

Засіб для захищеного резервного копіювання

Анотація

Робота присвячена покращенню існуючих інструментів для захищеного резервного копіювання даних в комп'ютерних мережах, створенню застосунку для досягнення даної мети.

Ключові слова: резервування даних, програмні застосунки, протокол, метод.

Abstract

The work is devoted to improving the existing tools for secure data backup in computer networks, creating an application to achieve this goal.

Key words: data backup, software applications, protocol, method.

Вступ

Сьогодні більша частина інформації зберігається в електронному вигляді і втрата цієї інформації може призвести від негативних емоцій, якщо йдеться про інформацію на персональному комп'ютері рядового користувача, до значних збитків, а іноді і повного банкрутства, якщо мова йде про компанії. Резервне копіювання – процес створення копії даних з носія, призначений для відновлення цих даних у разі їх пошкодження або видалення [1]. Резервування даних, як метод надійного збереження інформації є одним з найважливіших елементів для забезпечення надійної роботи мереж. Введення надмірності, завдяки якому резервування дозволяє підвищити характеристики надійності технічних пристроїв, поділяється на кілька видів: апаратне, програмне, часове та функціональне [2]. Об'єктом резервного копіювання є дані або їх сукупність, з яких можна створити резервну копію [3]. Прикладом таких об'єктів є : файли баз даних, дані програм, дані операційної системи чи сама операційна система. Результатом роботи буде програмний застосунок для операційної системи Windows, який буде шифрувати та резервувати дані на захищені сервери, при цьому дотримуючись їх цілісності, та доступності перед користувачем.

Результати дослідження

Спершу потрібно розглянути методи резервного копіювання, провести дослідження і вибрати оптимальний для розробки програмного застосунку на його основі в подальшому. В галузі систем резервного копіювання існують такі методи [4] :

- повне резервування – створення детальної копії всіх файлів на дисках (робочих та системних), без врахування змін, що відбулись між сеансами резервування;
- диференціальне резервування – цей спосіб має на увазі те, що всі файли, які були змінені після повного резервування, копіюються заново;
- інкрементне резервування – процедура схожа на диференціальну за винятком того, що копії не створюються.

Резервні копії можуть зберігатися на різних носіях в залежності від потреб. Найчастіше використовують сервер резервного копіювання, який керує процесами резервного копіювання та сховищами. Сховища бувають такими [5]:

- стример або стрічкова бібліотека – запис копій відбувається на магнітну стрічку стримеру;
- дискові сховища - запис на диски, що можуть бути об'єднані в надлишковий масив незалежних дисків або на дискову систему збереження;
- віртуальна стрічкова бібліотека – запис відбувається на диски, але саме сховище для клієнта виглядає як стрічкова бібліотека;
- «хмарний» бекап – запис копій за «хмарною» технологією через онлайн-служби спеціальних провайдерів.

Для даного технічного застосунку доцільно використати саме диференціальне резервування. Даний тип резервування дозволить зменшити обсяг даних на резервному носії і при необхідності прискорити процес відновлення даних. Оскільки диференціальне копіювання зазвичай проводиться набагато частіше, ніж повне резервне копіювання, воно є дуже

ефективним, так як дозволяє відновлювати ті дані, які зазнали змін зовсім недавно, і відслідковувати історію зміни файлів з моменту повного копіювання. Крім того, диференціальне резервне копіювання також захистить дані від вірусів, тому що буде гнучкіша можливість відновлення файлів.

Також систему резервного копіювання прийнято вважати розподіленою, якщо складові системи є фізично рознесеними та є окремими мережними вузлами [6].

Структура запропонованого засобу показана на рис.1

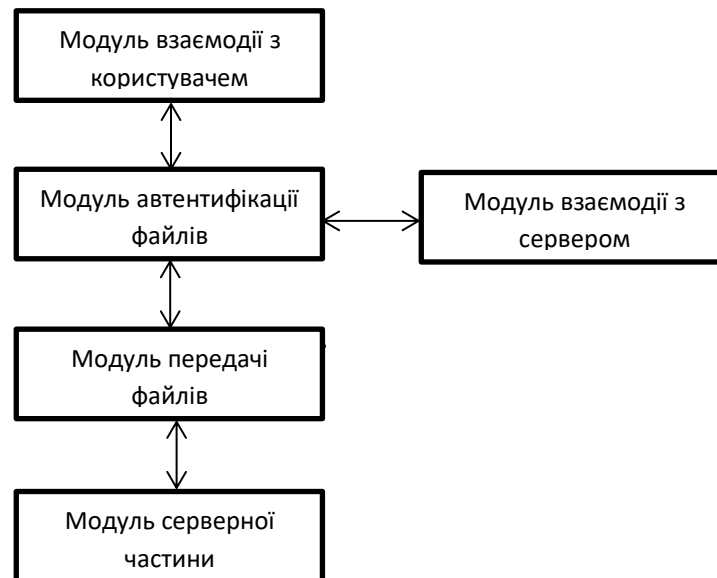


Рисунок 1 – Структурна схема засобу для захищеного резервного копіювання

Узагальнена структура програмного засобу: модуль взаємодії з користувачем модуль взаємодії з сервером, модуль передачі файлів, модуль автентифікації файлів (перевірка на цілісність), модуль серверної частини.

Висновки

Вдалося розкрити причини виникнення механізму резервного копіювання як методу захисту даних, його сутність. Описано види та методи резервного копіювання. Проведено дослідження даних методів і на основі сукупності даних було обрано оптимальний варіант.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Франик В.М. Резервне копіювання даних / DOI 10.31392/NPU-nc.series2.2018.20(27).10
2. Backup and migrate Kubernetes resources and persistent volumes - [Електронний ресурс] – Режим доступу до ресурсу: <https://velero.io/blog/velero-1.5-for-and-bycommunity/>
3. Системні бази даних [Електронний ресурс] – Режим доступу: [https://msdn.microsoft.com/ru-ru/library/ms178028\(v=sql.90\).aspx](https://msdn.microsoft.com/ru-ru/library/ms178028(v=sql.90).aspx) (дата звернення 25.05.2022)
4. Ніконова А., Лесна Н.. Дослідження ефективності методів і моделей резервного копіювання та післяаварійного відновлення даних у SAP Hybris Commerce. International Electronic Scientific Journal «Science Online», 2020
5. Бондарь А. Microsoft SQL Server 2014, 2015. – 592с
6. Storage Networking Industry Association (SNIA). A Dictionary of Storage Networking Terminology — 2018. — Режим доступу: <http://www.snia.org/education/dictionary/>. (дата звернення 20.05.2022)

П'ятак Руслан Олегович - студент Кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: 20012006ruslan@gmail.com

Войтович Олеся Петрівна - к.т.н., доцент, професор кафедри захисту інформації. Вінницький національний технічний університет, м. Вінниця, email: voytovych.op@gmail.com.

Piatak Ruslan Olegovich - student of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: 20012006ruslan@gmail.com

Voytovych Olesya Petrivna - Ph.D., Associate professor of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: voytovych.op@gmail.com