

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
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

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

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ
ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції



Одеса

20-21 квітня 2023 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р. - Одеса, Видавництво ОНТУ, 2023 р. – 449 с.

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

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області ІТ, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямками і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

7. Порівняльний аналіз сучасних шляхів діагностики складних технічних виробничих систем. Лактіонов О. (Національний університет «Полтавська політехніка») 93	93	
8. Optimization of paths, taking into account the significance of intermediate points. Мазурок І.Є., Веремйов К.В. (Одеський національний університет ім. Мечникова) 95	95	
9. Методика навчання фахівців із інформаційної безпеки соціальної інженерії з використанням OSINT і мови SIEVE. Міронов І. В., Болтач С. В. (Одеський національний технологічний університет) 97	97	
10. Дослідження факторів впливу на безпеку мобільних застосунків на прикладі клієнтської частини кіберфізичної системи розумної парковки. Павлова О.О., Авсієвич В.Р., Кузьмін А.А. (Хмельницький національний університет) 98	98	
11. Парсинг тексту: використання потужностей NLP задля підвищення точності отримуваних даних. Пелович Д. В., Смиш О. Р. (Національний університет «Києво-Могилянська академія») 100	100	
12. Захист підприємств від кібератак на корпоративні мережі. Петрук Д. С. (Волинський національний університет імені Лесі Українки) 102	102	
13. Використання мобільних застосунків у роботі з документацією ТОВ "Агрона Фрут Україна". Погоріла Ю. В. (Донецький національний університет імені Василя Стуса) 103	103	
14. Технологія HDR у моніторах. Романюк О. Н., Захарчук М. Д., Романюк О.В., Коробейнікова Т. І. (Вінницький національний технічний університет, Національний університет «Львівська політехніка») 105	105	
15. Проектування інформаційної системи управління сегрегаційним комплексом збору відходів оперативної поліграфії. Сторожук Д.І. (Українська академія друкарства) 107	107	
16. Дослідження методів перетворення повідомлень у бортових автомобільних системах. Чайковський О.Р., Селіванова А.В. (Одеський національний технологічний університет) 109	109	
17. Процес безпечної передачі інформації у мобільному додатку “Студент ЧДТУ” з використанням Spring Security на основі JWT. Куницька С.Ю., Архіпов М.О., Чоповенко В.М. (Черкаський державний технологічний університет) 110	110	
18. Захист даних та вихідних файлів від несанкціонованого доступу та копіювання комп’ютерних відеоігор. Шаповал В.В. (Київський національний університет імені Тараса Шевченка) 112	112	
19. Програмне забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах. Шевчук Р.П., Заріцький О.І. (Західноукраїнський національний університет) 114	114	
20. Вплив війни в Україні на кібербезпеку. Шередега Р.О., Бутенко Т.А. (Харківський державний біотехнологічний університет) 116	116	
21. Дослідження застосування стандартів PAPERLESS у закладах вищої освіти. Чіклікчі О.С., Лукашенко Д.О., Ольшевська О.В. (Одеський національний технологічний університет) 117	117	
22. 3-D візуалізація авторадіограмм радіоактивних частинок. Новіков А.М. (Інститут проблем безпеки атомних електростанцій Національної академії наук України) 119	119	
Розділ 3: Нові інформаційні технології в освіті		121
1. Development of a methodology for evaluating the efficiency of ship operator model. Nosov P.S., Masonkova M.M., Diahyleva P.S., Solovey O.S. (Херсонська державна морська академія) 121	121	
2. Optimization of management processes for maritime transport personnel qualification. Nosov P.S., Ponomaryova V.P., Diahyleva O.S., Ben A.P. (Херсонська державна морська академія) 123	123	
3. Using SolidWorks in modern education and science. Rudyk O.Yu., Baranov I.I., Gereta M.M., Dytynyuk V.O., Fedoryshyn S.I. (Хмельницький національний університет) 125	125	

програмного забезпечення». Впевнені, що прийняття подібного рішення в багатьох ВНЗ України призведе до збільшення кількості якісних спеціалістів у даній сфері.

Як висновок, хочемо зазначити, що наші пропозиції можуть усунути не всі проблеми, що пов'язані із захистом даних та вихідних файлів комп'ютерних відеоігор, однак реалізація наших пропозицій може значно зменшити рівень копіювання відеоігор, порушення авторських прав, створення чіт-кодів чи іншого шкідливого забезпечення, що порушує умови компанії-розробника відеоігор та користувачів загалом.

УДК 004.056.5:004.738.5

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РЕЗЕРВНОГО АРХІВУВАННЯ ДАНИХ У ХМАРНИХ СИСТЕМАХ

ШЕВЧУК Р.П. (rsh@wunu.edu.ua), ЗАРІЦЬКИЙ О.І. (olekszaritski@gmail.com)
Західноукраїнський національний університет

У роботі проведено аналіз існуючих хмарних систем резервного копіювання даних та запропоновано програмне забезпечення для забезпечення безпеки резервного архівування даних. Архітектура розробленого програмного забезпечення складається з шести основних модулів, які забезпечують безперебійну роботу системи резервного копіювання та мінімізують ризики викрадення архівних даних за рахунок покращення контролю доступу до них.

Вступ. Резервне архівування даних є важливою складовою забезпечення безпеки даних, та незамінним інструментом для забезпечення їх відновлення у випадку втрати [1]. Однак, при зберіганні даних в хмарі, існують додаткові ризики безпеки, такі як втрата даних внаслідок відмови обладнання, неправильної конфігурації, несанкціонованих доступ до даних, а також кібератаки [2,3]. Одним із підходів для зменшення цих ризиків є використання надійного програмного забезпечення для резервного архівування даних.

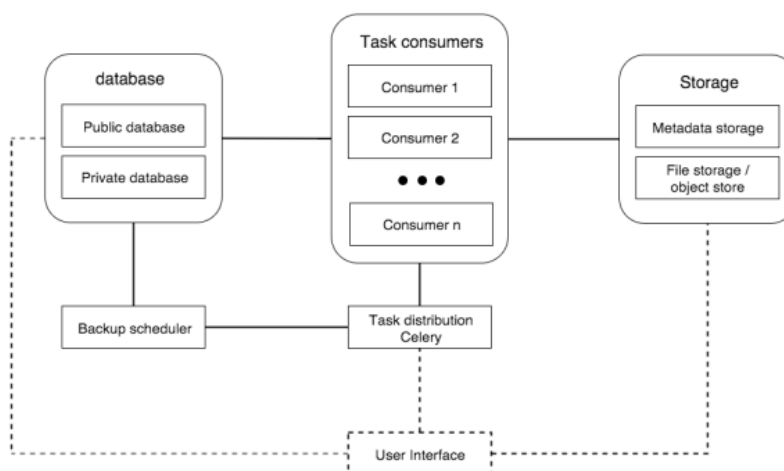
Мета роботи. Метою даної роботи є розробка програмного забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах, яке дозволить мінімізувати ризики викрадення архівних даних.

Основна частина. У роботі проведено аналіз існуючих систем резервного копіювання, зокрема: Amazon Web Services (AWS) Backup, Microsoft Azure Backup, Google Cloud Storage, Backblaze, Dropbox, Acronis Cloud Backup, IDrive Cloud Backup. За результатами аналізу описано технічні можливості та функціонал систем, виділено їх переваги та недоліки, а також оцінено ефективність їх роботи. Показано, що проаналізовані системи не враховують ряд ризиків, пов'язаних з використанням резервного архівування даних у хмарі.

Для зменшення цих ризиків у роботі розроблено спеціалізоване програмного забезпечення резервного архівування даних, яке дозволяє мінімізувати ризики викрадення архівних даних. Для розробки програмного забезпечення використано мови програмування C#, фреймворк ASP.Net та базу даних PostgreSQL.

Архітектура розробленого програмного забезпечення складається з наступних модулів: бази даних, черги розподілу завдань, вузлів обробки, модуля зберігання метаданих файлів, об'єктного сховища та планувальника резервного копіювання (рисунок 1).

У програмному забезпеченні для ідентифікації користувачів, контролю доступу та шифрування даних використано протокол Kerberos [4], а для авторизації сторонніх додатків для доступу до архівних даних протокол OAuth [5]. Використання цих протоколів дозволило забезпечити безпеку даних у хмарних сервісах, зменшити ризики викрадення даних та збільшити контроль за доступом до даних.



Рисуюнок 1- Архітектура програмного забезпечення

Висновки. У роботі проведено аналіз існуючих хмарних систем резервного копіювання даних. Визначено технічні можливості та функціонал кожної з цих систем, а також їх переваги та недоліки. Показано, що існуючі системи не враховують ряд ризиків безпеки, пов'язаних з використанням резервного архівування даних у хмарі. Для зменшення цих ризиків було розроблено програмне забезпечення на базі мови програмування C#, платформи ASP.Net та бази даних PostgreSQL з використанням протоколів Kerberos та OAuth. Архітектура розробленого програмного забезпечення складається з шести основних модулів, які забезпечують безперебійну роботу системи резервного копіювання та мінімізують ризики викрадення архівних даних за рахунок покращення контролю доступу до них.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Jiang, Tao, et al. "ReliableBox: Secure and Verifiable Cloud Storage with Location-Aware Backup." *IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society*, vol. 32, no. 12, 2021, pp. 2996–3010, doi:10.1109/tpds.2021.3080594.
2. Kumari, Sushila, et al. "Analysis of Cloud Computing Security Threats and Countermeasures." *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, 2022, pp. 1–6.
3. Selvamani, K., and S. Jayanthi. "A Review on Cloud Data Security and Its Mitigation Techniques." *Procedia Computer Science*, vol. 48, 2015, pp. 347–352, doi:10.1016/j.procs.2015.04.192.
4. Pachaghare, Swatee, and Pragati Patil. "Improving Authentication and Data Sharing Capabilities of Cloud Using a Fusion of Kerberos and TTL-Based Group Sharing." *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, 2020, pp. 1401–1405.
5. Oh, Se-Ra, and Young-Gab Kim. "Interoperable OAuth 2.0 Framework." *2019 International Conference on Platform Technology and Service (PlatCon)*, IEEE, 2019, pp. 1–5.