

Окрім зручності та простоти використання розробленої програми ще одним явною перевагою є створений алгоритм виконання роботи. Цей алгоритм оптимізує роботи пристрою завдяки його роботі не по периметру, а по вектору. Цей алгоритм забезпечує зменшення часу виконання завдання, чітко виділяє контури та переходи та оптимально використовує роботу лазера, що призводить до меншого зношення лазера, та запобігає перегріванню.

Висновок: У даній роботі проведено аналіз сучасного програмного забезпечення, для станків/граверів з ЧПК. Зроблено порівняння ПЗ, виявлено їх переваги та недоліки. Також було зроблено замітки по цих програмах. Після обґрунтування було створено висновки, та встановлено, що саме потрібно для розробки зручного та якісного ПЗ. Оскільки головною ідеєю для створення даного програмного забезпечення було зручність та простота використання, було створено перелік необхідних функцій, а також розроблено графічний інтерфейс програми.

1. <https://mirstankov.com/uk/yak-ce-pracyuye-chpu/>
2. <https://mirstankov.com/uk/catalog/nastolnyj-lazernyj-graver-msl4040-nezamenimyj-pomoshhnik-2/>
3. <https://prom.ua/p780861960-uluchshenyj-lazernyj-graver.html>

О. Мусянович

Науковий керівник – к.т.н., доц. Ю. В. Морозов

ПІДСИСТЕМА ЗАХИСТУ МУЛЬТИМЕДІЙНОЇ ІНФОРМАЦІЇ НА ВЕБ-САЙТІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ДИСКІВ

Завдяки безперервному розвитку технологій, зростає частота нелегального використання мультимедійної інформації і, в наслідок чого, виникає необхідність посилення захисту даної інформації. Сучасні програмні засоби захисту, не завжди справляються з цим завданням, оскільки після розшифрування файлів, вони передають дані в вихідному вигляді стороннім програмам для відтворення інформації. Загальним недоліком такого підходу є те, що система захисту не завжди може бути впевнена в програмі, яка відтворюватиме розшифровану інформацію.

Отже, **актуальною є задача** розробка системи захисту мультимедійної інформації в поєднанні з відтворювачем даної інформації.

У роботі розглянуто розв'язок цієї задачі, за допомогою розробки підсистеми, на базі клієнт-серверної архітектури, що складається з

шифратора, дешифратора та веб-сервісу, що їх поєднує. Цей підхід повинен суттєво зменшити можливість отримання зашифрованих даних в доступному для відтворення форматі.

Обмеження доступу та забезпечення шифрування інформації було вирішено реалізовувати на базі технології віртуальних дисків VeraCrypt. Дана технологія дозволяє на льоту виконувати шифрування файлів та дисків та створювати віртуальні зашифровані диски [5]. Особливістю обраної технології є те що, по-замовчуванню, після монтування диску як окремого розділу, усі дані представляються в вихідному форматі. Тому, було вирішено виконувати монтування диску не як окремого розділу, а як своєрідну директорію, прямий доступ до файлів з якої буде закритий для загалу, а надаватиметься він через реалізований програмний інтерфейс. Для цього розробляється драйвер, який матиме можливість створити зашифрований диск з розміщеними в ньому необхідними файлами та відтворити файли з їх дешифруванням в режимі реального часу. Після розшифрування даних драйвер передаватиме їх програмі-відтворювачу, яка є частиною розробленого клієнтського додатку.

Для організації передачі файлів та доступу до них у вигляді ключів розробляється Веб-сервіс, який забезпечуватиме збереження та передачу дисків, авторизацію та автентифікацію користувачів Веб-сайту [2]. Веб-сервіс створюється засобами мови PHP з використанням бібліотеки Laravel Passport, яка має реалізовані методи авторизації та автентифікації.

Оскільки, диск буде зашифровано, щоб його розшифрувати, необхідні ключі. Протоколом обміну ключів було обрано протокол Diffie-Hellman [3], а для шифрування файлів віртуальних дисків було обрано PGP. Платформою для розробки клієнтських аплікацій було обрано Xamarin.

Для того щоб передати Веб-сервісу зашифровану інформацію її потрібно отримати з внутрішнього сховища пристрою. Користувачу достатньо обрати необхідні файли, а програма, в свою чергу, виконає всі необхідні маніпуляції з ними. Після завершення процедури шифрування віртуального диску, він надсилається на сервер, звідки його можна отримати, маючи необхідний доступ [1]. Щоб переглянути зашифровану інформацію необхідно авторизуватись і програма автоматично завантажить ключі, щоб розшифрувати файл віртуального диску та, безпосередньо, сам диск. Після розшифрування та монтування диску, користувачу будуть доступні необхідні файли в режимі читання через відтворювач, який є частиною даної підсистеми.

Висновок: Розроблена підсистема захисту представила можливість збереження, передачі та відтворення мультимедійної інформації з

мінімальними ризиками бути скомпрометованою, оскільки відтворювач інформації є безпосередньою частиною даної підсистеми, а дані після монтування віртуального диску не зберігаються в відкритому вигляді в файлової 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 системи 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 показників експлуатаційної надійності та визначення залишкового ресурсу їх вузлів, найскладнішим з яких в плані технічного виконання є двигун. Тому вирішення даної проблеми 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