Таким чином, усі кроки побудови проміжної полісітки розглянуто, що відкриває можливість подальшої програмної реалізації цього алгоритму в системах тривимірної комп'ютерної графіки.

Висновки і пропозиції.

1. Поєднання («зшивання») двох полігональних сіток через побудову третьої, проміжної полісітки може бути виконана за регулярним алгоритмом, основні кроки якого викладені у статті.
2. Алгоритм використовує як складові частини прийоми теорії множин та векторної алгебри, тому для його успішної програмної реалізації потрібно забезпечити доступ до відповідних математичних бібліотек.
3. У випадку програмної реалізації цей алгоритм може бути використаний як складова частина технології автоматизованої побудови поверхневих моделей реальних об'єктів з використанням тривимірного сканування останніх.

Список використаних джерел

1. *HDS Laser* Scanners & SW. Leica Geosystems Products [Електронний ресурс]. – Режим доступу : http://www.leica-geosystems.com/en/HDS-Laser-Scanners-SW_5570.htm.
2. *Bloomenthal J.* Convolution Surfaces / J. Bloomenthal, K. Shoemake // SIGGRAPH'91, Computer Graphics. – 1991. – Vol. 25, № 4. – P. 251–256.
3. *Шикин Е.* Компьютерная графика. Полигональные модели / Е. Шикин, А. Боресков. – М. : Диалог-МИФИ, 2000. – 464 с.
4. *Baumgart, B.* Winged Edge Polyhedron Representation. Technical Report. – Stanford University, Stanford, CA, USA. – 1972.
5. *Бронштейн И. Н.* Справочник по математике для инженеров и учащихся втузов / И. Н. Бронштейн, К. А. Семендяев. – М. : Наука, 1981. – 720 с.
6. *Фоли Д. Ж.* Основы интерактивной машинной графики : в 2 кн. Кн. 2 / Д. Ж. Фоли , Андрис вэн Дэм ; пер. с англ. В. А. Галактионова, Ю. М. Лазутина, О. Н. Родинко. – М. : Мир, 1985. – 368 с.

УДК 004.056.5:004.057.42

В.В. Соломаха, старш. викладач
М.В. Верьовко, аспірант
І.В. Соломаха, канд. екон. наук
Чернігівський національний технологічний університет, м. Чернігів, Україна

ДОСЛІДЖЕННЯ АЛГОРИТМІВ СИМЕТРИЧНИХ КРИПТОСИСТЕМ

В.В. Соломаха, ст. преподаватель
М.В. Веревко, аспирант
И.В. Соломаха, канд. экон. наук
Черниговский национальный технологический университет, г. Чернигов, Украина

ИССЛЕДОВАНИЕ АЛГОРИТМОВ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Valerii Solomakha, senior teacher
Mariia Verovko, PhD student
Iryna Solomakha, PhD in Economics
Chernihiv National University of Technology, Chernihiv, Ukraine

THE STUDY OF ALGORITHMS FOR SYMMETRIC CRYPTOSYSTEMS

Наведено результати практичних порівняльних досліджень сучасних алгоритмів симетричних криптосистем DES і IDEA по швидкодії під час роботи з різним об'ємом інформації і в різних режимах.

Ключові слова: *алгоритм шифрування, секретність ключа, криптосистема, швидкодія.*

Приведены результаты практических сравнительных исследований современных алгоритмов симметричных криптосистем DES и IDEA по быстродействию при работе с различным объемом информации и в различных режимах.

Ключевые слова: *алгоритм шифрования, секретность ключа, криптосистема, быстродействие.*

The article contains the results of comparative studies of modern algorithms of symmetric cryptosystem DES and IDEA on performance when working with different amount of information and in different modes.

Key words: *the encryption algorithm, the secret key, cryptosystem, performance.*

Постановка задачі. Метою дослідження було порівняння роботи сучасних алгоритмів симетричних криптосистем у ході шифрування (розшифрування) різних об'ємів інформації і при різних режимах роботи криптосистем.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження криптографічних алгоритмів останнім часом зробили як зарубіжні науковці (Джеймс Мессі (Університет ETH, Швейцарія), Е. Фуджісакі, Т. Окамото (Японія)), так і вітчизняні (В. Мельніков, Б. Ключевський, П. Ісаєв, Д. Зегжда та інші). Переважна кількість наукових робіт з питань відкритих криптографічних систем присвячена принципам функціонування блокових і потокових шифрів, в яких практично не порівнюють їх характеристики. Так, не виявлено порівнянь швидкості роботи різних режимів блокових алгоритмів і під час шифрування різних об'ємів інформації.

Мета статті. Існує безліч (не менше двох десятків) алгоритмів симетричних шифрів, істотними параметрами яких є:

– стійкість;
– довжина ключа;
– число раундів;
– довжина оброблюваного блока;
– складність апаратної/програмної реалізації;
– складність перетворення.

Метою дослідження було порівняння швидкодії алгоритмів DES і IDEA при шифруванні (розшифруванні) різних об'ємів інформації при різних режимах роботи криптосистем. Для цього використовувалася комп'ютерна система вивчення методів і засобів апаратно-програмного захисту інформації CRYPTO, яка написана на мові JAVA та дозволяє досліджувати криптографічні алгоритми і протоколи, формальні політики безпеки [5].

Виклад основного матеріалу. Історично першими з'явилися симетричні алгоритми шифрування. Основою секретності цих алгоритмів є секретність симетричного ключа, який має бути відомий як відправнику повідомлення, так і одержувачеві [5]. Схема шифрування з використанням симетричного ключа зображена на рис. 1.

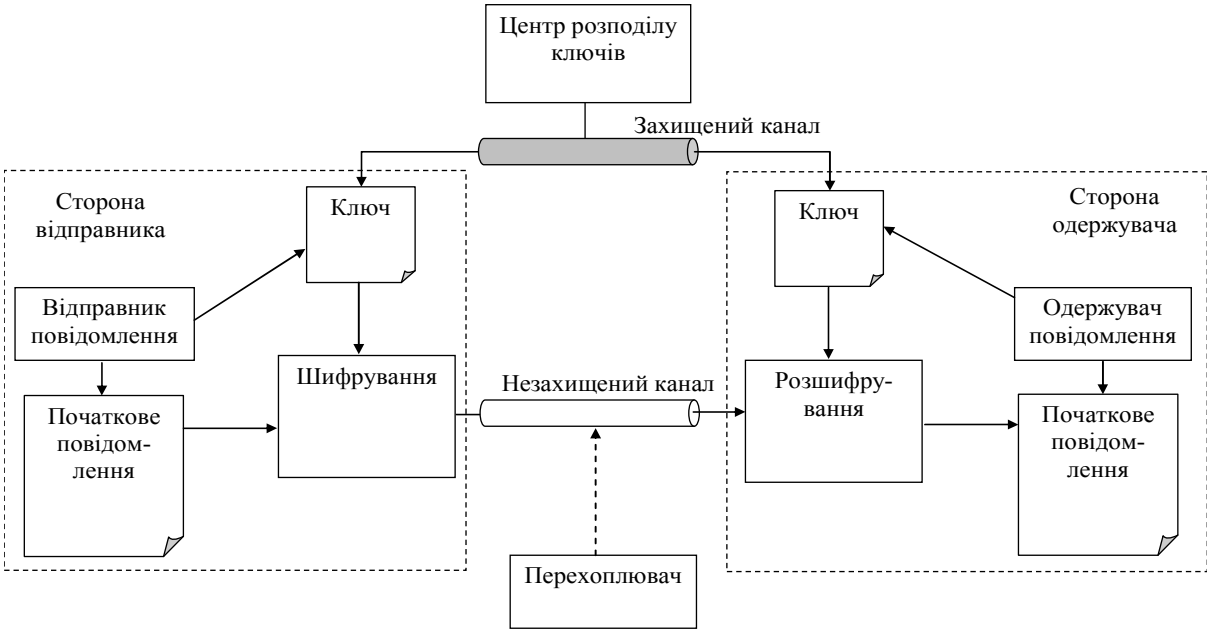

Рис. 1. Схема симетричного шифрування

Серед сучасних алгоритмів шифрування з симетричним ключем відомі і широко використовуються DES (Data Encryption Standard), IDEA, ГОСТ 28147-89, Blowfish, RC5 та інші [6].

Симетричні алгоритми шифрування ґрунтуються на застосуванні двох способів перетворення біт даних:

– дифузія;

– конфузія.

Дифузія виконує роль розсіювання статистичних особливостей відкритого тексту по широкому діапазону статистичних характеристик шифрованого тексту. Це досягається тим, що значення кожного елементу відкритого тексту впливає на значення багатьох елементів шифрованого тексту або, що виявляється еквівалентним сказаному, будь-який з елементів шифрованого тексту залежить від безлічі елементів відкритого тексту. В результаті застосування дифузії частотні характеристики використання окремих символів і послідовностей символів повинні ставати близькими до рівномірних.

Конфузія є механізмом складних підстановок, які утрудняють встановлення статистичного взаємозв'язку між шифрованим текстом і ключем. Метою застосування конфузії є протистояння тексту.

Перевагою симетричних алгоритмів є висока швидкодія і мала довжина ключа в порівнянні з ключами в алгоритмів з відкритим ключем.

Криптосистема DES (Data Encryption Standard):

розробник:	IBM
створено:	1977 р.
опубліковано:	1977 р.
розмір ключа:	56 біт
розмір блока:	64 біт
число раундів:	16

тип: мережа Фейстеля

режими роботи: електронна кодова книга (ECB),

зчеплення блоків (CBC),

зворотний зв'язок по шифротексту (CFB),

зворотний зв'язок по виходу (OFB).

Алгоритм DES використовує комбінацію підстановок і перестановок. DES здійснює шифрування 64-бітових блоків даних за допомогою 64-бітового ключа, в якому значущими є 56 біт (інші 8 біт – перевірочні біти для контролю на парність). Дешифрування в DES є операцією, зворотною шифруванню, і виконується через виконання операції шифрування у зворотній послідовності [1].

Схема шифрування алгоритму DES наведена на рис. 2, а детальна схема – на рис. 3.

Рис. 2. Схема шифрування DES

Початковий текст – блок 64 біт.

Шифрування (рис. 2):

– початкова перестановка;
– 16 циклів шифрування;
– кінцева перестановка.

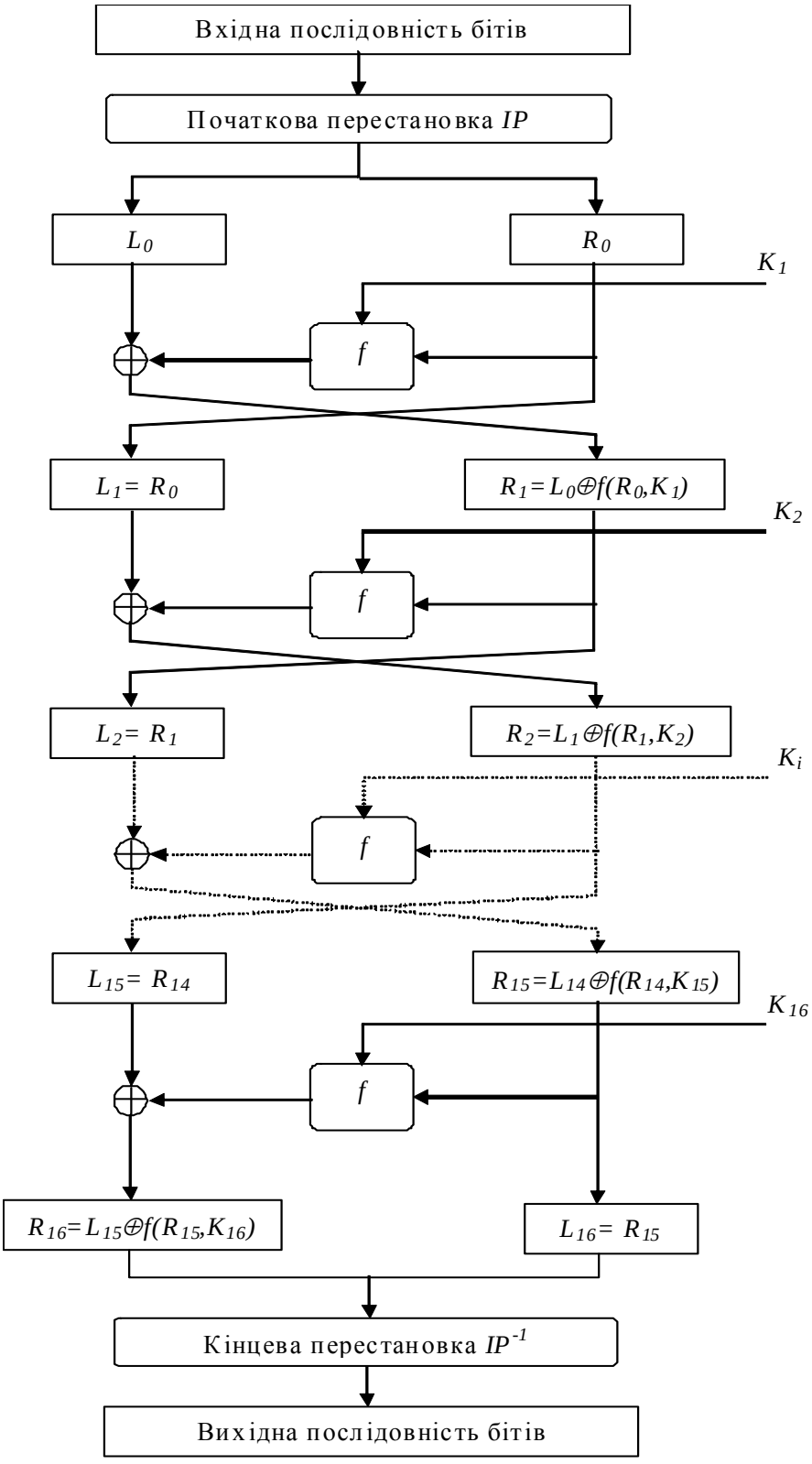

Рис. 3. Детальна схема алгоритму DES

Шифрований текст – блок 64 біт.

Детальна схема алгоритму DES наведена на рис. 3, де:

L_i, R_i, i=1,2… ліва та права половини 64-бітового блоку;

K_i – 48-бітові ключі;

f – функція шифрування;

IP – початкова перестановка;

IP^{-1} – кінцева перестановка.

Криптосистема IDEA (International Data Encryption Algorithm):

розробник:	Ascom
створено:	1991 р.
опубліковано:	1991 р.
розмір ключа:	128 біт
розмір блока:	64 біт
число раундів:	8,5

тип: модифікація мережі Фейстеля

IDEA – міжнародний симетричний блоковий алгоритм шифрування, запатентований швейцарською фірмою Ascom. Застосовується в пакеті програм шифрування PGP і в його вільній альтернативі GnuPG [2].

Шифрування представлено на рис. 4: – 8 однакових раундів шифрування;

– 1 вихідне перетворення.

Початковий текст ділиться на блоки по 64 біта.

Кожен такий блок ділиться на чотири підблоки по 16 біт кожен (D_1, D_2, D_3, D_4).

У кожному раунді використовуються свої подключі згідно з таблицею подключів.

Над 16-бітовими підключами і підблоками відкритого тексту робляться такі операції:

– множення за модулем $2^{16+1} = 65537$, причому замість нуля використовується 2^{16};

– складання за модулем 2^{16};

– побітове складання за модулем 2.

У кінці кожного раунду шифрування є чотири 16-бітові підблоки, які потім використовуються як вхідні підблоки для наступного раунду шифрування.

Вихідне перетворення є укороченим раундом: чотири 16-бітові підблоки на виході восьмого раунду і чотири відповідних підключа піддаються операціям:

– множення за модулем 216 + 1;

– складання за модулем 2^{16}.

Після виконання вихідного перетворення конкатенація підблоків D_1', D_2', D_3' і D_4' є зашифрованим текстом.

Потім береться наступний 64-бітовий блок відкритого тексту й алгоритм шифрування повторюється, поки не зашифруються всі 64-бітові блоки початкового тексту.

З 128-бітового ключа генерується:

– для кожного з восьми раундів шифрування по шість 16-бітових підключів;

– а для вихідного перетворення чотири 16-бітових підключі.

Всього знадобиться $52 = 8 \cdot 6 + 4$ різних підключа по 16 біт кожен.

128-бітовий ключ розбивається на вісім 16-бітових блоків. Це будуть перші вісім підключів по 16 біт кожен. Цей 128-бітовий ключ циклічно зрушується вліво на 25 позицій. Після цього новий 128-бітовий блок знову розбивається на вісім 16-бітових блоків. Це вже наступні вісім підключів по 16 біт кожен. Процедура циклічного зрушення і розбиття на блоки триває доти, поки не будуть згенеровані всі 52 16-бітних підключа.

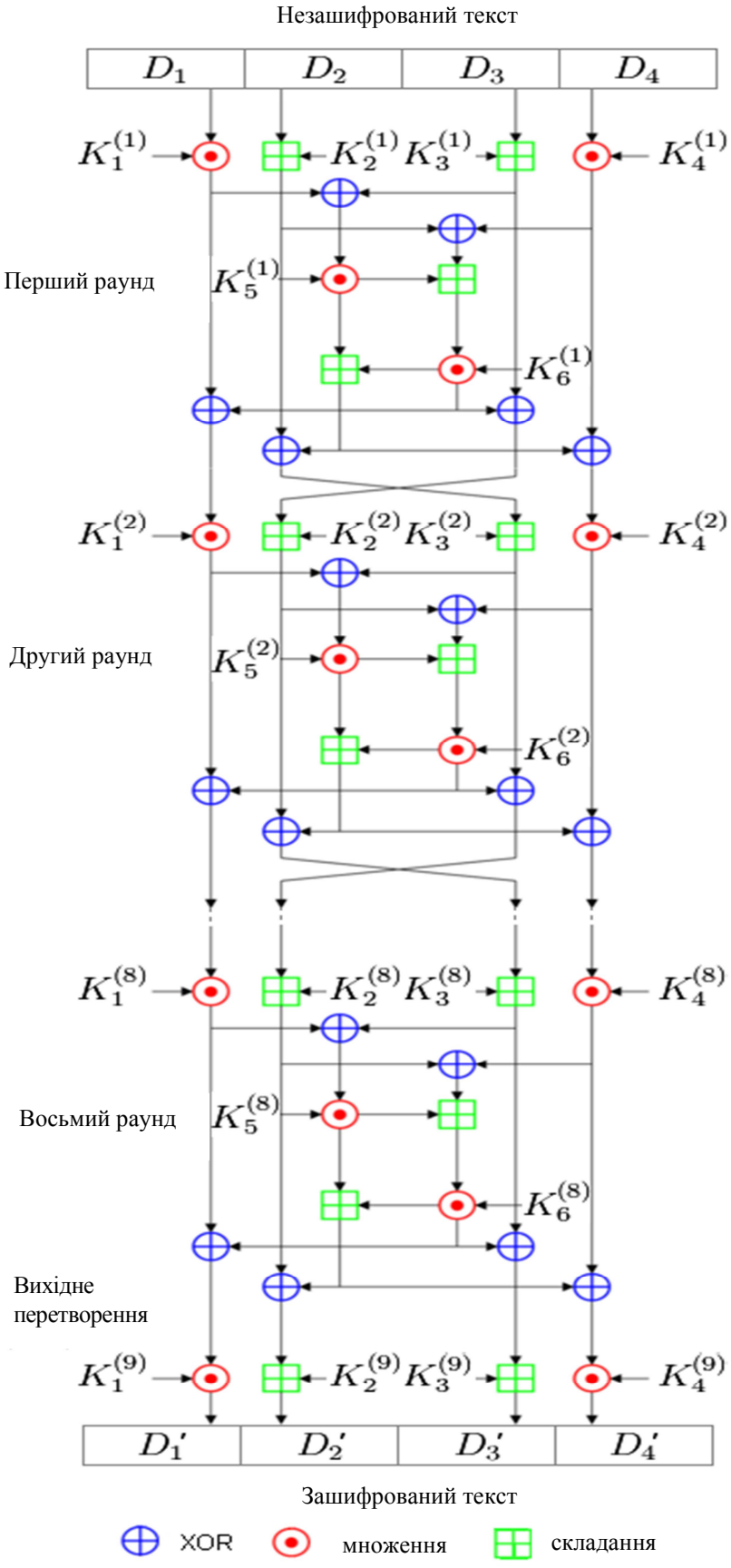

Рис. 4. Схема алгоритму IDEA

Порівняння алгоритмів за основними параметрами наведено в табл. 1:

Таблиця 1

Параметри алгоритмів

Алгоритм	Розмір ключа, біт	Довжина блока, біт	Число раундів	Основні операції
DES	56	64	16	Підстановка, перестановка, побітове АБО, що виключає
IDEA	128	64	8	Множення за модулем $2^{16}+1$, складання за модулем 2^{16}, побітове АБО, що виключає

Джерело: [2].

Порівняння симетричних та асиметричних криптосистем [4]:

Головною перевагою криптосистем з відкритим ключем є їх потенційно висока безпека: не треба передавати значення секретних ключів.

У симетричних криптосистемах є небезпека розкриття секретного ключа під час передачі.

Недоліки асиметричних криптосистем:

– генерація нових ключів заснована на генерації великих простих чисел, а перевірка простоти чисел займає багато процесорного часу;

– процедури, пов'язані з піднесенням до степеня багатозначного числа, досить громіздкі.

Тому швидкодія криптосистем з відкритим ключем у сотні і більше разів менша швидкодії симетричних криптосистем із секретним ключем.

Криптосистеми реалізуються як апаратно, так і програмно.

Для апаратної реалізації розроблено спеціальні процесори на (СВІС), що дозволяють виконувати піднесення великих чисел до колосально великого степеня за модулем N за відносно короткий час.

Кращими з них, які серійно випускаються, є процесори фірми CYLINK, що виконують 1024-бітове шифрування RSA.

Результати досліджень. Швидкодії алгоритмів DES та IDEA під часи шифрування та розшифрування різних об'ємів інформації та при різних режимах роботи криптосистем наведені в табл. 2.

Таблиця 2

Час роботи криптосистем у різних режимах, мс

Криптосистема	Процес	Об'єм інформації, байт			Об'єм інформації, байт			Об'єм інформації, байт		
		1000	10 000	100 000	1000	10 000	100 000	1000	10 000	100 000
IDEA	шифр	6	35	60	2	6	24	0	17	31
	розшифр	6	29	57	1	2	20	0	15	16
DES	шифр	64	264	511	7	21	152	0	40	230
	розшифр	57	255	498	2	18	149	0	38	218
		зворотний зв'язок по виходу			зчеплення блоків			електронна кодова книга		

Висновки і пропозиції. 1. Алгоритм IDEA працює швидше, ніж DES, особливо при великих об'ємах інформації, що обумовлено використанням більш швидких операцій множення за модулем $2^{16}+1$, складання за модулем 2^{16}.

2. Розшифрування робиться швидше за шифрування.

3. Найшвидше працюють алгоритми в режимі зчеплення блоків.

4. Недоліками алгоритму IDEA є те, що він запатентований, тобто не може вільно поширюватися, а також у ньому не передбачена можливість збільшення ключа.

5. Апаратна реалізація асиметричної криптосистеми ≈ в 1000 разів повільніше за апаратну реалізацію симетричного криптоалгоритму.

6. Програмна реалізація RSA ≈ в 100 разів повільніше DES.

З розвитком комп'ютерних технологій ці оцінки можуть дещо змінюватися, але асиметрична криптосистема ніколи не досягне швидкодії симетричних криптосистем [6].

Список використаних джерел

1. *Зегжда Д. П.* Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия–Телеком, 2000. – 452 с.

2. *Диффи У.* Защищенность и имитостойкость. Введение в криптографию / У. Диффи, М. Э. Хэллмэн // ТИИЭР. – 1979. – Т. 67, № 3. – С. 71–109.

3. *Домашев А. В.* Программирование алгоритмов защиты информации / А. В. Домашев, В. О. Попов, Д. И. Правиков. – М. : Нолидж, 2000. – 279 с.

4. *Мельников В. В.* Защита информации в компьютерных системах / В. В. Мельников. – М. : Финансы и статистика, 1997. – 368 с.

5. *Романец Ю. В.* Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с.

6. *Столингс В.* Криптография и защита сетей / В. Столингс. – М. : Вильямс, 2001. – 672 с.

7. *Ященко В. В.* Введение в криптографию / В. В. Ященко. – СПб. : Питер, 2001. – 288 с.

UDC 004.451.9

Volodymyr Kazymyr, Doctor of Technical Sciences
Ihor Karpachev, PhD student
Chernihiv National University of Technology, Chernihiv, Ukraine

FUNCTIONAL SECURITY IN AN ANDROID MOBILE ARCHITECTURE

В.В. Казимир, д-р техн. наук
І.І. Карпачев, аспірант
Чернігівський національний технологічний університет, м. Чернігів, Україна

ФУНКЦІОНАЛЬНА БЕЗПЕКА АРХІТЕКТУРИ МОБІЛЬНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

В.В. Казимир, д-р техн. наук
И.И. Карпачев, аспирант
Черниговский национальный технологический университет, г. Чернигов, Украина

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ АРХИТЕКТУРЫ МОБИЛЬНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

Android is currently the most popular operating system used on smartphones. However, users feel their private information is at threat, facing a rapidly increasing number of malware for Android, which significantly exceeds that of other platforms. Antivirus software promises effective protection against malware on mobile devices and many products are available for free or at reasonable prices. Their effectiveness is supported by various reports, attesting very high detection rates. Neither do the exceedingly high numbers of different malware variants reflect the real threat in comparison to other platforms, nor do the results of testing antivirus software against a set of already known malware samples (retrospective tests) provide a clear picture of the capabilities and limitations of antivirus software on the Android platform.

***Key words**: android security, malware protection, viruses, protection software.*

Досліджено проблеми функціональної безпеки, вразливостей мобільних пристроїв не тільки з боку операційної системи, але також з боку стороннього програмного забезпечення.

***Ключові слова:** функціональна безпека, операційна система андроїд, функціональний захист.*

Исследованы проблемы функциональной защиты, уязвимостей мобильных устройств не только со стороны операционной системы, но так же со стороны постороннего программного обеспечения.

***Ключевые слова**: функциональная безопасность, операционная система андроид, функциональная защита.*

Introduction to the topic of the study. The general perception of Android security has been largely shaped by two classes of reports: first, antivirus vendors – as they have access to