УДК 004.4
Вітоль І. – ст. гр. СНм – 51
Тернопільський національний технічний університет імені Івана Пулюя

СИСТЕМА ЗАХИСТУ ВИКОНУВАНИХ ФАЙЛІВ ВІД КОПІЮВАННЯ ІЗ ВИКОРИСТАННЯМ WEB-ТЕХНОЛОГІЙ

Науковий керівник: д.т.н., професор Приймак М.В.

Захист від копіювання – одне із найбільш важливіших і складних завдань для розробників програмного забезпечення. Разом із стрімким розвитком всесвітньої мережі Інтернет, збільшується розповсюдження не ліцензованих та не дозволених авторами копій програмного забезпечення. Основним завданням таких систем є забезпечення виконання розробленого програмного продукту лише на конкретному, ліцензованому ПК чи іншому кінцевому пристрої. Програмна система має використовувати унікальну інформацію кінцевого пристрою, до якої можна було б прив'язати програмний продукт. При цьому, автор програмного забезпечення повинен дізнаватись унікальні дані клієнтського пристрою, а далі самостійно розробити алгоритми захисту із використанням отриманих даних. Автоматизація наведеного процесу і розроблення окремої програмної системи для захисту інших програмних продуктів, звільняє більшість розробників програмного забезпечення від побудови власної системи захисту від нелегального використання, та дозволяє їм зосередитись на більш вагомих для їхньої задачі проблемах.

Для створення такої програмної системи, було проведено аналіз проблематики задачі. В результаті розгляду специфіки задачі визначено дві її базові проблеми. Перша складність полягає в створенні зручної системи доставки кінцевого, захищеного продукту клієнтам. Вирішенням цієї проблеми є розробка Web-сайту, який би взаємодіяв із системою захисту на сервері. Зручний інтерфейс дозволить завантажити автору свій програмний продукт, та отримати URL доступу для його клієнтів, які під час завантаження продукту нададуть серверу унікальні дані свого пристрою. Друга проблема полягає у прийнятній швидкості роботи системи захисту, яка залежить від вибраних алгоритмів захисту та рівня взаємодії з користувачем.

Після визначення основних проблем задачі, проведено порівняння ефективності хеш-функцій та алгоритмів шифрування. В результаті обрано хеш-функцію MD5 та симетричний вид алгоритму шифрування. Алгоритм MD5 та симетричне кодування забезпечують найкращу швидкодію шифрування / дешифрування, як на стороні клієнта, так і на стороні сервера. Незважаючи на імовірність виникнення колізій в результуючій хеш-сумі, рівень безпеки компенсується довжиною ключа шифрування.

Для початку було сформовано список завдань для підпрограм, які будуть необхідні для формування унікального ключа системи, шифрування програмного продукту та його виконанні на цільовій системі. Наступним кроком стала програмна реалізація сформованих завдань для кожної із підпрограм. Також було розроблено Web-сайт, в роботу якого інтегровано підпрограму шифрування продукту в залежності від отриманої інформації клієнта.

Підсумовуючи, необхідно сказати, що використання розробленої програмної системи, на відміну від існуючих аналогів, полегшує роботу як самих авторів програмнго забезпечення, так і їх клієнтів. Система захисту виконуваних файлів від копіювання виконує всі операції по шифруванню, дешифруванню та завантаженню програмних продуктів у віртуальній пам'яті, та містить надійні алгоритми контролю цілісності та захисту від зовнішніх втручань.