ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ НАВЧАННЯ
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ

ЗБІРНИК МАТЕРІАЛІВ І ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ МОЛОДИХ УЧЕНИХ «НАУКОВА МОЛОДЬ-2013»

12 грудня 2013 року
Київ

УДК 044 : [001+37] : 005.745 (082)
ББК 72с51я431+74с51я431

Збірник матеріалів І Всеукраїнської науково-практичної конференції молодих учених «Наукова молодь-2013» / за заг. ред. проф. Бикова В.Ю. та Спіріна О.М. – К.: ІТЗН НАПН України, 2014. – 190 с.

Рецензенти:
Запорожченко Ю.Г. – к.пед.н., завідувач відділу інформатизації навчально-виховних закладів ІТЗН НАПН України;
Литвинова С.Г. – к.пед.н., старший науковий співробітник відділу інформатизації навчально-виховних закладів ІТЗН НАПН України;
Яцишин А.В. – к.пед.н., с.н.с., провідний науковий співробітник відділу комп'ютерно орієнтованих систем навчання і досліджень ІТЗН НАПН України.

Рекомендовано до друку Вченою радою Інституту інформаційних технологій і засобів навчання НАПН України протокол № 2 від 27 лютого 2014 року.

Збірник матеріалів містить наукові статті та тези доповідей поданих на І Всеукраїнську науково-практичну конференцію молодих учених «Наукова молодь-2013», яка відбулася 12 грудня 2013 року. Під час роботи конференції розглянуто низку проблем, що пов'язані з впровадженням і використанням інформаційно-комунікаційних технологій в освіті та наукових дослідженнях.

Збірник адресовано науковим, науково-педагогічним працівникам, аспірантам, докторантам, студентам вищих навчальних закладів і всім хто цікавиться проблемами інформатизації освіти.

УДК 378:004.056.55

Загацька Н.О., аспірант,
Житомирський державний університет
імені Івана Франка, м. Житомир

КРИПТОГРАФІЧНІ МОЖЛИВОСТІ MICROSOFT WINDOWS

У зв'язку із глобальним розвитком інформаційних технологій забезпечення конфіденційності, цілісності, достовірності інформаційних ресурсів є одним із найважливіших питань сьогодення. Найбільш надійний та поширений в наші дні метод захисту даних від несанкціонованого доступу – криптографічний. Цей метод передбачає перетворення повідомлення шляхом шифрування його змісту. Тому у процесі підготовки фахівця з інформатики варто приділяти увагу не лише формуванню у студентів знань щодо основних принципів захисту інформації, а також формуванню у них умінь та навичок з практичного використання криптографічних методів у комп'ютерних системах.

В останні роки область застосування криптографії значно розширилася. Її стали повсякденно використовувати приватні особи, державні організацій, комерційні

фірми. Зокрема, операційні системи сімейства Microsoft Windows надають широкі можливості для використання криптографії. Студенти можуть застосовувати криптографічні засоби Windows у своїх проектах, при цьому, не витрачаючи час на програмну реалізацію складних алгоритмів шифрування. Одним із таких засобів являється **CryptoAPI** (Crypto Application Programming Interface) – криптографічний інтерфейс прикладного програмування, що визначає порядок звернення прикладних програм до бібліотеки функцій, які дозволяють здійснювати криптографічні перетворення. Оскільки різні додатки потребують різні засоби шифрування, крім того, слід врахувати можливість появи в майбутньому нових криптографічних алгоритмів, тому була обрана структура інтерфейсу, яка б дозволяла використовувати для роботи з криптографічними функціями вбудовані компоненти, які називають криптографічними провайдерами.

Криптопровайдер або **CSP** (Cryptographic Service Provider) – це спеціалізоване програмне забезпечення фірми Microsoft, призначене для вирішення криптографічних завдань в сімействі операційних систем Windows. Криптопровайдер являє собою незалежну динамічну бібліотеку (DLL) криптографічних алгоритмів, доступних програмістам за допомогою інтерфейсу CryptoAPI. При взаємодії з будь-яким криптопровайдером додатки викликають функції CryptoAPI, які звертаються до системних бібліотек операційної системи, одна з яких фільтрує виклики та передає їх далі відповідним функціям криптопровайдера (див. рис. 1).

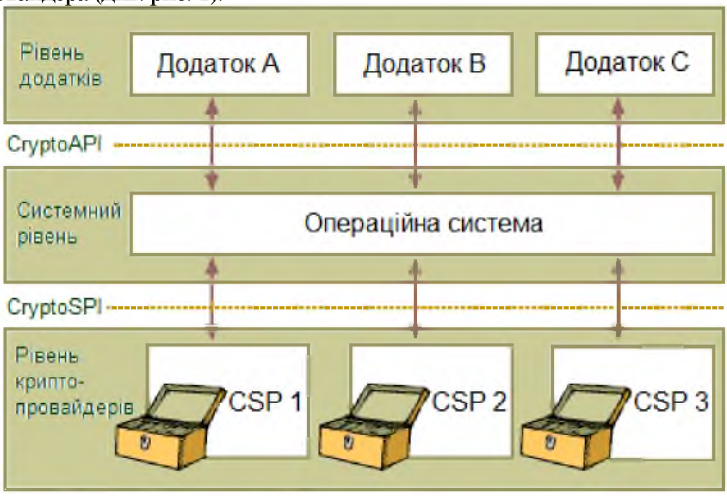

Рис.1. Схема взаємодії додатків із криптопровайдерами

Функції CSP програміст може викликати з програми, що написана на мові програмування Visual Basic, Object Pascal, C++, Java або Delphi. Існує велика кількість криптопровайдерів для операційних систем сімейства Windows, створених як самою Microsoft, так і іншими розробниками. Можна переходити від одного криптопровайдера до іншого з мінімальними змінами вихідного коду, так як інтерфейс (CryptoAPI) не змінюється. Основний провайдер Microsoft має назву

Microsoft Base Cryptographic Provider. Саме з ним за замовчуванням будуть взаємодіяти всі програми. Криптопровайдер із підтримкою CryptoAPI забезпечує виконання таких основних функцій:

– управління криптопровайдерами та їх контекстами [1, с. 32];

– створення, конфігурування, знищення криптографічних ключів, а також обмін ключами [1, с. 33];

– функції, що реалізують операції шифрування, дешифрування і обчислення імітовставки [1, с. 33];

– обчислення значень хеш-функцій, а також створення і перевірки цифрового підпису повідомлень [1, с. 33].

Реалізуються криптопровайдери зазвичай у вигляді однієї або декількох динамічних бібліотек. Кожен криптопровайдер характеризується власним ім'ям та типом [2]. Криптопровайдери відрізняються один від одного:

– складом функцій (наприклад, деякі криптопровайдери не виконують шифрування даних, обмежуючись створенням і перевіркою електронних цифрових підписів);

– вимогами до обладнання (спеціалізовані криптопровайдери можуть вимагати пристрої для роботи зі смарт-картами для виконання аутентифікації користувача);

– алгоритмами, що здійснюють базові дії (створення ключів, хешування тощо).

Під час виконання лабораторних робот студентам можна запропонувати створити програму, що виводить відомості про встановлені в операційній системі криптопровайдери та список криптоалгоритмів, які вони підтримують. Використання функції Microsoft CryptoAPI буде доцільним на практичних заняттях під час реалізації алгоритмів шифрування, створення електронного цифрового підпису файлів тощо.

Отже, CryptoAPI надає широкий набір криптографічних можливостей, які дозволяють організувати власну систему захисту даних без використання сторонніх засобів, що може значно підвищити рівень навіть досвідченого фахівця з інформатики.

Список використаних джерел:

1. Щербаков Л. Ю. Прикладная криптография. Использование и синтез криптографических интерфейсов / Л. Ю. Щербаков, А. В. Домашев. – М.: Издательско-торговый дом «Русская Редакция», 2003. – 416 с.

2. Виноградов К. Delphi и Windows API для защиты секретов (части 1,2,3) [Електронний ресурс] / К. Виноградов, Л. Виноградова. – Режим доступу: http://citforum.ru/security/articles/defense. – 07.12.2013.

НАУКОВЕ ВИДАННЯ

Матеріали надруковані в авторській редакції. За достовірність фактів, посилань, стилістичне та орфографічне оформлення відповідальність несуть автори публікацій та їх наукові керівники.

Відповідальні за випуск:
Яцищин А.В., Запорожченко Ю.Г., Литвинова С.Г.

Комп'ютерна верстка: Коваленко В.В.