мінімальними ризиками бути скомпрометованою, оскільки відтворювач інформації є безпосередньою частиною даної підсистеми, а дані після монтування віртуального диску не зберігаються в відкритому вигляді в файловій системі.

Література

1. Класифікація засобів модульної взаємодії між клієнтом і сервером / Ю. В. Морозов, І. І. Пастернак // Вісн. Нац. ун-ту "Львів. політехніка". – 2012. – № 717. – С. 108-112. – Бібліогр.: 10 назв. – укр;

2. Мережні інтерфейси рівня клієнт-сервер / Ю. Морозов, І. Пастернак // Вісн. Нац. ун-ту "Львів. політехніка". – 2012. – № 743. – С. 121-130. – Бібліогр.: 16 назв. – укр;

3. Морозов Ю.В., Сокіл В.М. Цифрові сертифікати – основа системі ідентифікації в комп'ютерних мережах // Вісник Національного університету «Львівська Політехніка»: «Комп'ютерні системи та мережі». 2002. – № 463. – С. 62–65;

4. В. О. Кононова, О. В. Харкянен, С. В. Грибков Оцінка засобів захисту інформаційних ресурсів. // Вісник Національного університету «Львівська Політехніка»: «Комп'ютерні системи та мережі» 2015р.;

5. Rubens, Paul (October 13, 2014). "VeraCrypt a Worthy TrueCrypt Alternative". eSecurity Planet. Quinstreet Enterprise. Archived from the original on December 3, 2018.

Д. Горошко

Науковий керівник – д.т.н., проф. А. Й. Наконечний

АНАЛІЗ СИСТЕМ ДІАГНОСТУВАННЯ ДВИГУНІВ АВТОМОБІЛІВ НА ОСНОВІ ОЦІНКИ ВЗАЄМНИХ ХАРАКТЕРИСТИК ЇХ КОМПОНЕНТІВ

З різким збільшенням кількості автомобілів в останні десятиліття постає проблема підвищення показни- ків експлуатаційної надійності та визначення залишкового ресурсу їх вузлів, найскладнішим з яких в плані технічного виконання є двигун. Тому вирішення даної проблему напряму пов'язане з вибором ефективного методу діагностування двигунів автомобілів, застосування якого буде доцільним впродовж усього їх життєвого циклу: від проектування до технічного огляду.

Сьогодні методи діагностування автомобілів та механізмів вивчають у наступних напрямках:

- діагностування за керуючими сигналам
- за допомогою віброакустичних сигналів

- за результатами аналізу випускних газів
- аналіз концентрації продуктів зносу в мастильних матеріалах
- осцилографічне діагностування

Діагностування на основі аналізу віброакустичних сигналів є високоперспективним, оскільки дозволяє точно визначати несправності у випадках, коли інші методи є малоефективними. Зокрема, цей метод розширює можливості виявлення дефектів на ранніх стадіях їх розвитку і прогнозування залишкового ресурсу двигуна, а також підлягає автоматизації з відносно невеликими затратами.

В основному для математичних методів аналізу віброакустичних застосовують швидке перетворення Фур'є, фазо-циклічний аналіз або аналіз спектру низькочастотних сигналів. Однак використання даних методів для аналізу віброакустичних сигналів не можна вважати найбільш ефективними інструментами, оскільки такі типи сигналів є нестаціонарними та складається з багатьох компонентів. Оскільки сигнали елементів двигуна автомобіля, отримані під час процесу діагностування, відзначаються певною нестаціонарністю, використання взаємної обробки таких сигналів на інтервалі спостереження може значно покращити коефіцієнт передачі всієї системи обробки сигналів і дозволить виявляти наявність залежності між ними.

Використання вейвлет аналізу сигналів для вищезгаданих областей в багатьох випадках є дуже ефективним. Подання обох сигналів (опорного і досліджуваного) у вейвлет-області дозволяє суттєво збільшити інформацію про аналізовані сигнали, а обчислення їх взаємних залежностей дає додаткову інформацію, яка є корисною при виявленні дефектів та несправностей.

З огляду на можливості даного математичного інструменту доцільним є використання взаємного вейвлет-перетворення для вхідних сигналів, отриманих за допомогою віброперетворювачів з елемента двигуна, який обрано як опорний, та з інших досліджуваних елементів.

Враховуючи висновки, отримані в результаті наведеного аналізу, запропоновано алгоритм діагностування двигуна автомобіля на базі оцінки взаємних характеристик його компонентів. В його основі лежить порівняння результатів взаємного вейвлет-перетворення часочастотних характеристик вібрації опорного та залежних від нього компонентів еталонного і діагностованого двигунів. За результатами аналізу визначається ступінь розходження отриманих взаємних характеристик, локалізується імовірний дефект і визначається його причина.

Висновок. Таким чином, в процесі дослідження порівняно ефективність методів діагностування ДВЗ та обрано віброакустичний як

найбільш перспективний. Крім того, обґрунтовано доцільність використання взаємного вейвлет-перетворення для математичного методу обробки сигналів для даного методу. Запропоновано алгоритм діагностування роботи двигунів автомобілів на основі оцінки взаємних характеристик їх компонентів та розроблено його функціональну схему.

М. Дьоміна
Науковий керівник – д.т.н., проф. В. С. Глухов

ПЕРЕВІРКА РЕАЛІЗАЦІЇ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ «КАЛИНА» ЗА ДОПОМОГОЮ ТЕСТОВИХ ПРИКЛАДІВ

Користувачам глобальних і локальних мереж потрібні засоби захисту інформації, що здатні зберегти конфіденційність, цілісність і доступність. Криптографічний захист цілком відповідає цим вимогам. Одним з способів захисту є блоковий шифр "Калина".

Калина (ДСТУ 7624:2014) – це сучасний новий український стандарт, який підтримує розмір блоку і довжину ключа шифрування 128, 256 і 512 біт, забезпечуючи нормальний, високий та надвисокий рівень стійкості (єдиний у світі стандарт блокового шифрування, що підтримує 512-бітові симетричні ключі). Основні параметри шифру, такі як довжина ключа k і блоку даних l, кількість раундів t та кількість стовпців матриці стану c представлені в табл. 1

Таблиця 1

Довжина блоку (l)	Довжина ключа (k)	Кількість раундів (t)	К-сть стовпців матриці стану (c)
128	128	10	2
256	256	14	4
512	512	18	8

Отже, **актуальною є задача** забезпечення надійного захисту даних за допомогою криптографічного захисту, а саме за допомогою блокового шифру «Калина».

У роботі розглянуто методику перевірки правильності програмної реалізації блокового симетричного криптографічного перетворення: