколи та існуючі розподілені системи. У роботі властивість конфіденційності винесено за лапки і дисертація сфокусована на дві інші властивості – готовність та цілісність.

— так дійсно, у роботі був використаний хмарний провайдер AWS. Якщо експериментальні дослідження провести з залученням інших хмарних провайдерів, такі як Azure, GCP, тоді конкретні цифри будуть відрізнятися, однак, взаємодія між узгодженістю та швидкодією залишиться сталою і не залежать від провайдера хмарних послуг;

— так дійсно, фреймворк YCSB має багато параметрів, які можна налаштувати під конкретну задачу. Розмір пакету у 1000 байт обраний тому, що для навантажувального тестування створюється база даних з 10-ма полями. Також більшість наукових робіт, використовують типову конфігурацію. Тому це необхідно для порівняння з результатами інших дослідників;

— так дійсно, у роботі використовується припущення про те що під час запису даних до однієї репліки-вузла, може бути порушена цілісність інформації. Але може бути ситуація, коли скомпрометовано більшість реплік, з огляду на цей

факт, цей метод застосовувати не можна. Для протидії потрібно використовувати більше реплік у кластері, але це потребує додаткових досліджень;

— з іншими зауваги погоджуюсь.

5. Відповіді на зауваги опонента Смірнова О.А.:

— так дійсно, існують також інші методи оцінки загроз окрім методу STRIDE. Це можуть бути DREAD, PASTA та інші. На відміну від перелічених методів, метод STRIDE є частиною Microsoft Software Development Lifecycle, що є досить вживаною. Також важливим моментом є інструментальний засіб, який дозволяє використати метод STRIDE. У роботі використовується інструмент з відкритим кодом OWASP Threat Dragon;

— так дійсно, задача оптимізації вирішувалася і полягала у забезпечені мінімальної затримки при встановленому рівні узгодженості. Але розмірність задачі є такою, що не потребує використання спеціальних методів оптимізації, а отже йде мова про кількість реплік. У експериментальних дослідженнях був використаний типовий рівень реплікації, який дорівнює трьом і у такому випадку можна використати повний перебір варіантів;

— так дійсно, використання моделі масового обслуговування надає багато переваг. Однак, теорія масового обслуговування накладає жорсткі обмеження та припущення, які добре працюють у локальній мережі, але вони не виконуються у глобально-розподілених реплікованих системах зберігання даних, наприклад, властивість стаціонарності, однорідний потік заявок. У глобально-розподілених реплікованих системах зберігання даних не можливо відділити затримку в мережі та час обробки на стороні сервера саме ці обмеження зумовили не використання теорії масового обслуговування;

— так дійсно, важливим компонентом функціонування глобально-розподіленої реплікованої системи є її фізична інфраструктура. Як відомо, хмарні провайдери використовують SLA, де зазначають доступність своїх сервісів. У роботі здебільшого були використані віртуальні машини, які можуть бути схильні до відмов або деградації. Це можуть бути «шумні сусіди», відмова підсистем тощо. У дисертації рівень SLA не було враховано, але це досить гарна тема для подальшого дослідження.

Члени разової ради визнали відповіді задовільними незадовільними

Результати голосування: "За" 5 членів ради, "Проти" 0 членів ради.

На підставі результатів голосування разова спеціалізована вчена рада присуджує *Карпенку Андрію Сергійовичу* ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Голова разової спеціалізованої вченої ради _____ Володимир ЛУКІН

Підпис голови разової ради доктора тех. наук,
професора Володимира Лукіна засвідчую.

Учений секретар
Національного аерокосмічного університету
ім. М. Є. Жуковського
«Харківський авіаційний інститут» _____ Тетяна БОНДАРЄВА

М.П. «28» лютого 2024 року