УДК 004.41

Ю. Г. Даник, Ю. І. Дерпак

ПРОГРАМНИЙ КОМПЛЕКС ВІЗУАЛІЗАЦІЇ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У статті розглянуто питання захисту даних в інформаційно-комунікаційних системах та мережах від несанкціонованого доступу криптографічним алгоритмом. Виявлено й обґрунтовано необхідність створення та модернізації сучасних систем комплексного захисту інформації, визначено основоположне місце криптографічних методів у них за умови глобальної інформатизації. Також розглянуто криптоалгоритм Triple DES: його програмну реалізацію мовою програмування C# з максимальною візуалізацією процесів забезпечення конфіденційності даних при його використанні.

Постановка проблеми. Швидкий розвиток засобів обчислювальної техніки в умовах глобальної інформатизації відкрив небувалі можливості в питаннях автоматизації розумової праці і призвів до створення великої кількості різних автоматизованих інформаційних систем та систем управління, до виникнення інформаційних технологій.

Є вагомі підстави вважати, що заходи, яких вживають у даний час більшість організацій, не забезпечують необхідного рівня безпеки суб'єктів, що беруть участь у процесі інформаційної діяльності, і не здатні в необхідній мірі протистояти різного роду несанкціонованим діям з метою доступу до таємної інформації та дезорганізації роботи автоматизованих систем.

Беручи до уваги теперішній стан справ у сфері захисту інформаційно-комунікаційних систем та мереж (ІКСМ), неабияку увагу привертають до себе криптографічні алгоритми, методи та засоби забезпечення конфіденційності даних. Серед уже відомих симетричних алгоритмів шифрування знаходяться такі, як Lucifer, DES, 3DES, FEAL, IDEA, AES, RIJNDAEL та ін. Характерна особливість кожного з них – це відповідність алгоритму та ключа для двох зворотних процесів шифрування та розшифрування даних.

У даній статті описано структурну схему програмного комплексу криптографічного захисту інформаційних потоків в інформаційно-комунікаційній мережі (ІКМ) з візуалізацією процесів забезпечення конфіденційності даних та з реалізацією клієнт-серверної архітектури з використанням стандарту алгоритму шифрування даних 3DES та стеку протоколу TCP/IP транспортного рівня моделі OSI. Запропонований програмний комплекс розглядається як наочне приладдя для автоматизації процесу навчання, підвищення кількісних та якісних показників у знаннях студентів, які навчаються у вищих навчальних закладах (ВНЗ) за відповідними спеціальностями з галузі безпеки інформації.

Огляд останніх досліджень і публікацій. Вирішення проблем забезпечення конфіденційності даних (ЗКД) від несанкціонованого доступу (НСД) розглядалися в роботах В. І. Коржика, Ф. Г. Хісамова, Ю. С. Харіна та інших видатних вчених у відповідній галузі знань [2, 11]. Серед них слід було б відзначити такі технічні рішення, в яких пропонується використовувати комплексні системи захисту інформації,

обов'язковим елементом яких мають бути криптографічні методи забезпечення конфіденційності даних від НСД [1].

Ґрунтовну оцінку стійкості до криптоаналізу алгоритму шифрування DES дає Брюс Шнаєр. Він зауважує на доцільності вивчення та використання криптоалгоритмів, зокрема й 3DES, та інших симетричних блочних шифрів у незахищених інформаційно-комунікаційних системах та мережах для забезпечення конфіденційності даних в них [2]. Криптоалгоритм 3DES є модифікацією алгоритму DES, але з усуненими основними недоліками останнього. Програмних продуктів, які б реалізовували відображення процесів з даними при їх шифруванні та розшифруванні відповідним криптоалгоритмом та наочно відображали інваріантну складову їх можливого застосування, не існує. Тому відповідний програмний комплекс запропоновано саме для підготовки фахівців у сфері інформаційної безпеки з метою автоматизації і підвищення якісного та кількісного стану процесу навчання під час вивчення профільних з даного напрямку дисциплін у ВНЗ.

Недоліки, які були присутні в DES, були усунуті в 3DES таким чином: 1) розмір ключа збільшився із 56 до 168 бітів; 2) підвищена стійкість до лінійного криптоаналізу (лінійна атака − знаходження ключа для злому зашифрованих даних швидше, ніж послідовний перебір); 3) стійкість до диференційного криптоаналізу [4].

Метою статті є розробка програмного комплексу візуалізації процесів забезпечення конфіденційності даних в інформаційно-телекомунікаційних системах з клієнт-серверною архітектурою при використанні алгоритму симетричного шифрування 3DES. Запропонований програмний комплекс забезпечить наочність підходу до підготовки висококваліфікованих фахівців у сфері інформаційної безпеки під час вивчення профілюючих дисциплін, зростання якісних та кількісних показників процесу навчання: за той же самий час збільшуватиметься обсяг викладеного матеріалу, при цьому нічого не втрачаючи в якості його засвоєння, відбуватиметься автоматизація процесу навчання.

Виклад основного матеріалу дослідження. Симетричний криптоалгоритм 3DES – це один із симетричних криптоалгоритмів, оснований на так званій петлі (функції) Фейстеля (рис. 1), це фактично DES, застосований 3 рази підряд з довжиною ключа 168 біт і 24 біти контролю парності і вхідним блоком даних довжиною 64 біти (рис. 2) [3].

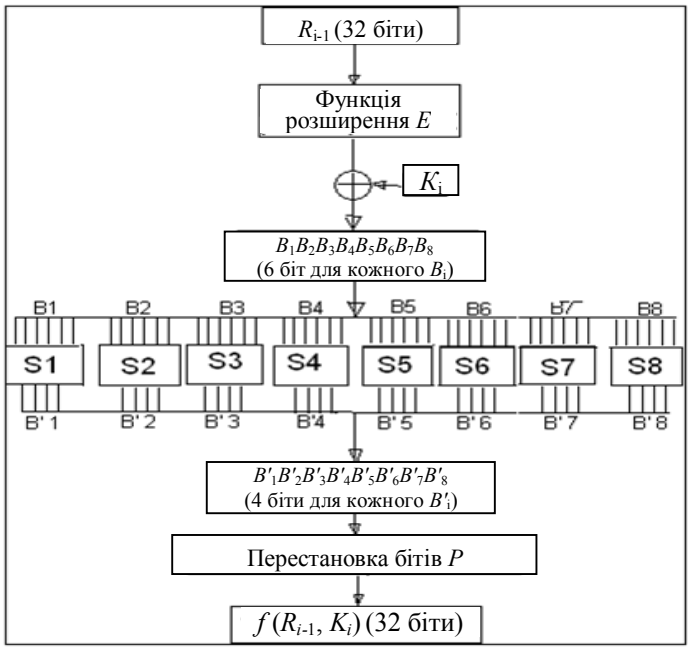

Рис. 1. Схема роботи функції Фейстеля

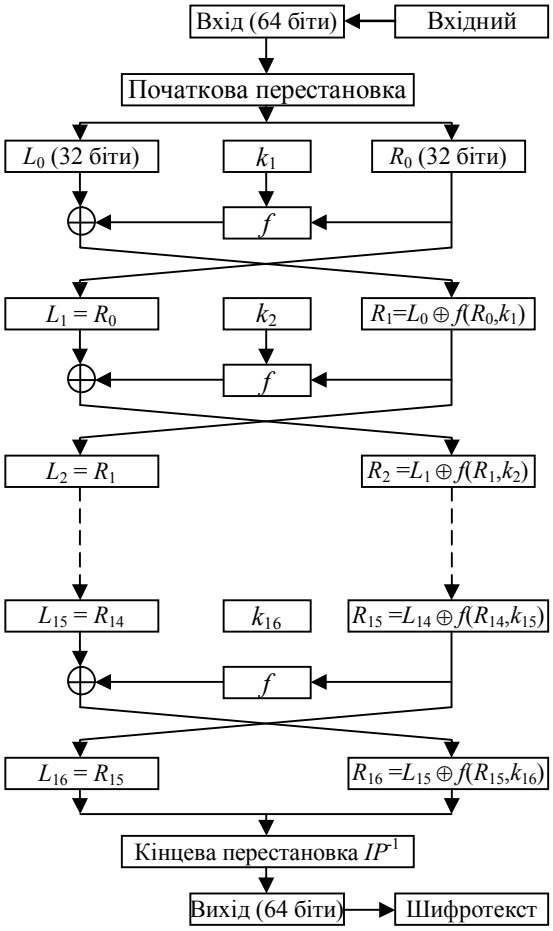

Рис. 2. Структурна схема шифрування даних в алгоритмі 3DES

Криптоалгоритм 3DES має в своєму арсеналі 48 раундів, які містять процеси перестановок (зі стискуванням та розширенням), підстановок, у тому числі і в нелінійних *S*-боксах, циклічних зсувів ключа, логічних операцій, таких як сумування за модулем два вхідної послідовності до раундового ключа (рис. 3) [5].

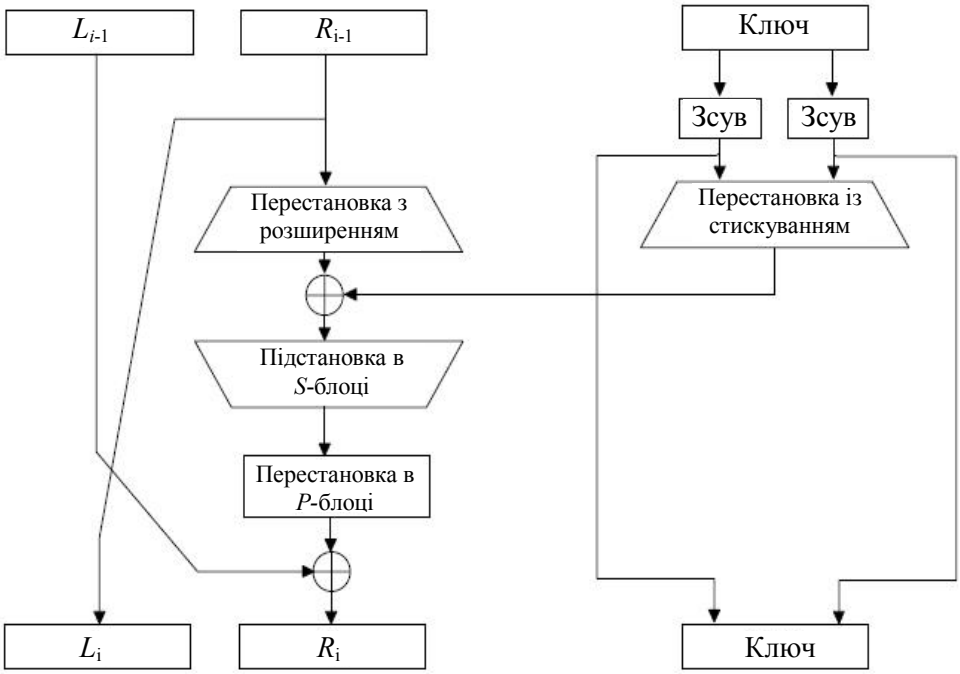

Рис. 3. Один із типових 48 раундів алгоритму шифрування даних 3DES

Відомі різні варіанти реалізацій криптоалгоритму, зокрема EEE, EDE, DED, але найвживанішим з-поміж них є EDE. Для нього кінцеві формули виведення шифротексту та відкритого тексту мають вигляд [5]:

1) шифрування:

$$C = E_{k_3}\left(E^{-1}_{k_2}\left(E_{k_1}(M)\right)\right);$$

2) розшифрування:

$$M = E^{-1}_{k_1}\left(E_{k_2}\left(E^{-1}_{k_3}(M)\right)\right).$$

При виконанні алгоритму 3DES ключі можна вибрати так:

k_1, k_2, k_3 незалежні;

k_1, k_2 незалежні, а $k_1 = k_3$;

$k_1 = k_2 = k_3$.

Типову систему захисту інформації доцільно відображати у вигляді взаємопов'язаних підсистем: криптографічного захисту; захисту від НСД; організаційно-правового захисту; управління системою захисту інформації; ідентифікації та аутентифікації; забезпечення мережевого зв'язку типу «клієнт-сервер».

Типова інформаційна система має структуру, що складається з таких компонентів: робоча станція, сервер застосувань, сервер баз даних (БД), система захисту даних. Структуру інформаційної системи можна зобразити таким чином (рис. 4) [8]:

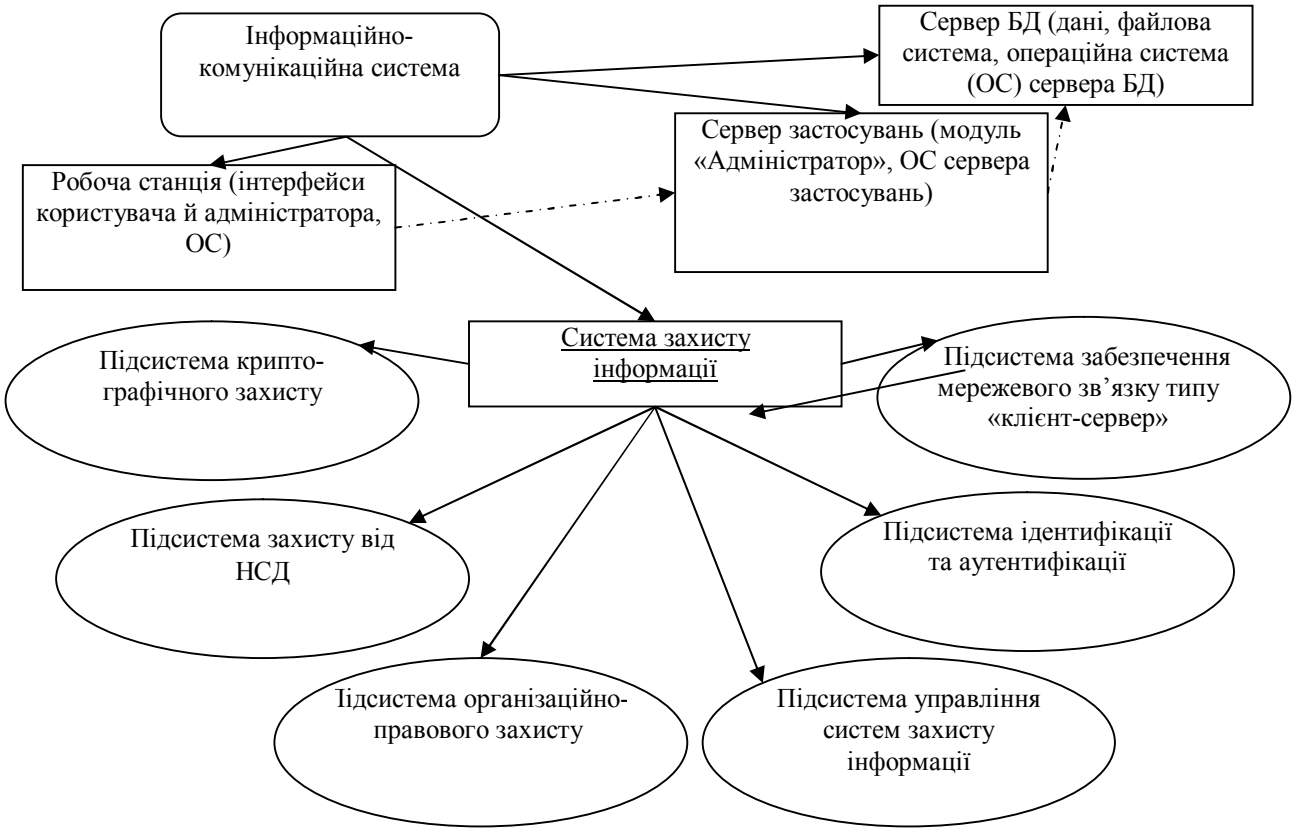

Рис. 4. Узагальнена структура інформаційної системи

Запропонований програмний комплекс належить до підсистеми криптографічного захисту і є лише одним з її складових, оскільки загалом підсистема криптографічного захисту займається не лише питанням конфіденційності, цілісності, достовірності даних, а також питанням унеможливлення відмови від авторства та ін.

У процесах аналізу і проектування систем криптографічного захисту інформації одним з основних засобів відображення структури компонентів систем є графічні моделі. Головними їх перевагами порівняно із словесними описами є простота і компактність, а також легкість сприйняття. Відповідно, запропонований програмний комплекс має структуру елементів, яка наведена на рис. 5 [10].

Рис. 5. Структура компонентів програмного комплексу забезпечення конфіденційності даних

Програмний комплекс складається з 5 компонентів (модулів), які забезпечують його функціонування.

Основною задачею Модуля 1 є робота з рядками в операційній пам'яті комп'ютера, тобто виконання їх шифрування та розшифрування, використовуючи певний, введений користувачем, ключ.

Основною задачею Модуля 2 є робота з текстовими файлами, тобто виконання їх шифрування та розшифрування, використовуючи секретний ключ, а також з можливістю збереження опрацьованих даних на постійному запам'ятовуючому пристрої (ПЗП) комп'ютера.

Основною задачею Модуля 3 (головний блок роботи майбутньої програми) є відображення (візуалізація) процесів забезпечення конфіденційності даних в ІКСМ стандартом криптографічного захисту Triple DES. Даний блок має вміщувати в собі, насамперед, ті основні методи і властивості, які наочно для рядового користувача зможуть охарактеризувати суть усіх процесів, які відбуваються з даними під час їх криптографічного перетворення криптоалгоритмом 3DES.

Модуль 4 є додатковим блоком до майбутньої проектованої програми. Даний блок міститиме лише короткий опис про роботу системи та функціональне забезпечення алгоритму криптографічного захисту даних 3DES.

Модуль 5 забезпечує обмін шифрованими повідомленнями між клієнтами за допомогою ресурсів сервера.

Статичну структуру проектованого програмного додатка зобразимо за допомогою діаграми класів (class diagram) засобами мови UML. Діаграма класів відображає взаємозв'язки між окремими об'єктами і проектованою системою, описує їхню внутрішню структуру і типи відносин, описує структурні взаємозв'язки логічної моделі системи, які не залежать або інваріантні від часу.

Діаграма класів проектованого додатка має такий вигляд (рис. 6):

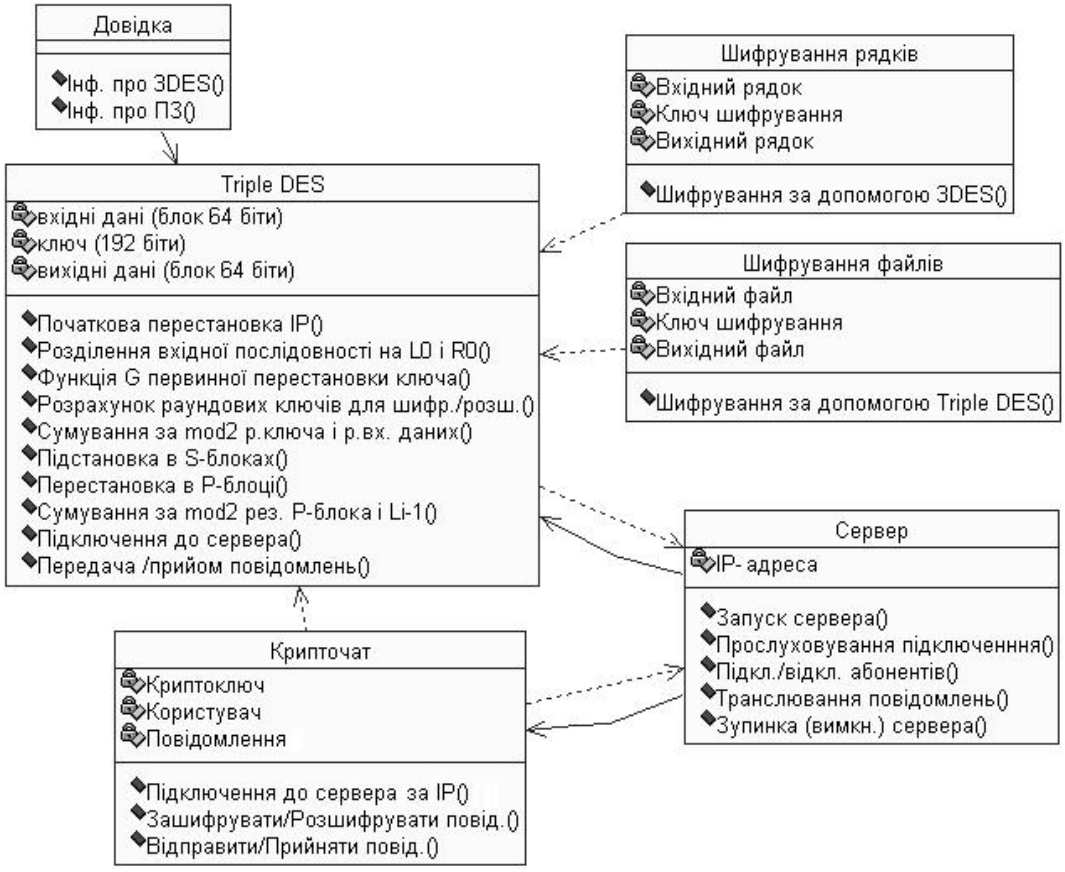

Рис. 6. Діаграма класів проектованого додатка засобами мови UML

Дана діаграма складається із шести класів:

клас «Triple DES»(клас, який відображає сутність усіх процесів шифрування та розшифрування даних при використанні алгоритму криптографічного захисту даних 3DES;

клас «Шифрування файлів», який знаходиться у відношенні «залежності» з класом «Triple DES» (відображає сутність процесів шифрування при роботі з текстовими файлами криптоалгоритмом 3DES);

клас «Шифрування рядків», який знаходиться у відношенні «залежності» з класом «Triple DES» (відображає сутність процесів шифрування при роботі з рядками криптоалгоритмом 3DES в оперативній пам'яті комп'ютера);

клас «Крипточат» знаходиться у відношенні «залежності» з класами «Triple DES» і «Сервер» (забезпечує обмін шифрованими повідомленнями);

клас «Сервер» знаходиться у відношенні «асоціації» з класами «Triple DES» та «Крипточат»;

клас «Довідка» знаходиться у відношенні «асоціації» з класом «Triple DES» (відображає основні довідкові матеріали щодо роботи криптоалгоритму 3DES і роботи з проектованим програмним забезпеченням (ПЗ)).

Засобом розробки пропонованого додатка забезпечення конфіденційності даних в ІКСМ було обрано мову об'єктно орієнтованого програмування C#.

Додаток містить 5 основних вікон (вікно відображення процесів забезпечення конфіденційності даних, вікно шифрування повідомлень, вікно шифрування файлів, вікно крипточата, вікно запуску серверного додатка та одного додаткового вікна довідки). Описувати та відображати всі вікна розробленого ПЗ недоцільно, слід зробити акцент лише на вікні візуалізації процесів забезпечення конфіденційності даних за допомогою криптоалгоритму 3DES та на вікні, яке реалізовує інваріанту складову можливого застосування розглянутого алгоритму в інформаційно-телекомунікаційних системах (ІТС) на базі крипточата (рис. 7–13).

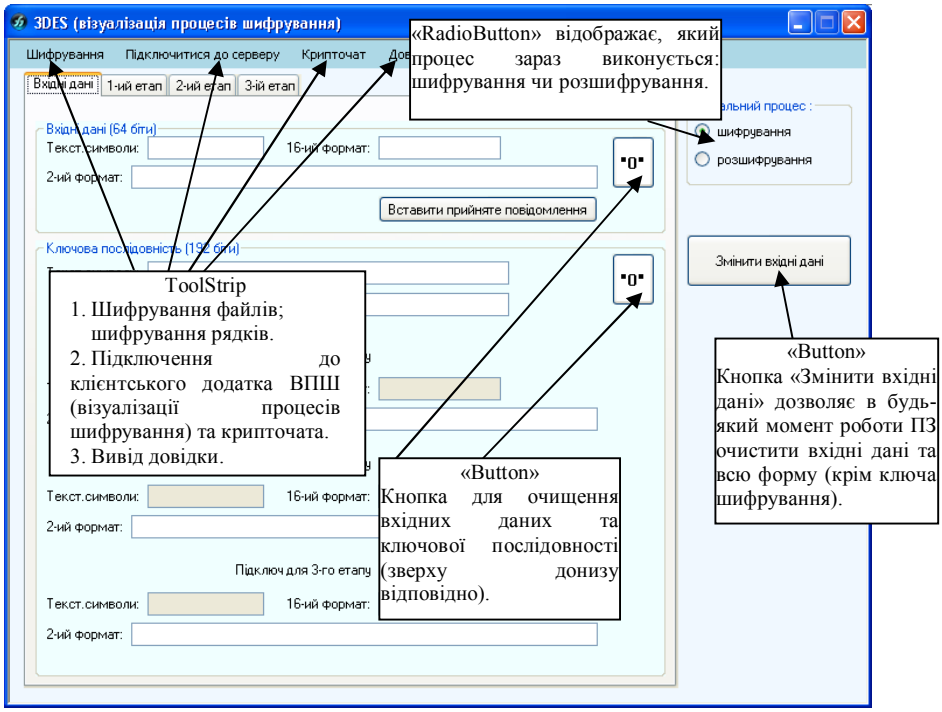

Рис. 7. Головне вікно програми (перша вкладка)

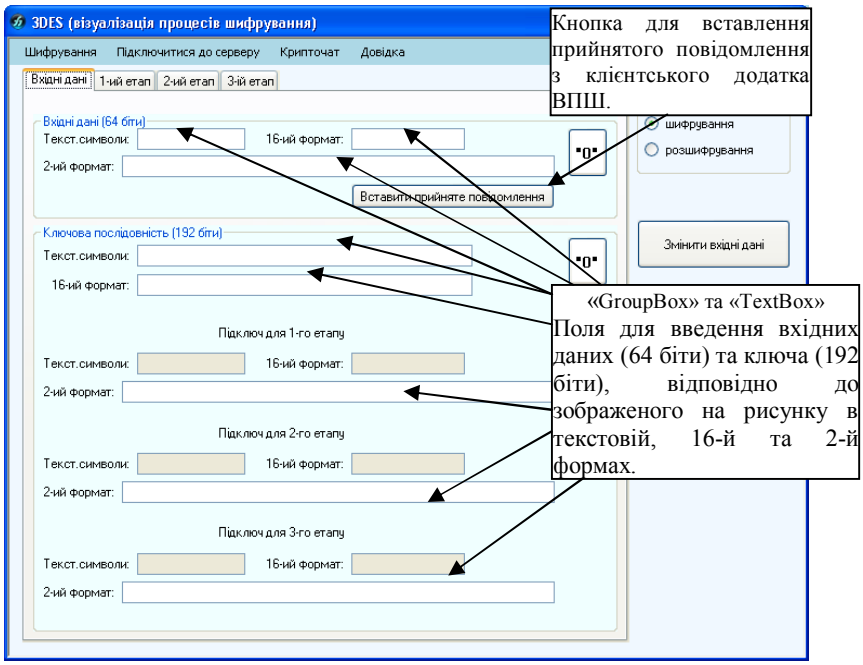

Рис. 8. Головне вікно програми (перша вкладка)

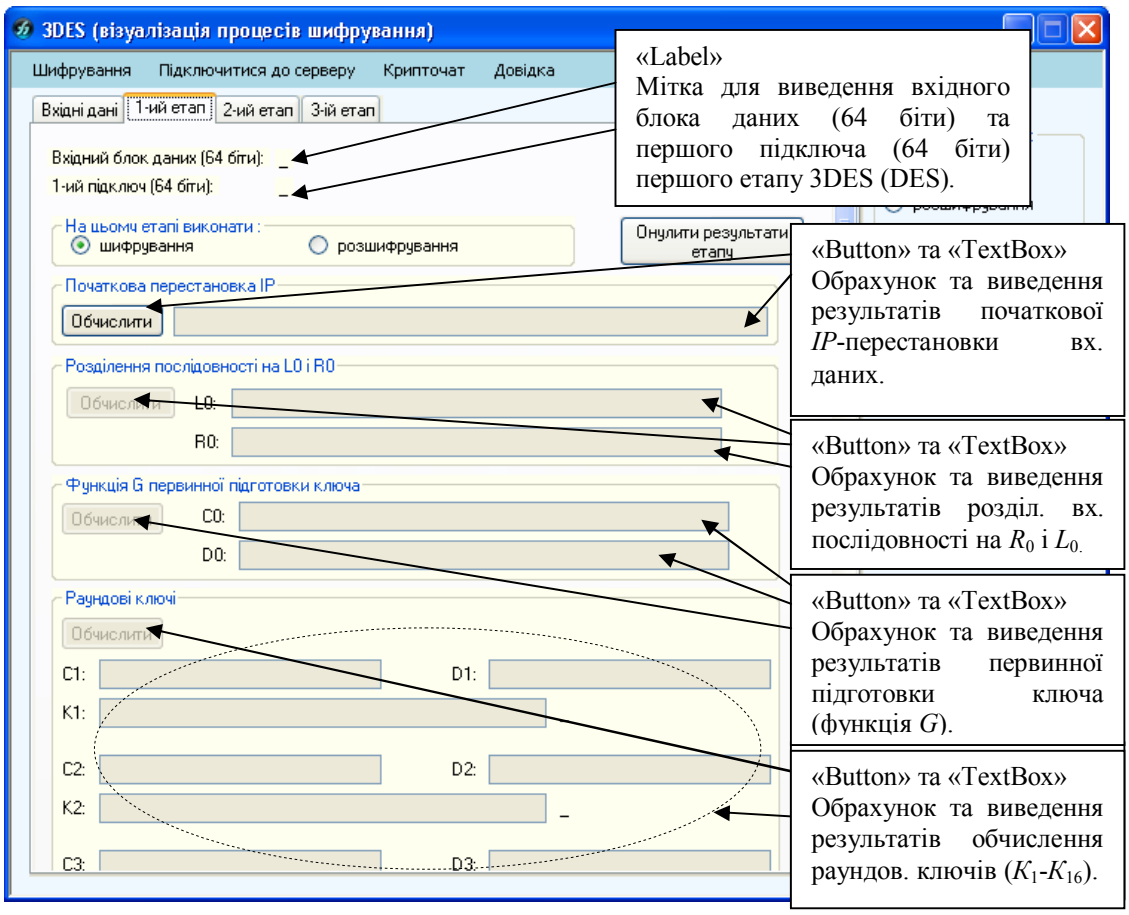

Рис. 9. Головне вікно програми (друга вкладка)

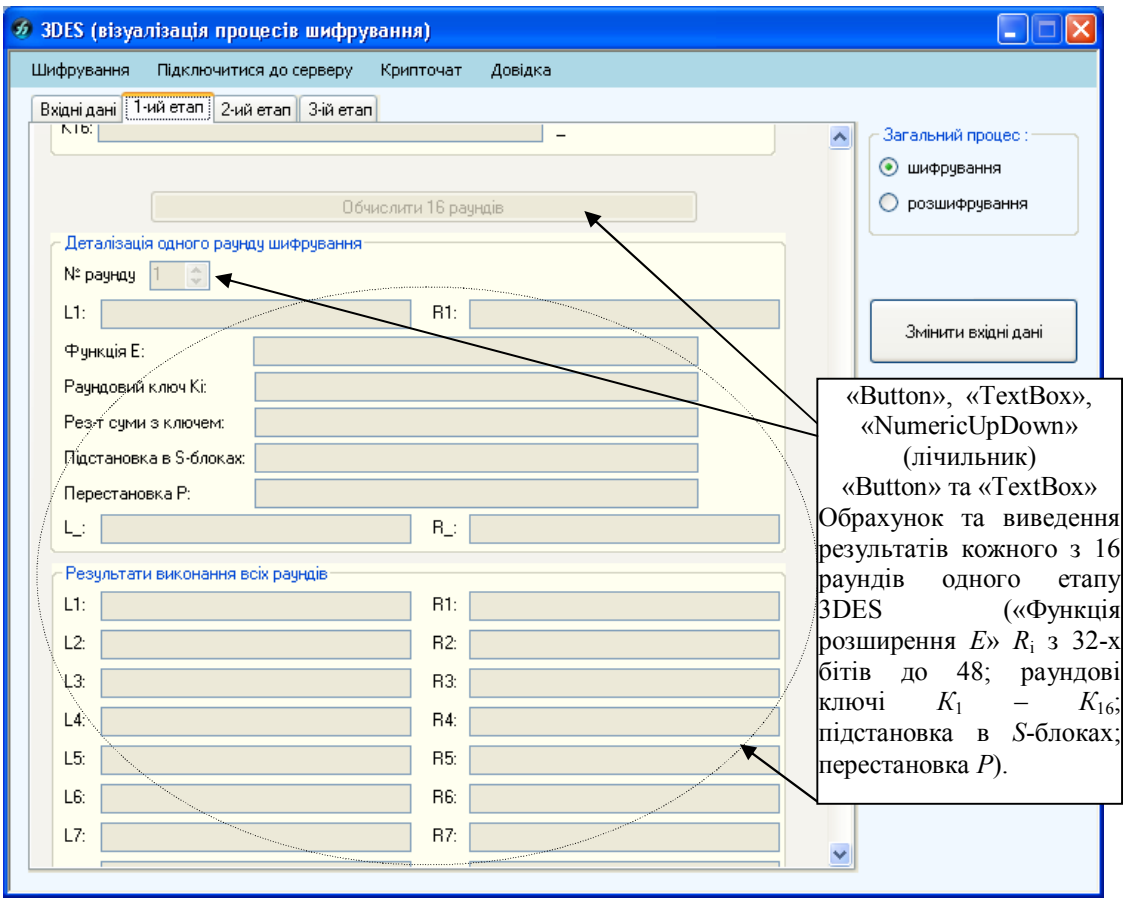

Рис. 10. Головне вікно програми (друга вкладка)

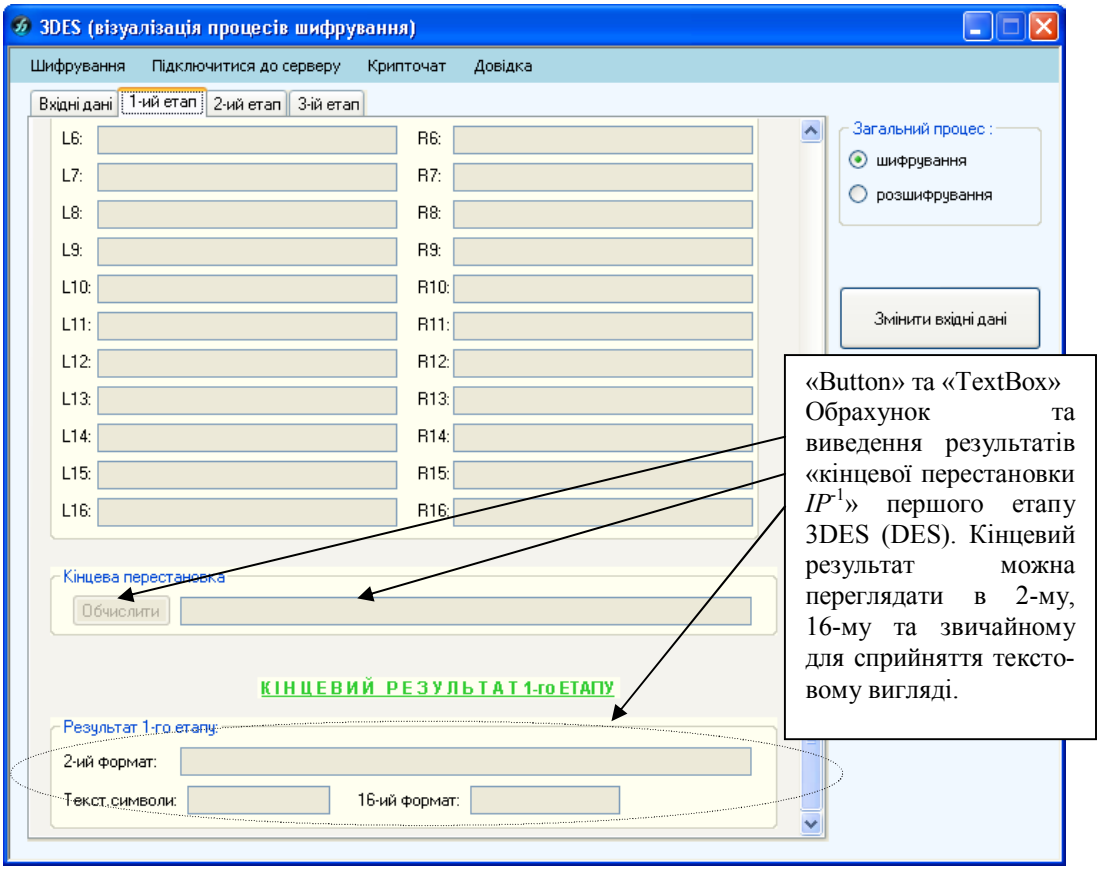

Рис. 11. Головне вікно програми (друга вкладка)

Рис. 7–11 візуально відображають інтерфейсне наповнення першого етапу програмної реалізації власного користувацького класу алгоритму забезпечення конфіденційності даних 3DES – алгоритму DES. Наступні етапи (другий та третій – 2DES та 3DES відповідно) ідентичні між собою: вхідними даними 2-го етапу будуть вихідні дані 1-го етапу, для 3-го – 2-го також окремо беруться ключі для кожного етапу, а функціональне наповнення інших елементів кожного з них залишається без змін (ідентичним).

На рис. 12 відображено головне вікно серверного додатка з описом його функціонального наповнення.

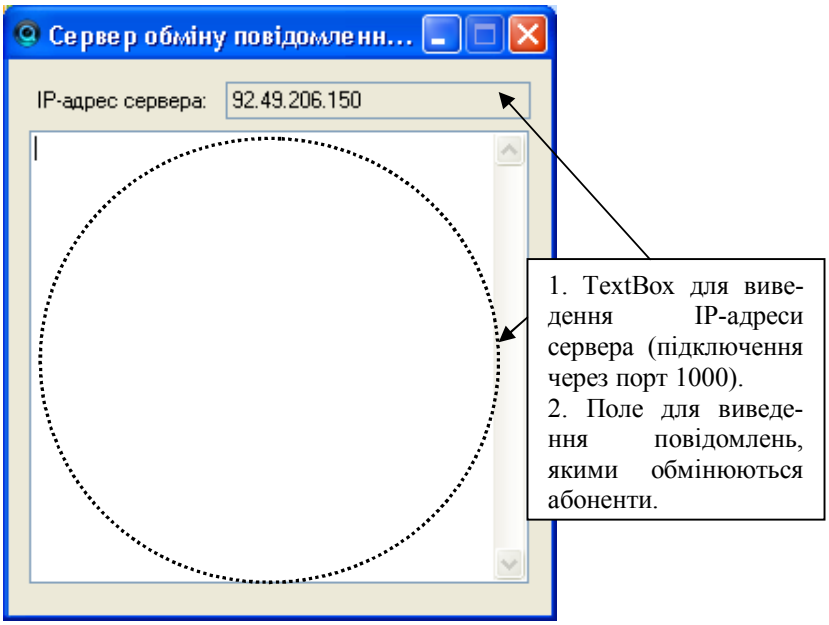

Рис. 12. Головне вікно серверного додатка з описом його функціонального наповнення

На рис. 13 відображено головне вікно клієнтського додатка «крипточата» (обміну шифрованими повідомленнями) з описом їх функціонального наповнення.

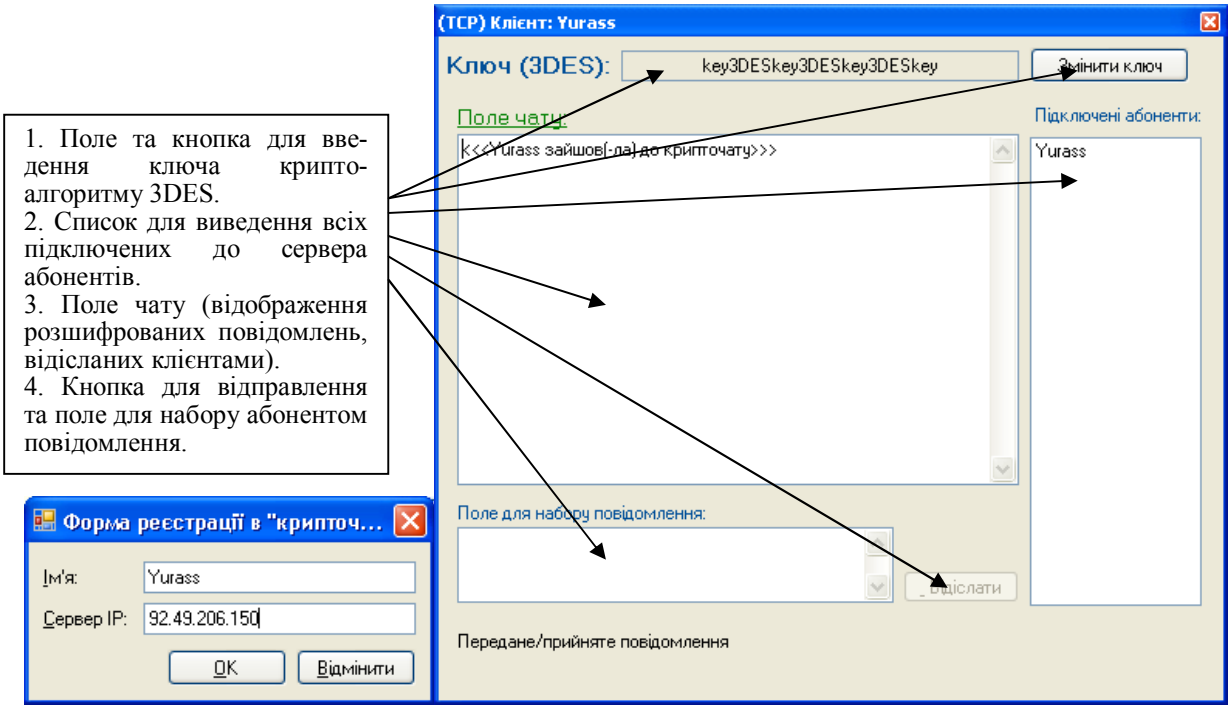

Рис. 13. Головне вікно клієнтського додатка «крипточата» з описом його функціонального наповнення

Висновки. Таким чином, розроблено програмний продукт візуалізації процесів забезпечення конфіденційності даних в ІТС з клієнт-серверною організацією зв'язку при використанні алгоритму симетричного шифрування 3DES. Отримані результати досліджень підтвердили теоретичні розрахунки і показали, що даний програмний продукт повністю програмно реалізує всі функції та алгоритми стандарту 3DES для забезпечення конфіденційності даних в ІКСМ.

Розроблений програмний комплекс є перспективною розробкою і може служити для підготовки фахівців у сфері інформаційної безпеки з метою автоматизації і підвищення якісного стану процесу навчання, а також може використовуватися в інформаційно-комунікаційних системах для забезпечення конфіденційності типових даних як під час зберігання їх на постійному носії ЕОМ, так і у ході роботи в обчислювальній комп'ютерній мережі.

У перспективі планується розробка типових програмних комплексів, базуючись на інших відомих алгоритмах з усіма можливими складовими інваріативного їх застосування.

СПИСОК ЛІТЕРАТУРИ

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с. : іл.
2. Основы криптографии : учеб. пособ. / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М. : Гелиос АРВ, 2002. – 480 с. : ил.
3. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В.Ф. Шаньгина. – М. : Радио и связь, 2001. – 376 с. : ил.

4. Смарт Н. Криптография ; пер. с англ. / Н. Смарт. – М. : Техносфера, 2005. – 528 с.: ил.
5. Корченко О. Г. Системи захисту інформації : монографія / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002. – 816 с .: ил.
7. Тимошенко А. О. Методи аналізу та проектування систем захисту інформації : курс лекцій / А. О. Тимошенко. – К. : Політехніка, 2007. – 174 с.
8. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Издательство Агентства «Яхтсмен», 1996. – 187 с.
9. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. – М. : «Горячая линия» – Телеком, 2004. – 280 с.
10. Корт С. Теоретические основы защиты информации / С. Корт. – СПб. : Издательство Гелиос – АРВ, 2004. – 240 с.
11. Коржик В. И. Теоретические основы информационной безопасности телекоммуникационных систем : учеб. пособ. / В. И. Коржик, Д. В. Кушнир. – СПб. : СПбГУТ, 2000. – 134 с.

Подано 26.08.13

Ю. Г. Даник, Ю. И. Дерпак

ПРОГРАММНЫЙ КОМПЛЕКС ВИЗУАЛИЗАЦИИ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В статье рассмотрены вопросы защиты данных в информационно-коммуникационных системах и сетях от несанкционированного доступа криптографическим алгоритмом. Выявлена и обоснована необходимость создания и модернизации современных систем комплексной защиты информации, определено основополагающее место криптографических методов в них в условиях глобальной информатизации. Также был рассмотрен криптоалгоритм Triple DES: его программная реализация на языке программирования C# с максимальной визуализацией процессов обеспечения конфиденциальности при его использовании.

Y. G. Danyk, Y. I. Derpak

SOFTWARE OF VISUALIZATION PROCESS PROVIDING DATA PRIVACY IN THE INFORMATION AND TELECOMMUNICATION SYSTEMS

This article describes the data protection issues in the information-communication systems and networks from an unauthorized access using cryptographic algorithms. The author revealed and substantiated the need for creating and upgrading advanced integrated systems of information protection and defined the fundamental place of cryptographic techniques for them in the context of global informatization. In the article was discussed cryptographic algorithm Triple DES, namely its software implementation by the programming language C# with maximum visualization processes when using it to ensure confidentiality of information.