УДК 004.056.55:004.056.53:004.415.2

АНАЛІЗ ЧАСОВИХ ПОКАЗНИКІВ ШИФРУВАННЯ/ДЕШИФРУВАННЯ ФАЙЛІВ БАЗ ДАНИХ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Є. Б. Лопін

Науково-дослідний інститут проблем військової медицини Збройних Сил України

У статті у вигляді конкретного прикладу наведені результати досліджень стосовно часу шифрування/дешифрування файлів баз даних медичних інформаційних систем, проведеного з використанням трьох принципово різних алгоритмів, складовими частинами яких, у свою чергу, є криптоалгоритм Blowfish. Встановлено, що шляхом оптимізації роботи алгоритмів програмного забезпечення можливе зменшення часу шифрування/дешифрування відносно великих файлів (десятки мегабайт) до прийнятних для повсякденного використання величин.

Ключові слова: алгоритм Blowfish, швидкість шифрування/дешифрування, шифрування/дешифрування файлів.

АНАЛИЗ ВРЕМЕННЫХ ПОКАЗАТЕЛЕЙ ШИФРОВАНИЯ/ДЕШИФРОВАНИЯ ФАЙЛОВ БАЗ ДАННЫХ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е. Б. Лопин

Научно-исследовательский институт проблем военной медицины Вооружённых Сил Украины

В статье на конкретном примере приведены результаты исследований относительно времени шифрования/дешифрования файлов баз данных медицинских информационных систем, проведенных с использованием разработанных трёх принципиально разных алгоритмов, использующих, в свою очередь, как составную часть криптоалгоритм Blowfish.

Исследования проводились с использованием специально разработанной (в среде программирования Delphi 7) компьютерной программы “Generators” (авт. название) и двух компьютеров устаревшей конфигурации, собранных на базе процессоров Intel Core 2 Duo E8400 и DualCore Intel Pentium E2180.

Проведенные исследования позволили установить, что шифрование/дешифрование файлов с использованием первого разработанного алгоритма, при выполнении которого осуществляется многократное обращение к жесткому диску вследствие считывания и записи блоков размером 8 байт, занимает намного больше времени (приблизительно в 10 раз), чем шифрование/дешифрование с использованием второго и третьего алгоритмов, при выполнении которых обращение к жесткому диску осуществляется для считывания и записи файла целиком, то есть однократно.

В сравнении с третьим алгоритмом, в ходе работы которого все операции осуществляются только в исходном буфере, при использовании второго алгоритма многократное копирование в оперативной памяти компьютера блоков информации по 8 байт замедляет скорость шифрования/дешифрования файла размером 80,97 мегабайт на обоих компьютерах в среднем приблизительно на 1 с ($P<0,001$).

Таким образом, наименьшее время шифрования/дешифрования файлов (3,7-3,63 с и 6,56-6,6 с для двух вышеуказанных компьютеров и файла размером 80,97 мегабайт) было достигнуто при использовании именно третьего алгоритма, который предусматривает однократное обращение к жёсткому диску для считывания/записи файла и осуществление шифрования/дешифрования непосредственно в буфере памяти, в который обрабатываемый файл считывается.

В результате временные показатели шифрования/дешифрования файлов, полученные при использовании второго и третьего алгоритмов, позволяют сделать вывод про целесообразность и практическую применимость как метода криптографической защиты информации шифрования файлов баз данных медицинских информационных систем. При этом относительно большой размер файлов (десятки и сотни мегабайт) не является критическим препятствием для успешного и комфортного использования с целью криптографической защиты информации шифровальных компьютерных программ или отдельных, встроенных в программное обеспечение, процедур и функций.

Ключевые слова: алгоритм Blowfish, скорость шифрования/дешифрования, шифрование/дешифрование файлов.

✉ Є. Б. Лопін

ANALYSIS OF TIME DISTANCES OF ENCRYPTION/DECRYPTION OF MEDICAL INFORMATION SYSTEMS DATABASES FILES

Ye. B. Lopin

Research Institute of Military Medicine of Ukraine Armed Forces

In the article on the specific example the results of studies medical information systems databases files encryption/decryption time have been presented. The present studies are performed using the developed three fundamentally different algorithms, that include Blowfish encryption algorithm as a part.

The studies were performed using a specially developed (in the programming environment Delphi 7) computer program "Generators" (author's title) and two computers having obsolete configuration and assembled with the Intel Core 2 Duo E8400 processor and the DualCore Intel Pentium E2180 processor.

The studies have established that the encryption/decryption of files using the first developed algorithm during execution of which multiple access to the hard drive for reading/writing of 8-byte information blocks of is implemented, takes much longer time (about 10 times) than the encryption/decryption using the second and third algorithms during execution of which access to the hard drive for a file reading/writing is performed once.

In comparison with the third algorithm during execution of which all the operations are carried out only in the starting memory buffer, while using the second algorithm multiple copying process into RAM 8-byte information blocks of slows down encryption/decryption a file with the size of 80.97 MB on both computers an average of about 1 s ($P<0,001$).

Therefore the least time encryption/decryption of files (3,7-3,63 s and 6,56-6,6 s for two above-mentioned computers and a file with the size of 80.97 MB) has been achieved by using just the third algorithm, which provides a single access to the hard drive for reading/writing of a file and a file encryption/decryption directly in the starting memory buffer into which the processed file is read.

As a result, time distances of files encryption/decryption, obtained with the use of the second and third algorithms, allow us to conclude about the desirability and feasibility of encryption of medical information systems databases files as a method of information cryptographic protection.

Under such conditions the relatively large size of the files (tens or hundreds of megabytes) is not a critical obstacle to a successful and comfortable use of cryptographic information protection using encryption software or separate embedded in other software functions and procedures.

Key words: algorithm Blowfish, encryption/decryption speed, files encryption/decryption.

Вступ та актуальність. Аналіз прийнятих у світі підходів до розробки комплексних систем захисту інформації показує, що окрім технічних (апаратних) пристроїв (приладів) та відповідних організаційних заходів ефективним є використання програмно-технічних засобів захисту інформації, у тому числі засобів криптографічного захисту інформації або, говорячи простою мовою, програмного забезпечення, призначеного для шифрування даних [1]. При цьому може використовуватись як шифрування даних, які вже потім (після шифрування) зберігаються до файлу [2], так і шифрування безпосередньо каталогів та файлів, у тому числі файлів баз даних медичних інформаційних систем.

Попередні дослідження в даній області показали, що одним із основних напрямків використання засобів криптографічного захисту інформації в автоматизованих інформаційних системах є забезпечення зберігання в захищеному (зашифрованому) вигляді інформації, необхідної для ідентифікації конкретних осіб (так званий "електронний підпис" [1], паролі та ін.), а також деякої іншої конфіденційної інформації (про платіжні банківські карти, персональних даних та ін.).

Нескладно припустити, що зберігання в базах даних зашифрованої числової, символьної (текстової) та іншої інформації значно обмежуватиме можливості її автоматизованої обробки та використання з пошуковою метою SQL-запитів, внаслідок чого більш доцільним в деяких випадках може бути використання саме шифрування файлів баз даних.

Звісно, ключовим питанням в цьому випадку є визначення максимально можливої швидкості, з якою могли б шифруватись та дешифруватись достатньо великі файли баз даних. Окрім цього, дослідників та інших читачів можуть зацікавити оптимізовані з метою зменшення витрат часу на шифрування/дешифрування алгоритми роботи програмного забезпечення.

Вищенаведені міркування, вимоги статей Закону України "Про захист персональних даних" від 1 червня 2010 року № 2297-VI [4], а також практична відсутність інформативних публікацій з даної тематики в наукових виданнях та інших широкодоступних джерелах інформації (Інгернет, довідкова література) обумовлює можливий інтерес, який може викликати наведене нижче дослідження у певних категорій читачів (потенційних замовників медичних інформа-

ційних систем, програмістів, спеціалістів із захисту інформації та ін.).

Метою даного дослідження була кількісна оцінка часових параметрів (показників) шифрування/дешифрування файлів баз даних медичних інформаційних систем, а також оцінка відповідності даних параметрів суб'єктивним критеріям комфортності роботи користувача медичної інформаційної системи.

Матеріали та методи досліджень. Для проведення даного досить складного за своєю природою дослідження була використана спеціально розроблена (в середовищі програмування Delphi 7) комп'ютерна програма "Generators", яка за своїм призначенням не є засобом криптографічного захисту інформації. Функції шифрування/дешифрування в даній програмі реалізовані із використанням незапатентованого та дозволеного для вільного використання симетричного криптографічного алгоритму Blowfish [5].

Для шифрування використовувався адаптований для виконання наукових досліджень файл бази даних обліку пролікованих хворих Головного військового клінічного госпіталю Міністерства оборони України (зараз Головний військово-медичний клінічний центр Міністерства оборони України) в форматі Microsoft Office Access 2003 (*.mdb) розміром 80 969 728 байт. В якості ключа для шифрування/дешифрування використовувалась послідовність символів "1qw,kg785io3mgk;drtyepslc".

Для виконання дослідження використовувались 2 комп'ютери із встановленою операційною системою Windows XP наступної конфігурації:

№1 – процесор Intel Core 2 Duo E8400, 3000 MHz (9 x 333), материнська плата ASUSTeK Computer INC P5G41T-M/USB3, системна пам'ять 3584 Мб (DDR3-1333 DDR3 SDRAM), відеоадаптер ATI Radeon HD 5600 Series (1024 Мб), дисковий накопичувач Hitachi HDS721032CLA362 (320 Гб, 7200 RPM, SATA-II);

№2 – процесор DualCore Intel Pentium E2180, 2000 MHz (10 x 200), системна плата Biostar GF7100P-M7S (2 PCI, 1 PCI-E x1, 1 PCI-E x16, 2 DDR2 DIMM, Audio, Video, Gigabit LAN), системна пам'ять 1024 Мб (DDR2-800 DDR2 SDRAM), відеоадаптер NVIDIA GeForce 6600 GT (128 Мб), дисковий накопичувач SAMSUNG HD200HJ (200 Гб, 7200 RPM, SATA-II).

Дослідження виконували наступним чином: створювали 10 копій вищевказаного файлу, які шифрувались, а потім дешифрувались. Для доведення лінійності залежності часу шифрування від розміру файлу використовувались фрагменти файлів, отримані за допомогою комп'ютерною програми Total Commander версії 7.55. Шифрування цих фрагментів здійснювалось по 10 разів, після чого визначались середнє арифметичне та інші показники.

Результати досліджень та їх обговорення. Для оцінки швидкості шифрування/дешифрування файлів в ході підготовки даного дослідження були розроблені зображені на рисунку 1 алгоритми, в яких є посилання на програмну реалізацію (процедуру EncryptBlowFish_1) відомого криптоалгоритму Blowfish [5]. Також розроблені, багато у чому ідентичні зображеним на рис. 1, алгоритми дешифрування, в якості складової яких використана процедура DecryptBlowFish_1, на рисунках в цій статті не наводяться.

На даний час у світі розроблено та використовується багато криптографічних алгоритмів (IDEA [6], Twofish [7], AES [8], DES [9], Triple DES [10], RC6 [11], SEED [12], Camellia [13], CAST-128 [14], XTEA [15], "ГОСТ 28147-89" [16] та ін., див. ресурс мережі Internet "http://ru.wikipedia.org/"), практично кожен з них може бути використаний як складова частина алгоритмів, зображених на рисунку 1, а алгоритм Blowfish був обраний тільки тому, що він є незапатентованим та вільно розповсюджуваним [5], окрім цього існує достатньо багато його програмних реалізацій.

Як бачимо на рисунку 1, для зчитування-запису файлів в усіх трьох алгоритмах використовувались стандартні функції Delphi FileRead та FileWrite, виділення пам'яті здійснювалось функцією AllocMem, копіювання – CopyMemory [17, 18], безпосередньо шифрування здійснювалось під час виконання (роботи) процедури EncryptBlowFish_1, інші пояснення див. безпосередньо після рис. 1.

Під час роботи першого алгоритму здійснюється зчитування з вихідного файлу (з дескриптором FileHandle_1) блоків по 8 байт до області пам'яті Buffer (перемінна-покажчик типу PChar), після шифрування дані блоки записуються до результуючого (зашифрованого) файлу (з дескриптором FileHandle_2).

В другому алгоритмі (у центрі на рис. 1) до області пам'яті (буферу) Buffer_All (покажчик типу PChar, див. [17]) зчитується одразу увесь вихідний файл (FileHandle_1), після чого з нього до буферу Buffer функцією CopyMemory копіюються блоки по 8 байт, які після шифрування копіюються до результуючого буферу Buffer_All_Result (також покажчик типу PChar), а з нього вже записуються до результуючого файлу (FileHandle_2).

Третій алгоритм найбільш простий серед усіх – до буферу Buffer_All зчитується одразу увесь вихідний файл (FileHandle_1), після шифрування даних безпо-

середньо в комірках пам'яті цього буферу зашифрована інформація записується до результуючого файлу (FileHandle_2).

Нескладно припустити, що саме під час використання третього принципу побудови алгоритмів час шифрування/дешифрування повинний бути найменшим. Другий варіант побудови алгоритму, у свою чергу, дозволить оцінити час, що витрачається на багатократне здійснення операцій копіювання в пам'яті, а перший – час на багатократне звернення до жорсткого диска для зчитування/запису блоків розміром у 8 байтів.

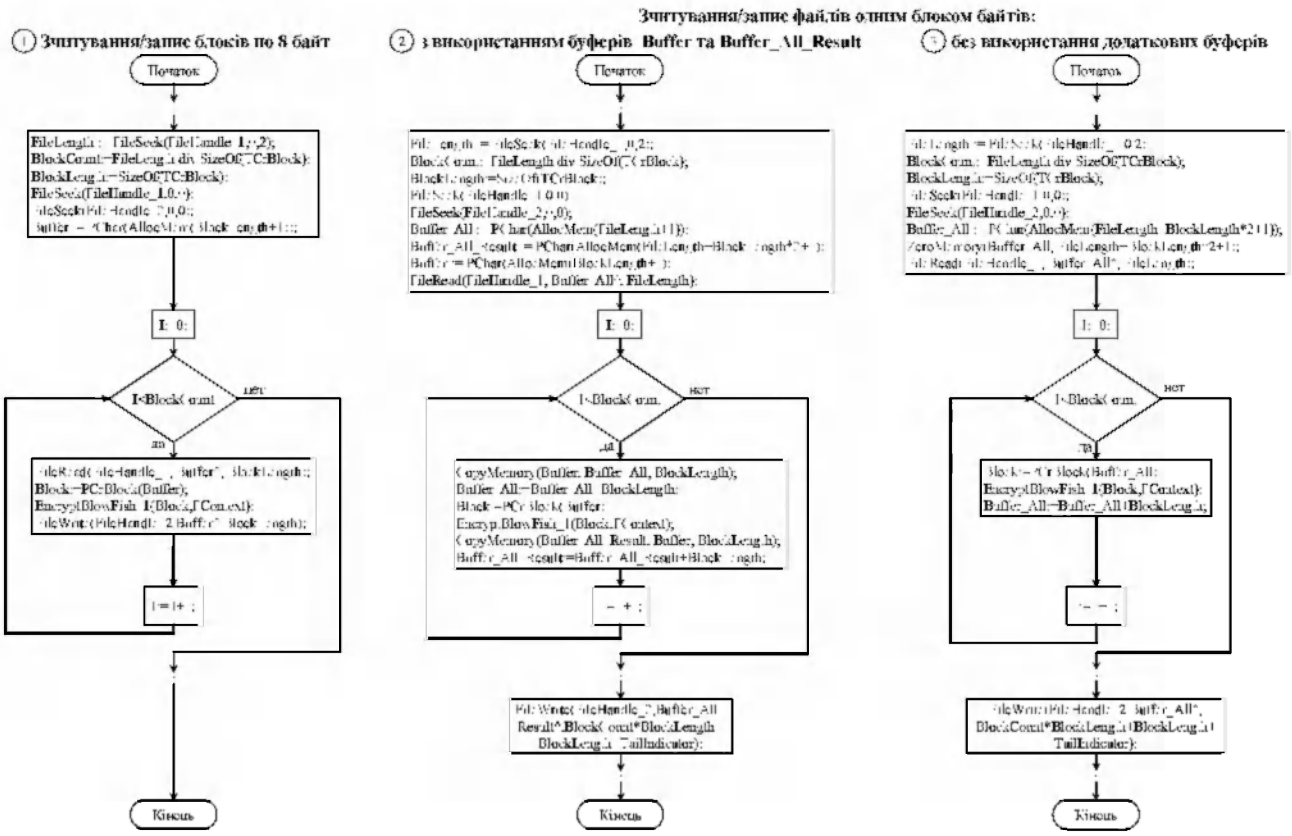

Рис. 1. Алгоритми шифрування файлів (перший варіант ліворуч, другий у центрі, третій праворуч):

FileSeek – функція Delphi, за допомогою якої здійснюється навігація в межах файлу і, у тому числі, визначається розмір файлу, який потім зберігається до перемінної FileLength (тип Integer);
BlockCount – перемінна типа Integer, кількість у файлі блоків по 8 байт;
SizeOf – функція Delphi, за допомогою якої визначається розмір в байтах перемінних або більш складних об'єктів;
AllocMem – функція Delphi, за допомогою якої виділяється область пам'яті, на яку вказують покажчики Buffer, Buffer_All и Buffer_All_Result;
CopyMemory – функція Delphi, яка дозволяє виконати копіювання обраної області пам'яті до іншої;
ZeroMemory – функція Delphi, що дозволяє очистити вказану область пам'яті;
FileHandle_1 и **FileHandle_2** – ідентифікатори вихідного файлу та зашифрованого/дешифрованого файлу;
EncryptBlowFish_1 – процедура шифрування блоку з 8 байтів (procedure EncryptBlowFish_1(CrData: PCrBlock; const CrContext: TCryptoContext););
TCryptoContext – тип даних, який містить в собі два масиви (TCrKeyArray = array[1..18] of Cardinal; TSBoxes= array[0..3, 0..255] of Cardinal;), необхідних для виконання процедури шифрування;
TCrBlock – тип даних, що являє собою масив із двох цілих чисел (TCrBlock = array[0..1] of Cardinal;);
PCrBlock – тип даних, що являє собою покажчик на дані типу TCrBlock (PCrBlock =^TCrBlock:):
Block – перемінна (тип PCrBlock);
FContext – дані (масиві) типу TCryptoContext;
FileRead та **FileWrite** – функції Delphi для зчитування та запису файлів.

Вищеописані алгоритми шифрування, а також розроблені на їх основі та багато у чому ідентичні їм алгоритми дешифрування, були реалізовані в спеціальній дослідницькій комп'ютерній програмі "Generators" (рис. 2), яка за допомогою спеціальних елементів управління дозволяє реєструвати час початку та закінчення роботи процедур шифрування/дешифрування файлів (рис. 3).

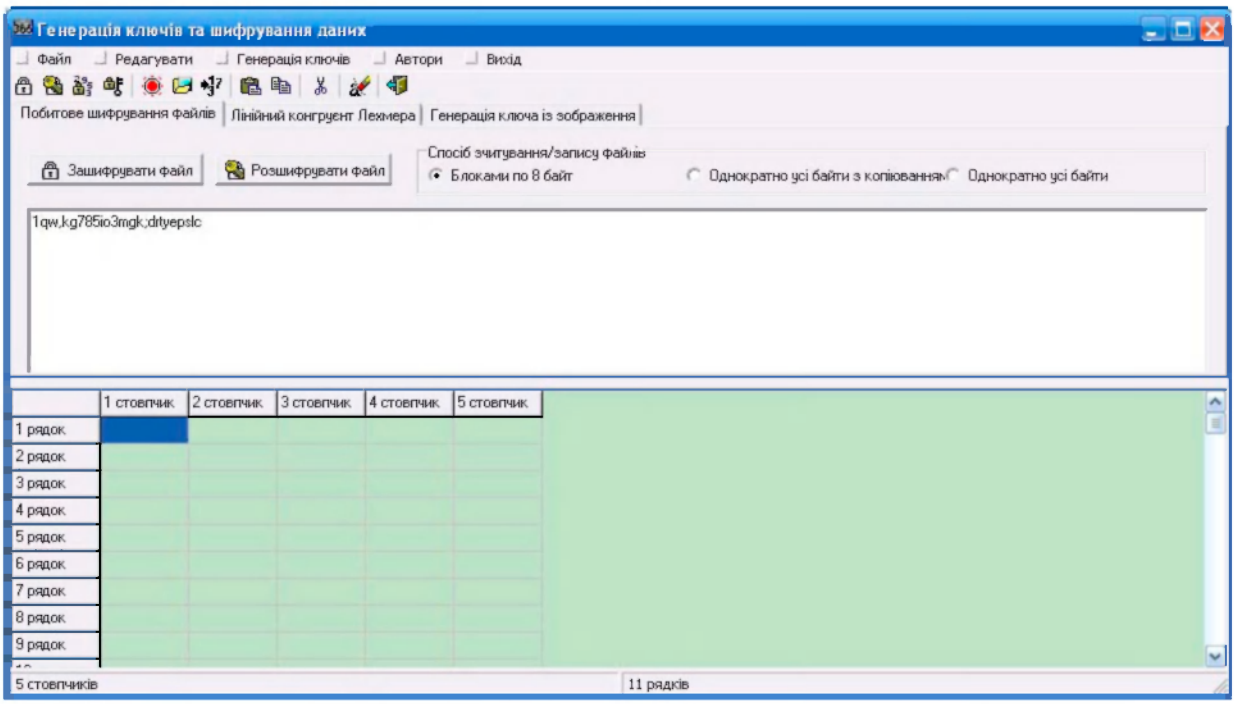

Рис. 2. Головна форма програми "Generators", за допомогою якої проводились вимірювання (реєстрація) часу шифрування/дешифрування.

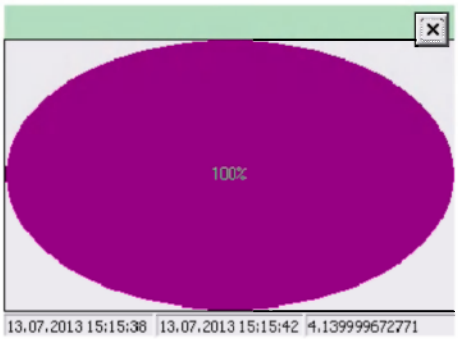

Рис. 3. Форма програми "Generators", призначена для виводу користувачу результатів вимірювань (реєстрації) часу шифрування/дешифрування.

Часові показники шифрування/дешифрування програмою "Generators" файлу бази даних медичної інформаційної системи "GVKG_2002.mdb" та його копій на двох різних комп'ютерах застарілої конфігурації (див. матеріали та методи досліджень на початку статті) наведені в таблиці 1.

З даних таблиці 1 бачимо, що шифрування/дешифрування з багатократним зверненням до жорсткого диску (перший варіант побудови алгоритму), яке здійснюється внаслідок зчитування та запису блоків по 8 байт, займає набагато більше часу, ніж шифрування/дешифрування з однократним зчитуванням до оперативної пам'яті одразу всього файлу (відмінність аксіоматично достовірна). Однак слід відмітити, що в цьому випадку потрібний мінімальний обсяг оперативної пам'яті – всього 8 байт.

Під час шифрування/дешифрування з однократним зверненням до жорсткого диска багатократні операції копіювання в оперативній пам'яті блоків по 8 байт (другий варіант побудови алгоритму) із вихідного буферу, в який завантажується файл, до проміжного і, потім, до результуючого, уповільнюють

даний процес для файлу розміром 80,97 мегабайт всього приблизно на 1 с.

Логічно припустити, що зміна розміру файлу, який шифрується, призведе до відповідної зміни часу шифрування. Як бачимо на рисунку 4, послідовне збільшення розміру файлу бази даних з »10 до »100 мегабайт призводить до лінійного збільшення середнього часу шифрування (n=10, P<0,001).

Таблиця 1. Час шифрування та дешифрування файлу бази даних з вихідним розміром 80 969 728 байт

№ іспиту	Час шифрування (с) у випадку:						Час дешифрування у випадку (с)[1]:					
	зчитування та запису файлів[2] блоками по 8 байт – перший варіант побудови алгоритму		зчитування та запису файлів одним блоком байтів з виконанням шифрування в додатковому буфері другий варіант побудови алгоритму		зчитування та запису файлів одним блоком байтів з шифруванням у вихідному буфері третій варіант побудови алгоритму		зчитування та запису файлів блоками по 8 байт перший варіант побудови алгоритму		зчитування та запису файлів одним блоком байтів з виконанням шифрування в додатковому буфері другий варіант побудови алгоритму		зчитування та запису файлів одним блоком байтів з шифруванням у вихідному буфері – третій варіант побудови алгоритму	
	комп. № 1	комп. № 2	комп. №1	комп. № 2	комп. № 1	комп. № 2	комп. № 1	комп. № 2	комп. № 1	комп. № 2	комп. № 1	комп. № 2
1	68,36	117,81	4,81	7,72	3,62	6,69	69,12	118,92	4,72	7,72	3,70	6,66
2	68,62	118,00	4,77	7,73	3,72	6,77	69,50	118,78	4,30	7,59	3,63	6,48
3	68,48	117,67	4,94	7,66	3,66	6,70	70,34	119,09	4,44	7,55	3,67	6,55
4	68,84	117,92	4,91	7,66	3,78	6,55	69,30	118,37	4,30	7,42	3,51	6,70
5	68,59	117,87	4,41	7,56	3,72	6,50	68,38	118,76	4,53	7,34	3,64	6,67
6	68,30	117,19	4,41	7,58	3,64	6,55	69,11	118,99	4,91	7,42	3,78	6,64
7	68,55	117,86	4,38	7,72	3,78	6,48	69,34	118,27	5,05	7,39	3,59	6,67
8	68,51	117,70	4,41	7,53	3,72	6,41	69,22	118,41	4,38	7,53	3,66	6,61
9	68,77	117,84	4,73	7,47	3,62	6,48	69,06	117,59	4,36	7,72	3,48	6,53
10	68,62	117,83	4,87	7,66	3,77	6,47	68,76	118,59	4,47	7,58	3,59	6,44
Середнє	68,57	117,77	4,66	7,63	3,70	6,56	69,21	118,58	4,54	7,53	3,63	6,60
Станд. відх.	0,17	0,23	0,24	0,09	0,06	0,12	0,51	0,44	0,26	0,13	0,09	0,09

Примітки: [1] Blowfish – симетричний алгоритм, тому час шифрування практично дорівнює часу дешифрування.
[2] Тут та далі мається на увазі зчитування з вихідного файлу та запис до результуючого зашифрованого/дешифрованого файлу.

Оскільки Blowfish є симетричним криптоалгоритмом, не потребує доведення твердження, що час дешифрування приблизно буде дорівнювати часу шифрування (див. також табл. 1) і при зміні розміру файлу буде змінюватись приблизно так само лінійно, як зображено на рисунку 4.

Таким чином досягнуті часові показники, наведені в стовпчиках 6–7 та 12–13 таблиці 1, а також зображені на рисунку 4, на наш погляд, достатні для практичного повсякденного використання шифрування/дешифрування таблиць баз даних медичних інформаційних систем. В результаті шифрування/дешифрування, на наш погляд, може використовуватись щонайменше в наступних випадках:

– під час відправлення за допомогою мережі Internet копій або фрагментів (окремих файлів) баз даних з сервера на клієнтський комп'ютер або навпаки за допомогою FTP-протоколу або будь-яким іншим способом;

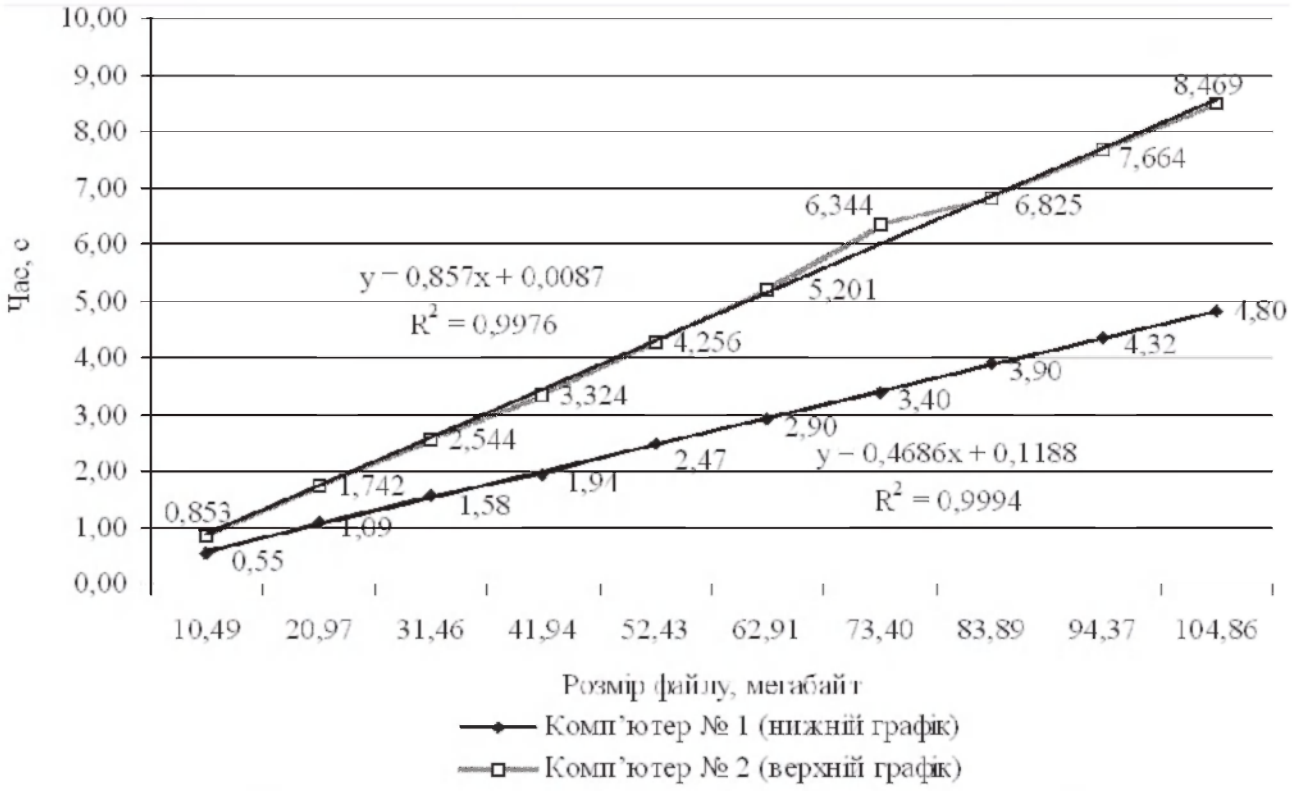

Рис. 4. Залежність середнього часу шифрування файлу від його розміру.

– під час пересилання копій баз даних за допомогою електронної пошти;

– на початку та наприкінці сеансу роботи користувача з базою даних медичної інформаційної системи у випадку зберігання таблиць бази даних в захищеному (зашифрованому) вигляді.

В статті наведені результати досліджень крайніх варіантів – зчитування/запис мінімальних блоків (8 байт) або максимально великих (за розміром файлу). Насправді розмір частки (блоку) файлу, який зчитується за один раз, може варіювати у вказаному діапазоні та часто визначається фактично на розсуд програміста-розробника. Тестові запуски деяких шифрувальних комп'ютерних програм, доступних для завантаження в мережі Internet (наприклад, програма Г. Брауна [19]), свідчать, що розробники вважають за краще використовувати блоки відносно невеликого розміру (>5 мегабайт), але практично ніколи не використовують блоки розміром в декілька байтів (8 та більше), що додатково підтверджує правильність запропонованих в даній статті підходів до прискорення процесів шифрування/дешифрування файлів.

Висновки. 1. В ході виконання даного дослідження була доведена доцільність та практична застосовність методу криптографічного захисту інформації шифрування файлів баз даних медичних інформаційних систем. При цьому було доведено, що відносно великий розмір файлів (десятки та сотні мегабайт) не є критичною перешкодою для успішного та комфортного використання з метою криптографічного захисту інформації шифрувальних комп'ютерних програм або окремих, вбудованих до іншого[1] програмного забезпечення, процедур і функцій.

2. Встановлено, що виконання процедур шифрування/дешифрування в оперативній пам'яті комп'ютера або іншого обчислювального пристрою з одномоментним зчитуванням та наступним одномоментним записом файлу на носій (жорсткий диск) здійснюється значно (приблизно в 10 разів) швидше, ніж у випадку зчитування/запису інформації невеликими блоками, наприклад по 8 байт. При цьому багатократне копіювання блоків інформації, які шифруються/дешифруються, в оперативній пам'яті комп'ютера із вихідного буферу обміну до інших уповільнює швидкість шифрування/дешифрування для файлу розміром 80,97 мегабайт в середньому відповідно на 0,959/0,917 (комп'ютер № 1, $P<0,001$) та 1,07/0,93 с (комп'ютер № 2, $P<0,001$).

[1] Мається на увазі програмне забезпечення медичних інформаційних систем.

Література

1. Информационная безопасность [Электронный ресурс] / созд. Александр Сигачёв ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 3 октября 2004. – Корректируется часто ; послед. корректировка : 31 августа 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Информационная_безопасность. – Загл. с экрана. – Яз. рус.
2. Крипто БД: защита баз данных [Электронный ресурс] / Компания "Аладдин Р.Д.". – Электрон. дан. – [б. м.], [201– ?]. – Режим доступа : http://www.aladdin-rd.ru/catalog/cryptobd/. – Загл. с экрана. – Яз. рус.
3. Шифрование данных в СУБД [Электронный ресурс] / автор admin ; разраб. сайта WordPress. – Электрон. дан. – [б. м.], 2011. – Режим доступа : http://compsmir.ru/?p=118. – Загл. с экрана. – Яз. рус.
4. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI [Електронний ресурс] / Верховна Рада України. – Електрон. дан. – [б. м.], 2010. – Редакція від 09.06.2013. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2297-17. – Загл. з екрану. – Мова укр.
5. Blowfish [Электронный ресурс] / созд. 33.102.141.21 ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 5 декабря 2006. – Корректируется часто послед. корректировка : 20 марта 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Blowfish. – Загл. с экрана. – Яз. рус.
6. IDEA [Электронный ресурс] / созд. 88.214.127.30 ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 23 апреля 2007. – Корректируется часто послед. корректировка : 13 августа 2013г. – Режим доступа : http://ru.wikipedia.org/wiki/IDEA. – Загл. с экрана. – Яз. рус.
7. Twofish [Электронный ресурс] / созд. Nerevar Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 29 июля 2007. – Корректируется часто послед. корректировка : 9 июня 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Twofish. – Загл. с экрана. – Яз. рус.
8. Advanced Encryption Standard [Электронный ресурс] / созд. Gdn Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 16 декабря 2006. – Корректируется часто ; послед. корректировка : 19 августа 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Advanced Encryption Standard. – Загл. с экрана. – Яз. рус.
9. DES [Электронный ресурс] / созд. Xmlx ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 26 января 2006. – Корректируется часто ; послед. корректировка : 1 августа 2013. – Режим доступа : http://ru.wikipedia.org/wiki/DES. – Загл. с экрана. – Яз. рус.
10. Triple DES [Электронный ресурс] / созд. Gdn Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 16 февраля 2007. – Корректируется часто ; послед. корректировка : 8 августа 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Triple DES. – Загл. с экрана. – Яз. рус.
11. RC6 [Электронный ресурс] / созд. Narada Lefvf ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 8 декабря 2007. – Корректируется часто ; послед. корректировка : 19 августа 2013. – Режим доступа : http://ru.wikipedia.org/wiki/RC6. – Загл. с экрана. – Яз. рус.
12. SEED [Электронный ресурс] / созд. Alexanderwdark ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 8 января 2009. – Корректируется часто ; послед. корректировка : 14 марта 2013. – Режим доступа : http://ru.wikipedia.org/wiki/SEED. – Загл. с экрана. – Яз. рус.
13. Camellia (алгоритм) [Электронный ресурс] / созд. 80.73.3.110 ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 17 сентября 2007. – Корректируется часто ; послед. корректировка : 15 июля 2013. – Режим доступа : http://ru.wikipedia.org/wiki/Camellia_(алгоритм). – Загл. с экрана. – Яз. рус.
14. CAST-128 [Электронный ресурс] / созд. Gdn ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 15 января 2007. – Корректируется часто ; послед. корректировка : 13 марта 2013. – Режим доступа : http://ru.wikipedia.org/wiki/CAST-128. – Загл. с экрана. – Яз. рус.
15. XTEA [Электронный ресурс] / созд. Narada Lefvf ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 8 декабря 2007. – Корректируется часто ; послед. корректировка : 30 мая 2013. – Режим доступа : http://ru.wikipedia.org/wiki/XTEA. – Загл. с экрана. – Яз. рус.
16. ГОСТ 28147-89 [Электронный ресурс] / созд. Xchgall ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 13 мая 2005. – Корректируется часто ; послед. корректировка : 19 июля 2013. – Режим доступа : http://ru.wikipedia.org/wiki/ГОСТ_28147-89. – Загл. с экрана. – Яз. рус.
17. Архангельский А. Я. Delphi-6: справочное пособие. – М. : ЗАО «Издательство БИНОМ», 2001. – 1024 с.
18. Чем отличаются CopyMemory и MoveMemory в Delphi? [Электронный ресурс] / созд dvmuratov@yandex.ru. – Электрон. дан. – [б. м.], созд. 2006-12-28. – Корректируется редко ; послед. корректировка : 2006-12-29. – Режим доступа : http://www.delphimaster.net/view/2-1167297116. – Загл. с экрана. – Яз. рус.
19. BlowFish 2000 v3.4 [Электронный ресурс] / Gregory Braun. – Электрон. прикладная прогр. (1 файл) – [б. м.], [20—?]. – Режим доступа : www.gregorybraun.com/BlowFish_Setup.exe. – Загл. со стартовой страницы. – Яз. англ.