– розрахунок автоматизований частково, тобто є програма, але на певному етапі розрахунку потрібне втручання людини, наприклад для уведення значень із діаграм або таблиць;

– програма застаріла настільки, що її неможливо запустити на сучасному комп'ютері;

– програма має незручний інтерфейс;

– програма не дозволяє зберегти вихідні дані для повторного використання й/або результати розрахунку в електронному виді;

– програма вимагає доробки, але через відсутність кваліфікованого фахівця їй користуються "як є";

– неможливість або труднощі наступності досвіду роботи із програмою молодими фахівцями.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи реінжинірингу та рефакторингу програмного коду до платформи .NET, є актуальною задачею.

Список літератури

1. Фаулер М., Бек К., Брант Д., Робертс Д., Апдайк У. Рефакторинг: улучшение существующего кода = Refactoring: Improving the Design of Existing Code (2000). – Спб: Символ-Плюс, 2009. – 432 с.
2. Скотт В. Эмблер, Прамодкумар Дж. Садаладж. Рефакторинг баз данных: эволюционное проектирование. – М.: «Вильямс», 2007. – 368 с.
3. Джошуа Кериевски Рефакторинг с использованием шаблонов. – Вильямс, 2008. – 400 с.

УДК 004.4

І.С. Кучеренко
Науковий керівник – Конопліцька О.К., асистент
Кіровоградський національний технічний університет

Програмне забезпечення системи запобігання аналізу та модифікації програмних продуктів

Система запобігання аналізу та модифікації програмних продуктів базується на використанні обфускації. Обфускація (від англ. to obfuscate – спантеличувати, заплутувати) – це приведення коду, що виконується, або вихідного тексту програми до виду, що зберігає її функціональність, але утрудняє розуміння, аналіз алгоритмів роботи, а також модифікацію при декомпіляції.

Мета обфускації:

– Продемонструвати неочевидні можливості мови й кваліфікацію програміста (якщо заплутування виробляється не інструментальними засобами, а вручну).

– Оптимізувати програму для зменшення розміру коду й прискорення роботи.

– Ускладнити декомпіляцію/налагодження й вивчення шкідливих програм, щоб запобігти виявленню їхньої шкідливої функціональності.

– Утруднити декомпіляцію пропрієтарных програм, щоб запобігти зворотній розробці або обхід систем перевірки ліцензій і DRM.

– Порушити авторські права програмістів і сховати авторство.

У пошуковій оптимізації обфускація javascript-файлів використовувалася для заплутування пошукових ботів при декомпіляції коду, нерідко в облудних цілях. На сьогоднішній день це неактуально.

Отже, розробка програмного забезпечення системи запобігання аналізу та модифікації програмних продуктів є актуальною задачею.

Список літератури

1. Альфред В. Ахо, Моника С. Лам, Рави Сети, Джеффри Д. Ульман. Компиляторы: принципы, технологии, инструментарий. – М.: Вильямс, 2008. – С. 719-760.
2. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vedhan S., Yang K. On the (Im)possibility of obfuscating programs // Lecture Notes in Computer Science, v. 2139, 2001, p. 1-18.
3. Лифшиц Ю. М. Запутывание (обфускация) программ. Обзор. - СПб.: СПб.отд.Мат.инст. им.В.А.Стеклова РАН, 2004. http://logic.pdmi.ras.ru/~yura/of/survey1.pdf.

УДК 004.4

С.Д. Сороколат
Науковий керівник – Приходькіна А.І., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0

Допомогти користувачеві зберегти, а головне – легко перенести великі обсяги контенту, покликані сучасні переносні жорсткі диски з використанням USB 3.0.

Інтерфейс USB 3.0 стає усе актуальнішим з кожним днем. Допомагають йому в цьому програмні системи та мультимедійні файли, розміри яких постійно збільшуються. Якщо торкнутися питання мультимедійних даних, то знімки, як правило, займають ще більше місця, не говорячи вже про все більше поширення RAW-формату. Не відстає й відеоконтент: наприклад, на початку квітня на українському ринку з'явився перший Quad-HD Ultra High Definition-телевізор з розрішенням 3840 x 2160 крапок. Допомогти користувачеві зберегти, а головне – легко перенести великі обсяги мультимедійного контенту покликані сучасні переносні жорсткі диски USB 3.0.

Крім цього, як правило, зовнішні жорсткі диски інтерфейсу USB 3.0 доволі часто використовуються як сховища даних, або резервні копії актуальних даних.

Але при цьому гостро стає проблема збереження даних на зовнішніх жорстких дисках інтерфейсу USB 3.0, зокрема збереження конфіденційних даних.

Проведені дослідження показали, що одним з найбільш перспективних напрямків управління даними з ціллю збереження конфіденційності інформації на зовнішніх носіях, зокрема на зовнішніх жорстких дисках інтерфейсу USB 3.0, є використання потокових шифрів.

Таким чином, розробка програмного забезпечення системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0 є актуальною задачею.

Список літератури

1. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учебное пособие / СПбГУТ. – СПб, 2000.
2. Жельников В. Криптография от папируса до компьютера. – М.:ABF, 1996.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
4. Коржик В.И., Кушнир Д.В., Морозов К.Г. Основы защиты информации в компьютерных системах: методические указания к лабораторным работам / СПбГУТ. – СПб, 1999.