РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ШИФРУВАННЯ ДАНИХ СИМЕТРИЧНИМ КРИПТОАЛГОРИТМОМ

Ткаченко О.С.
Науковий керівник – к.т.н., доц. Шаповалов С.О.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки 14, кафедра МІРЕС, т. 70-21-587
email: d_res@nure.ua

Information security is one of the eternal problems. The current history of mankind ways to solve this problem by determining the level of technology development. In today's information society, technology plays the role of an activator of this problem – computer crimes have become a characteristic feature of today.

Among the causes of computer crimes and related thefts of information are the following: Rapid transition from traditional paper storage technology and transmission of information to electronic while lagging information security technology recorded on the machine media; Widespread use of local area networks, creation of global networks and expansion of access to information resources; a permanent complication of the software, which causes a decrease in their reliability and an increase in the number of vulnerabilities in the Places.

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі: швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях; широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів; постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);

- вартість викрадених і скомпрометованих даних;
- витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо.

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Метою роботи було розробити програму, яка може зашифрувати будь-яку інформацію. В ході роботи була створена програма для захисту інформації на комп’ютері.

Для виконання роботи було проведено аналіз структури програмних засобів для шифрування інформації та задач які покладаються на метод шифрування. В ході роботи було розроблено код який може зашифрувати, а також розшифрувати будь-який файл.

Знаючи задачі та методи їх рішення був розроблений загальний алгоритм роботи програми для коректного вирішення поставленої задачі, на основі цього алгоритму була розроблена програма в середовищі Microsoft Visual Studio Рис. 1.

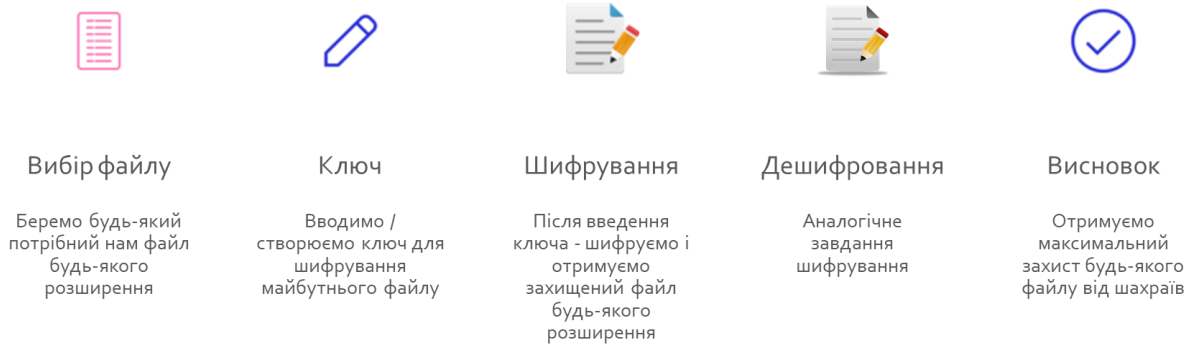

Рис. 1

Для перевірки коректності роботи та виявлення помилок виконання програми було використано вбудований засіб симуляції, в якому було перевірено функціонування блоків програми та правильності відображення виведених значень в залежності від встановлення вхідного коду.