

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КРИПТОГРАФІЧНО-ЗАХИЩЕНОГО ЕКСПОРТУ/ІМПОРТУ РЯДКІВ ТАБЛИЦЬ БАЗИ ДАНИХ

Є. Б. Лопін

*Науково-дослідний інститут проблем військової медицини
Української військово-медичної академії*

У статті наведено опис розробленої інформаційної технології криптографічно-захищеного експорту/імпорту інформації таблиць бази даних медичної інформаційної системи, а також результати здійснених за допомогою даної технології експериментів із експорту/імпорту інформації двох баз даних обліку пацієнтів закладів охорони здоров'я Міністерства оборони України. Отримані результати хронометражу експорту/імпорту інформації були зіставлені та порівняні із визначеними можливими щодобовими обсягами експорту/імпорту інформації у двох закладах охорони здоров'я Міністерства оборони України, в результаті чого зроблено висновки про можливість використання розробленої технології у медичних інформаційних системах. Наведено переваги, що забезпечуються шляхом застосування розробленої інформаційної технології. Визначено напрями використання розробленої інформаційної технології для побудови комплексних систем захисту інформації.

Ключові слова: експорт інформації баз даних, імпорт інформації до бази даних, криптографічний захист інформації, медична інформаційна система.

INFORMATION TECHNOLOGY OF CRYPTOGRAPHY-PROTECTED EXPORTS (IMPORTS) OF ROWS OF DATABASE TABLES

Ye. B. Lopin

Military Medicine Problems Research Institute of Ukrainian Military Medical Academy

Background. Despite the recent developments in eastern Ukraine and complicated economic situation in the state, Ukraine Armed Forces Medical Service is introducing medical information systems for informatization of Ukraine Ministry of Defense healthcare facilities functioning and, in particular, is planning the creation of the medical information system of components of defense forces.

At the same time, this project will be performed in low-resource environment with insufficiently developed information infrastructure, shortage of medical service funding and lack of qualified personnel.

This article is devoted to the possible solution of the scientific problem of ensuring functioning of territorially (geographically) and structurally scalable information systems in the absence of direct access to global networks (Internet, etc.) by developing and implementing information technology for cryptographic-protected export/import of databases information.

Materials and methods. Materials used for research: the database of patients registered and classified as combat casualties of the Military Medical Clinical Center of the Southern Region (Odessa) for the period of 2015-2016; the databases of patients registered and treated in the National Military Medical Clinical Center (Kyiv) and the Military Medical Clinical Center of Occupational Pathology of the Ukraine Armed Forces Personnel (Irpın) patients.

For the purposes of this study the developed by the author software and computer equipment that has characteristics similar to the characteristics of the equipment, which is employed in the health facilities of the Ukraine Armed Forces, were utilized.

Results. In order to resolve the research task, the information technology for cryptographically-protected export/import of database tables rows has been developed. The developed information technology is presented as the technological processes of an export and import of information. The description of this technology in a form of a list of stages and the algorithms of information processing is in this article.

The time intervals of execution of the technological processes of export and import of information from the patients' records databases tables of the Ukraine Armed Forces health facilities have been determined with the developed information technology-based software. The results of these experiments, namely, the average time of export and import, is presented in tables in the article.

In order to assess the amount of information that can be exported and imported daily in the medical information system, frequency characteristics of the number of patients who were admitted in the above-mentioned health facilities of the Ukraine Armed Forces.

On the basis of the frequency characteristics data, the ranges of values (the number of admitted patients) that include the maximum value and values, which are most often found in the sample, also have been determined.

© Є. Б. Лопін

Also, in the article the main directions of application of the developed information technology for the construction of integrated information security systems have been considered.

Conclusions. Based on the results of the above studies, conclusions about the advantages and a possibility of daily use of the developed information technology for an export and import of information during functioning of medical information system is formulated.

In particular, the main advantages of the developed information technology are: providing with it the possibility of territorial and structural scaling of medical information systems in the absence of access to global information networks (Internet, etc.); suitability and ease using for the construction of integrated information security systems; ensuring a reduction of dependence of informatization projects in military medicine from a underdeveloped information infrastructure of segregate health facilities or their groups.

Key words: export of database information, import of information into the database, cryptographic protection of information, medical information system.

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ КРИПТОГРАФИЧЕСКИ ЗАЩИЩЁННОГО ЭКСПОРТА / ИМПОРТА СТРОК ТАБЛИЦ БАЗЫ ДАННЫХ

Е. Б. Лопин

*Научно-исследовательский институт проблем военной медицины
Украинской военно-медицинской академии*

В статье приведено описание разработанной информационной технологии криптографически-защищенного экспорта/импорта информации таблиц базы данных медицинской информационной системы, а также результаты проведенных с помощью данной технологии экспериментов по экспорту/импорту информации двух баз данных учета пациентов учреждений здравоохранения Министерства обороны Украины. Полученные результаты хронометража экспорта/импорта информации были сопоставлены и сравнены с определенными возможными ежесуточными объемами экспорта/импорта информации в двух учреждениях здравоохранения Министерства обороны Украины, в результате чего были сделаны выводы о возможности использования разработанной технологии в медицинских информационных системах. Перечислены преимущества, обеспечиваемые за счет применения разработанной информационной технологии. Определены направления использования разработанной информационной технологии для построения комплексных систем защиты информации.

Ключевые слова: экспорт информации базы данных, импорт информации в базу данных, криптографическая защита информации, медицинская информационная система.

Вступ. Незважаючи на події останніх років на сході України та складну економічну ситуацію в країні, в медичній службі Збройних Сил України тривають роботи з впровадження в діяльність закладів охорони здоров'я Міністерства оборони України сучасних інформаційних технологій, зокрема, медичних інформаційних систем (МІС).

Відповідно до завдання 4.2.7 Матриці досягнення стратегічних цілей і виконання основних завдань оборонної реформи Стратегічного оборонного бюлетеня (СОБ) України, схваленого указом Президента України від 06.06.2016 № 240/2016 [1], передбачається створення медичної інформаційної системи складових сил оборони. Враховуючи те, що СОБ був покладений в основу Державної програми розвитку Збройних Сил України на період до 2020 року [1, 2], створення медичної інформаційної системи складових сил оборони на даний час є фактично запланованим.

У той же час, у медичній службі, як і в Збройних Силах України в цілому, існує цілий ряд проблем (повний перелік див. у Концепції інформатизації Міністерства оборони України, далі – Концепція [3]), серед яких слід зазначити:

- недостатній розвиток інформаційної інфраструктури;
- недостатнє фінансування галузі військової охорони здоров'я як у цілому, так і цільове, на потреби інформатизації;
- недостатня кількість або повна відсутність у закладах охорони здоров'я спеціалістів із інформаційних технологій, які мають відповідну освіту.

Відповідно за таких умов створення та впровадження територіально (географічно), функціонально та структурно масштабованих інформаційних систем, особливо побудованих за клієнт-серверною архітектурою, вимагатиме застосування

економічно обґрунтованих, а іноді – й нестандартних компромісних технічних рішень.

Можливим шляхом зменшення впливу ризиків на процес створення, впровадження та функціонування медичних інформаційних систем і, в тому числі, МІС складових сил оборони, є забезпечення здатності МІС до повноцінного функціонування та масштабування за відсутності локальних обчислювальних мереж, а також відсутності прямого доступу до глобальної мережі Інтернет або подібних.

Враховуючі те, що переважна більшість МІС базується на технологіях баз даних і передбачають використання певної системи управління базами даних (СУБД), здатність МІС до функціонування та обміну даних за відсутності доступу до мереж може бути досягнута за допомогою спеціальних прикладних інформаційних технологій, наприклад, інформаційної технології криптографічно-захищеного експорту/імпорту рядків таблиць локальної бази даних.

Мета дослідження: дослідження можливості вирішення наукової проблеми забезпечення функціонування територіально та структурно масштабованих медичних інформаційних систем в умовах відсутності прямого доступу до глобальних мереж (Інтернет або інш.)

Матеріали та методи дослідження. Для проведення даного дослідження використовувалось розроблене в ліцензійному середовищі програмування Delphi 7 прикладне програмне забезпечення (комп'ютерна програма "MilitaryCasualties", впроваджена наказом директора Військово-медичного департаменту Міністерства оборони України від 19.05.2015 р. № 31 тощо). Для реалізації функцій криптографічного захисту інформації під час проведення експериментів була використана програмна реалізація [4] незапатентованого та дозволеного для вільного використання симетричного криптографічного алгоритму Blowfish [5].

Для виконання тестувань та визначення швидкості роботи (хронометражу) процедур експорту та імпорту використовувались 3 комп'ютери такої конфігурації:

№ 1 – процесор DualCore Intel Celeron E1200, системна пам'ять 1014 Мб, операційна система Microsoft Windows XP Professional (Service Pack 3), спеціальне захисне програмне забезпечення – ESET Smart Security;

№ 2 – процесор Intel Core 2 Duo E8400, системна пам'ять 3584 Мб, операційна система Microsoft Windows XP Professional (Service

Pack 3), спеціальне захисне програмне забезпечення – Norton Internet Security;

№ 3 – Dell OptiPlex 780, процесор Intel Core 2 Duo E8500, системна пам'ять 3968 Мб, операційна система Microsoft Windows 7 Professional (Service Pack 1), спеціальне захисне програмне забезпечення – Dr.Web Security Space.

Для проведення дослідження використовувались такі локальні бази даних:

- база даних облікованих у Військово-медичному клінічному центрі Південного регіону (м. Одеса) протягом 2015-2016 років пацієнтів, віднесених до категорії бойових втрат;
- бази даних обліку пролікованих пацієнтів Національного військово-медичного клінічного центру «ГВКГ» (НВМКЦ «ГВКГ») та Військово-медичного клінічного центру професійної патології особового складу збройних Сил (ВМКЦ ППОС).

Стисла характеристика зазначених баз даних (БД) та отриманих із них вибірових даних, що використовувались для експериментів, наведено в табл. 1.

Дослідження виконувалось наступним чином: 10 разів до 10 файлів (1.bak, 2.bak ... 10.bak) здійснювався експорт рядків стосовно 50 (100, 150 ... 500) пацієнтів, після чого з кожного файлу (10 файлів – 10 разів) здійснювався імпорт до попередньо очищеної бази даних.

Для визначення типового обсягу експорту/імпорту даних на практиці було проведено визначення частотних характеристик потоку надходження пацієнтів до НВМКЦ «ГВКГ» та ВМКЦ ППОС на основі накопичених в інформаційних системах даних закладів облікових даних:

- з 01.01.2014 до 31.08.2017 для НВМКЦ «ГВКГ» (надійшло 114 769 пацієнтів);
- з 01.01.2014 до 10.07.2017 для ВМКЦ ППОС (надійшло 29 952 пацієнтів).

Під час створення частотної характеристики для укрупнення інтервалів використовувалась формула Стерджеса (Herbert Arthur Sturges) [6].

Результати та їх обговорення. В травні 2015 року пунктом 7 рішення Ради національної безпеки і оборони України від 6 травня 2015 року, введеним у дію указом Президента України від 26 травня 2015 року № 285/2015, Міністерству оборони України в двотижневий строк було доручено створити автоматизовану базу даних обліку військовослужбовців Збройних Сил України, інших утворених відповідно до законів України

Таблиця 1

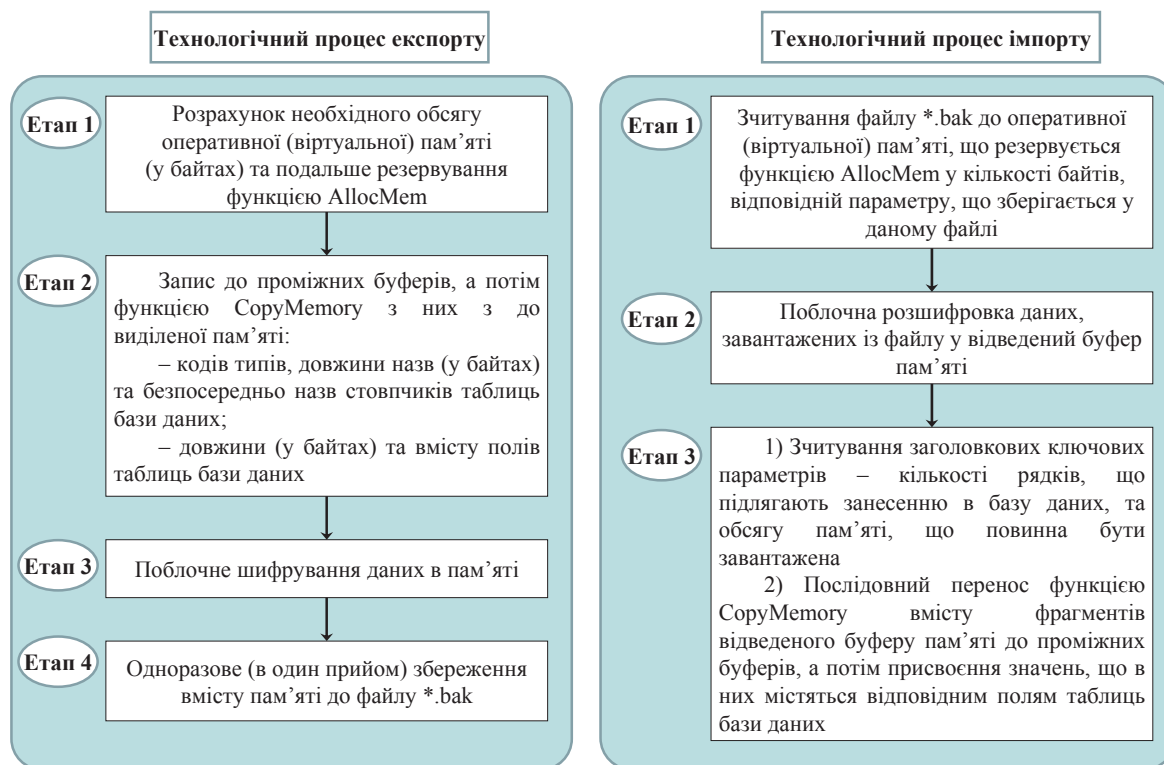
Характеристика баз даних та отриманих із них вибірових даних

База даних	Формат бази даних	Драйвера, що використовувались	Кількість таблиць, що використовуються для зберігання даних	Кількість стовпчиків у таблицях	Обсяг вибірки, пацієнтів	Середній обсяг даних про 1 пацієнта, байт
1	2	3	4	5	6	7
БД поранених ВМКЦ Південного регіону	Paradox 7	Borland Database Engine	2	58 та 4	500	2311
БД обліку пацієнтів НВМКЦ «ГВКГ»	Microsoft Access	ActiveX Data Objects (Microsoft.-Jet. OLE-DB.4.0)	1	85	500	1930

військових формувань, що були поранені, контужені або отримали каліцтво під час участі в анти-терористичній операції [7, 8].

Враховуючи вкрай стислі терміни для виконання даного завдання було вирішено створити зазначену автоматизовану базу даних на основі географічно

віддалених однотипних, прямо не підключених до мереж, локальних робочих місць, об'єднаних в інформаційну систему за допомогою інформаційної технології криптографічно-захищеного експорту/імпорту даних.

Рис. 1. Етапи технологічних процесів експорту та імпорту¹

¹ Тут і далі використовуються назви функцій, що застосовуються в середовищі програмування Delphi.

Для реалізації даного підходу була розроблена комп'ютерна програма "MilitaryCasualties", що під час серії відряджень була розповсюджена та впроваджена по закладам охорони здоров'я Міністерства оборони України. Окрім цього з дослідницькою метою додатково розроблено інше програмне забезпечення.

Відповідно до описаних у літературі підходів [9, 10] інформаційну технологію експорту/імпорту записів (рядків) таблиць бази даних, що є компонентом розробленого програмного забезпечення, можна представити у вигляді технологічних процесів, які розподіляються на етапи, а ті у свою чергу – на операції.

Технологічними процесами в даному випадку будуть (рис. 1):

- технологічний процес експорту рядків (кортежів) таблиць бази даних до зашифрованого файлу (далі технологічний процес експорту);

- технологічний процес імпорту рядків (кортежів) таблиць бази даних із зашифрованого файлу (технологічний процес імпорту).

У тексті розробленого програмного забезпечення (комп'ютерної програми "MilitaryCasualties" та іншого) технологічні процеси криптографічно захищеного експорту та імпорту представлені процедурами Delphi, алгоритми та принципи роботи яких наведені на рис. 2 та рис. 3.

Під час експорту можливі два варіанти розрахунку пам'яті – окремо, на 1 етапі (рис. 1), перед початком усіх операцій, або послідовне збільшення початкового буферу по мірі зчитування даних із таблиць (наприклад, функцією Delphi ReallocMem).

Середній час виконання технологічних процесів експорту та імпорту для різних обсягів даних наведений у табл. 2.

Обсяг інформації, що щоденно накопичується МІС, та, відповідно, підлягатиме експорту

Таблиця 2

Середній час виконання технологічних процесів експорту та імпорту¹

Середній час виконання технологічного процесу	Кількість пацієнтів, дані про яких експортуються та імпортуються									
	50	100	150	200	250	300	350	400	450	500
1	2	3	4	5	6	7	8	9	10	11
Комп'ютер № 1, база даних обліку поранених ВМКЦ Південного регіону										
експорту	2,77	5,51	7,97	10,44	12,89	15,33	17,95	20,47	23,11	25,82
імпорту	4,95	9,26	13,46	17,97	23,03	27,37	31,89	35,90	40,49	45,13
Комп'ютер № 2, база даних обліку поранених ВМКЦ Південного регіону										
експорту	1,26	2,54	3,67	4,80	5,94	7,10	8,23	9,31	10,48	11,67
імпорту	2,37	4,30	6,13	8,04	9,92	11,73	13,54	15,21	17,06	19,09
Комп'ютер № 1, база даних обліку пацієнтів НВМКЦ «ГВКГ»										
експорту	0,35	0,69	0,80	0,90	1,01	1,11	1,23	1,34	1,45	1,59
імпорту	1,39	1,92	2,26	2,68	3,06	3,57	3,94	4,38	4,86	5,20
Комп'ютер № 2, база даних обліку пацієнтів НВМКЦ «ГВКГ»										
експорту	0,16	0,30	0,38	0,49	0,60	0,71	0,80	0,88	1,06	1,20
імпорту	0,89	1,13	1,32	1,50	1,61	1,80	2,00	2,19	2,39	2,56
Комп'ютер № 3, база даних обліку пацієнтів НВМКЦ «ГВКГ»										
експорту	0,22	0,42	0,52	0,61	0,71	0,81	0,90	1,01	1,12	1,23
імпорту	1,25	1,41	1,55	1,73	2,03	2,32	2,60	2,62	2,80	3,05

¹ Часові показники експорту та імпорту, наведені в таблиці, були отримані під час експорту з таблиць, що містили лише експортовані рядки, та імпорту в попередньо очищені таблиці бази даних. У випадку таблиці, що містить, наприклад, 490 тис. рядків, час експорту та імпорту значно збільшується, але це збільшення обумовлено особливостями роботи драйверів баз даних

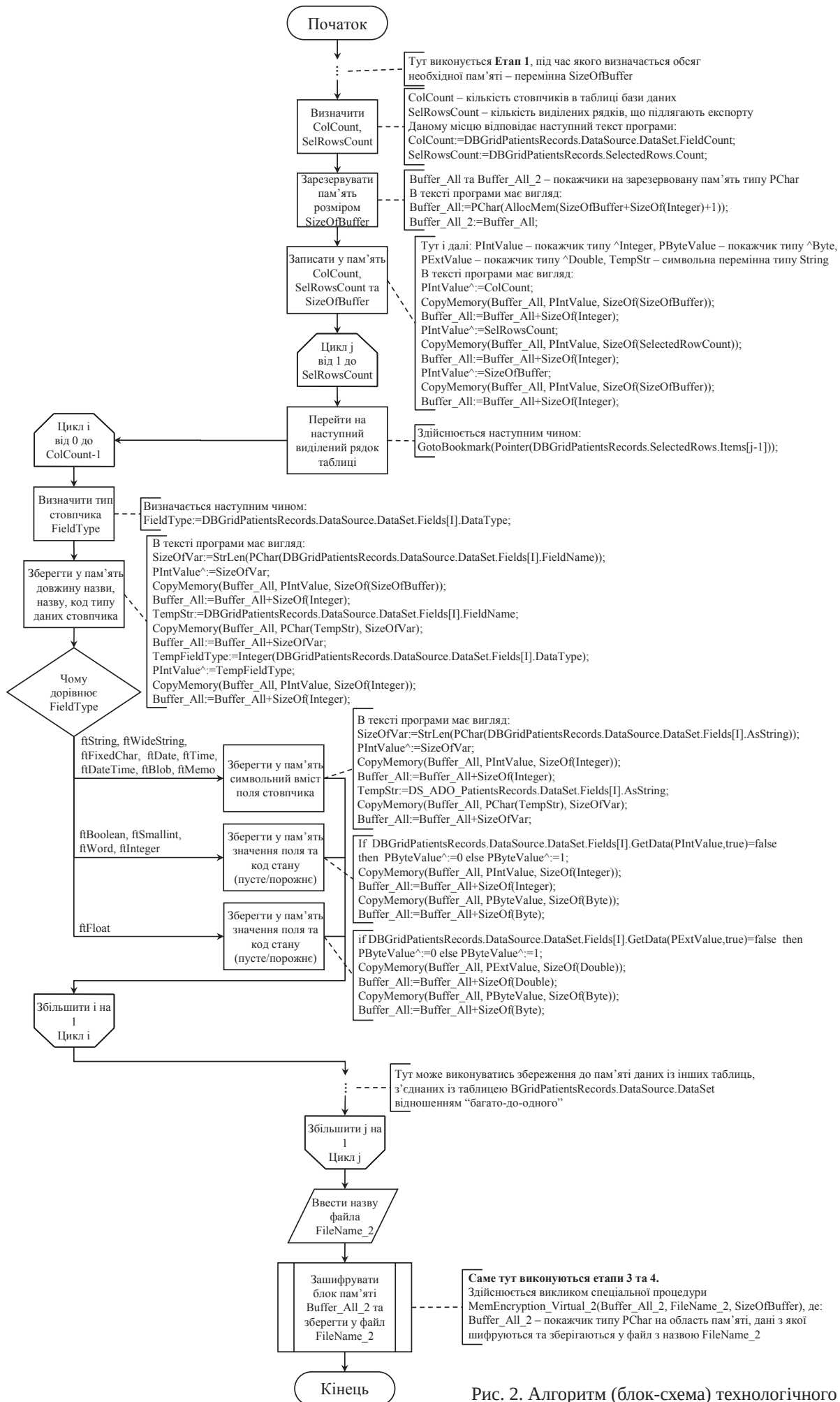


Рис. 2. Алгоритм (блок-схема) технологічного процесу експорту (варіант)

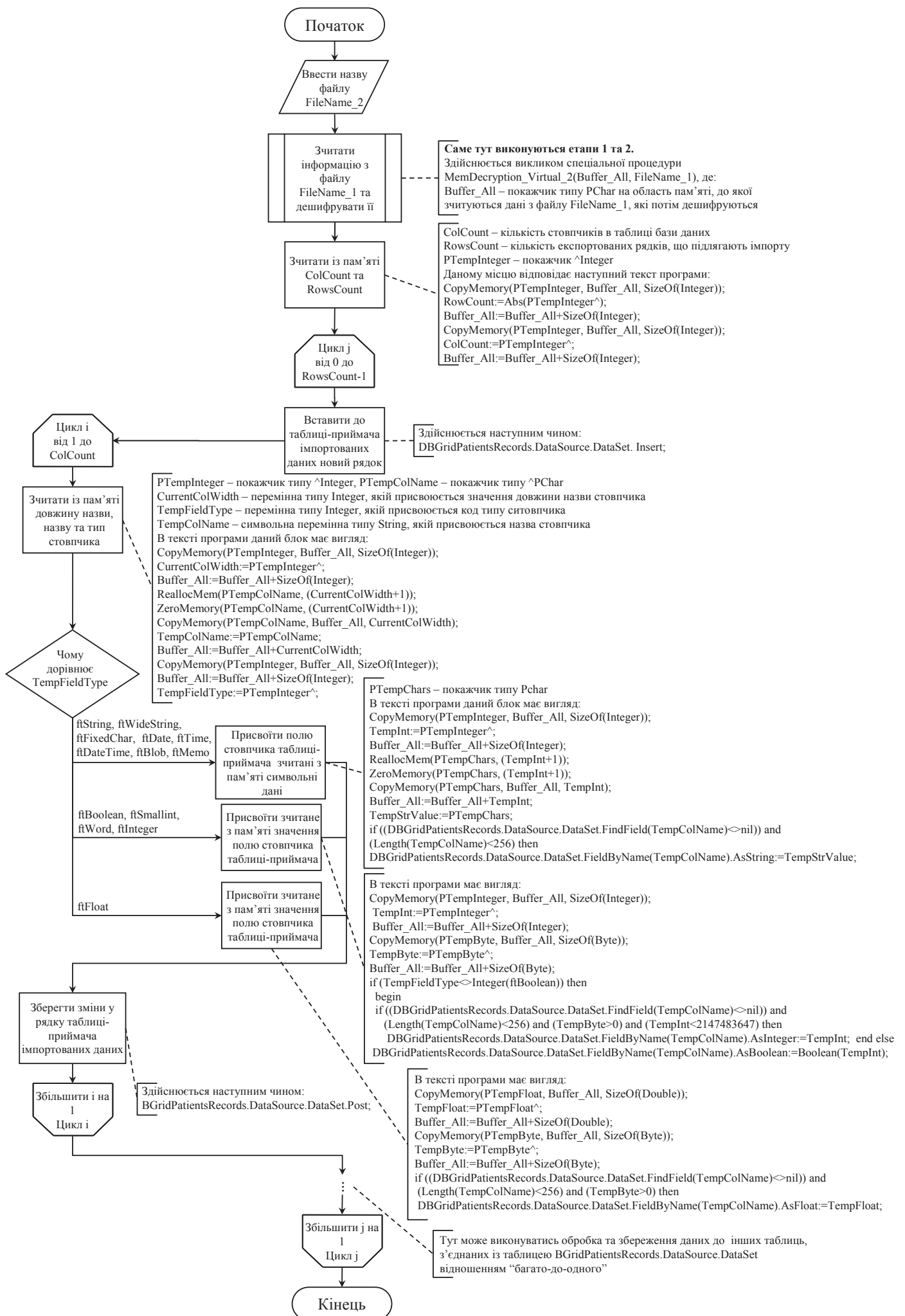


Рис. 3. Алгоритм (блок-схема) технологічного процесу імпорту (варіант)

та імпорту, може бути оцінений за допомогою частотних показників вхідного потоку пацієнтів до закладів охорони здоров'я Міністерства оборони України. Частотні характеристики вхідного потоку пацієнтів до НВМКЦ «ГВКГ», що є найбільшим закладом у медичній службі Збройних Сил України, та ВМКЦ ППОС наведено на рис. 4.

Відповідно до рис. 4 до НВМКЦ у робочі дні тижня найбільш часто надходила кількість пацієнтів в інтервалі від 91 до 112, максимальна кількість госпіталізованих пацієнтів склала 254. Кількість госпіталізованих пацієнтів до ВМКЦ ППОС була значно меншою та складала більше 83 пацієнтів лише в 4 випадках (157, 129, 183 та 199 пацієнтів відповідно 01.07.2014, 01.07.2015, 04.07.2016 та 03.07.2017), коли заклад приймав на обстеження кандидатів на навчання в Українській військово-медичній академії.

Відповідно до даних, наведених у табл. 1 та на рис. 4, можна зробити висновок, що часові показники експорту та імпорту даних за допомогою розробленої інформаційної технології мають прийнятну величину та негативно не вплинуть на функціонування медичної інформаційної системи.

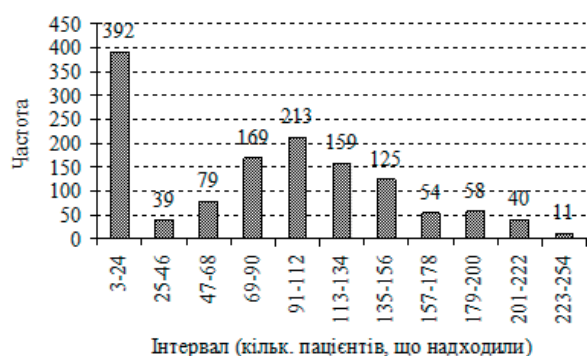
За час експлуатації комп'ютерної програми "MilitaryCasualties" було встановлено ряд переваг розробленої інформаційної технології і, в тому числі, наведених на рис. 2 та рис. 3 алгоритмів:

- алгоритми роботи процедур експорту та імпорту фактично не прив'язані до формату таблиць бази даних, так як їх робота базується на використанні властивостей та методів візуальних компонентів Delphi, згідно яких для об'єктів, наприклад, типу TTable (TDataSet), можливе представлення вмісту полів таблиць бази даних

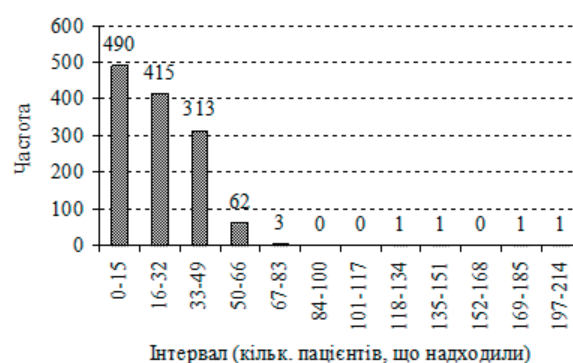
у вигляді стандартних типів даних (синтаксичні конструкції ...AsString, ...AsInteger, ...AsFloat, ...AsVariant тощо);

- алгоритми дозволяють використовувати у вигляді модулів включені процедури або функції, призначені для криптографічного захисту інформації [4], перевагою даного підходу є можливість використовувати програмні реалізації практично всіх відомих у світі криптографічних алгоритмів, призначених для захисту інформації [11];
- після незначної модифікації програмного коду за допомогою процедур експорту та імпорту можна здійснювати конвертацію даних із одного формату баз даних до іншого (наприклад, конвертацію з формату Paradox 7 до формату MySQL), у цьому випадку створювані під час технологічного процесу експорту файли являються універсальним проміжним сховищем-шлюзом;
- запропоновані технічні рішення дозволяють зменшити залежність від мережевих комунікацій та забезпечують можливість автономної роботи із географічно дистанційно розташованою базою даних в умовах недоступності прямого підключення до глобальної мережі (Інтернет або інш.);
- технологічні процеси експорту та імпорту дозволяють організувати автоматизоване часткове або повне резервне копіювання бази даних, внаслідок чого можна суттєво підвищити захист інформації в МІС.

Можливість використовувати розроблену технологію для побудови комплексних систем захисту інформації (КСЗІ) для МІС заслуговує на особливу



НВМКЦ «ГВКГ»



ВМКЦ ППОС

Рис. 4. Частотні характеристики вхідного потоку пацієнтів до НВМКЦ «ГВКГ» та ВМКЦ ППОС (з укрупненням інтервалів)

увагу. Як відомо, відповідно до нормативних документів із питань технічного захисту інформації в Україні до комп'ютерних систем висуваються вимоги можливості забезпечення так званого відкату та відновлення після збоїв [12]. При цьому комплекс засобів захисту інформації (КЗЗ) навіть технічно найпростіших автоматизованих інформаційних систем Класу «1» (одномашинний однокористувачевий комплекс, що обробляє інформацію однієї або кількох ступенів обмеження доступу [13]), повинний відповідно до стандартних функціональних профілів захищеності [13] забезпечувати відповідність мінімальним критеріям захищеності інформації, що характеризують можливість відкату та відновлення системи після збоїв.

Оскільки за допомогою запропонованої технології автоматизовано створюється придатна для зворотного завантаження повна або часткова копія бази даних, розроблена технологія дозволяє КЗЗ комп'ютерної системи досягнути відповідності критерію відкату ЦО-2 ("Повний відкат"). Окрім цього дана технологія може бути використана як компонент КЗЗ інформації, що забезпечуватимуть відповідність комп'ютерної системи критеріям відновлення після збоїв ДВ-1 ("Ручне відновлення"), ДВ-2 ("Автоматизоване відновлення") або ДВ-3 ("Вибіркове відновлення").

Окрім цього технологія може бути використана для забезпечення відповідності КЗЗ комп'ютерної системи критеріям конфіденційності.

Висновки. За результатами проведеного дослідження було встановлено:

- розроблена прикладна технологія експорту/імпорту даних дозволяє створювати МІС шляхом організації зв'язку між географічно віддаленими окремими робочими місцями та, відповідно, дозволяє здійснювати територіальне та структурне масштабування МІС в умовах відсутності прямого доступу до глобальних мереж (Інтернет або подібні);
- розроблена прикладна технологія експорту/імпорту даних може бути використана для побудови КСЗІ МІС;
- доведено можливість реалізації у закладах охорони здоров'я Збройних Сил України електронного обліку госпіталізованих пацієнтів при мінімальних економічних затратах, що особливо актуально в умовах відсутності фінансування та недостатнього розвитку інформаційної інфраструктури.

Література.

1. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президента України від 6 червня 2016 року № 240/2016 [Електронний ресурс] / Президент України. – Електрон. дан. – [б. м.], [20—?]. – Редакція від 06.06.2016. – Режим доступу : <http://zakon.rada.gov.ua/laws/show/240/2016/paran10#n10>. – Загол. з екрану. – Мов. укр.
2. Про Державну програму розвитку Збройних Сил України на період до 2020 року : рішення РНБО України від 29 грудня 2016 року, введене в дію Указом Президента України від 22 березня 2017 року № 73/2017 [Електронний ресурс] / РНБО України. – Електрон. дан. – [б. м.], 2016. – Редакція від 24.03.2017. – Режим доступу : <http://zakon.rada.gov.ua/laws/show/n0017525-16/paran2#n2>. – Загол. з екрану. – Мов. укр.
3. Про затвердження Концепції інформатизації Міністерства оборони України : Наказ Міністра оборони України від 17.09.2014 № 650 [Електронний ресурс] / МО України. – Концепція інформатизації МОУ (1 файл). – К., 2014. – Режим доступу: http://www.mil.gov.ua/content/other/MOU650_2014.pdf. – Загол. з файлу. – Мова укр.
4. Лопін Є. Б. Аналіз часових показників шифрування/дешифрування файлів баз даних медичних інформаційних систем / Є. Б. Лопін // Медична інформатика та інженерія. – 2013. – № 4. – С. 28-35.
5. Blowfish [Електронний ресурс] / созд. 83.102.141.21; Wikimedia Foundation, Inc. – Електрон. 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. Основы математической статистики: Учебное пособие для ин-тов физ. культ. / Под ред. В. С. Иванова. – М.: Физкультура и спорт, 1990. – 176 с., ил.
7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про стан виконання рішень Ради національної безпеки і оборони України та додаткові заходи щодо забезпечення обороноздатності держави": Указ Президента України від 26 травня 2015 року № 285/2015 [Електронний ресурс] / Президент України. – Електрон. дан. – [б. м.], [20—?]. – Редакція від 26.05.2015. – Режим доступу:

- <http://zakon.rada.gov.ua/laws/show/285/2015>. – Загол. з екрану. – Мов. укр.
8. Про стан виконання рішень Ради національної безпеки і оборони України та додаткові заходи щодо забезпечення обороноздатності держави : рішення Ради національної безпеки і оборони України від 6 травня 2015 р. [Електронний ресурс] / РНБО України. – Електрон. дан. – [б. м.], [20—?]. – Редакція від 28.05.2015. – Режим доступу : <http://zakon.rada.gov.ua/laws/show/n0007525-15/paran2#n2>. – Загол. з екрану. – Мов. укр.
 9. Козырев А. А. Информационные технологии в экономике и управлении: Учебник / А. А. Козырев. – 3-е изд., перераб. и доп. – СПб: Михайлов В. А., 2003. – 496 с.
 10. Технологический процесс [Электронный ресурс] / созд. Тривvvikky ; Wikimedia Foundation, Inc. – Электрон. дан. – [б. м.], созд. 2 октября 2009. – Корректируется часто ; послед. корректировка : 27 марта 2016. – Режим доступа : https://ru.wikipedia.org/wiki/Технологический_процесс. – Загл. с экрана. – Яз. рус.
 11. Delphi Encryption Compedium Part I v.3.0 [Электронный ресурс] / Hagen Reddmann. – Электрон. дан. – [б. м.], [20—?]. – Редакция от 31 Aug 1999. – Режим доступа : <http://torry.net/authorsmore.php?id=1881>. – Загол. с экрана. – Яз. англ.
 12. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу” [Електронний ресурс] / Держспецзв’язку України. – НД ТЗІ (1 файл). – [б. м.], [20—?]. – Режим доступу : <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>. – Загол. із сторінки “Інформаційний перелік Фонду НД ТЗІ та КЗІ” (“http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id=89734”). – Мова укр.
 13. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” [Електронний ресурс] / Держспецзв’язку України. – Електрон. дані. – [б. м.], [20—?]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?jsessionid=5510AAB9DB971D6B6F895BBA3ECD8BAD.app1?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407. – Загол. з екрану. – Мова укр.
 - “On the Strategic Defense Bulletin of Ukraine”]. (n.d.). Retrieved from <http://zakon.rada.gov.ua/laws/show/240/2016/paran10#n10> [in Ukrainian].
 2. Rishennia RNBO Ukrainy vid 29 hrudnia 2016 roku, vvedene v diiu Ukazom Prezydenta Ukrainy vid 22 bereznia 2017 roku № 73/2017 “Pro Derzhavnu prohramu rozvytku Zbroinykh Syl Ukrainy na period do 2020 roku” [The decision of the National Security and Defense Council of Ukraine dated December 29, 2016, put into effect by the Decree of the President of Ukraine dated March 22, 2017 No. 73/2017 “On the State Program for the Development of the Armed Forces of Ukraine for the period up to 2020”]. (n.d.). Retrieved from <http://zakon.rada.gov.ua/laws/show/n0017525-16/paran2#n2> [in Ukrainian].
 3. Nakaz Ministra oborony Ukrainy vid 17.09.2014 № 650 “Pro zatverdzhennia Kontseptsii informatyzatsii Ministerstva oborony Ukrainy” [Order of the Minister of Defense of Ukraine No. 650 dated 17.09.2014 “On Approval of the Concept of Informatization of the Ministry of Defense of Ukraine”]. (n.d.). Retrieved from http://www.mil.gov.ua/content/other/MOU650_2014.pdf [in Ukrainian].
 4. Lopin, Ye.B. (2013) Analiz chasovykh pokaznykiv shyfruvannia/deshyfruvannia failiv baz danykh medychnykh informatsiinykh system [Analysis of time distances of encryption/decryption of medical information systems databases files]. Medychna informatyka ta inzheneriia – Medical Informatics and Engineering, 4, 28-35 [in Ukrainian].
 5. Blowfish [Descr. of cryptographic algorithm]. (December 5, 2006). Retrieved from <http://ru.wikipedia.org/wiki/Blowfish> [in Russian].
 6. Ivanov, V.S. (Eds.), (1990). Osnovy matematicheskoy statistiki: Uchebnoe posobie dlya in-tov fiz. kul’t. [Fundamentals of mathematical statistics: Textbook for institutes of physical culture]. Moscow: Fizkul’tura i sport [in Russian].
 7. Ukaz Prezydenta Ukrainy vid 26 travnia 2015 roku № 285/2015 “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku “Pro stan vykonannia rishen Rady natsionalnoi bezpeky i oborony Ukrainy ta dodatkovy zakhody shchodo zabezpechennia oboronozdatnosti derzhavy” [Decree of the President of Ukraine dated May 26, 2015, No. 285/2015 “On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 “On the state of implementation of the decisions of the National Security and Defense Council of Ukraine and additional measures to ensure the defense of the state”]. (n.d.). Retrieved from <http://zakon.rada.gov.ua/laws/show/285/2015> [in Ukrainian].
 8. Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 r. “Pro stan vykonannia rishen Rady natsionalnoi bezpeky i oborony Ukrainy ta dodatkovy zakhody shchodo zabezpechennia oboronozdatnosti

References.

1. Ukaz Prezydenta Ukrainy vid 6 chervnia 2016 roku № 240/2016 “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 travnia 2016 roku “Pro Stratehichniy oboronnyi biuleten Ukrainy” [Decree of the President of Ukraine dated June 6, 2016 No. 240/2016 “On the decision of the National Security and Defense Council of Ukraine dated May 20, 2016,

- derzhavy” [The decision of the National Security and Defense Council of Ukraine dated May 6, 2015 “On the state of implementation of the decisions of the National Security and Defense Council of Ukraine and additional measures to ensure the defense capability of the state”]. (n.d.). Retrieved from <http://zakon.rada.gov.ua/laws/show/n0007525-15/paran2#n2> [in Ukrainian].
9. Kozyrev, A.A. (Eds.), (2003). *Informacionnye tekhnologii v ehkonomie i upravlenii: Uchebnik*. [Information Technologies in Economics and Management: A Textbook]. Saint Petersburg: Izd-vo Mihajlova V.A. [in Russian].
 10. Tekhnologicheskij process [Technological process]. (October 2, 2009). Retrieved from https://ru.wikipedia.org/wiki/Технологический_процесс [in Russian].
 11. Delphi Encryption Compendium Part I v.3.0. (n.d.). Retrieved from <http://torry.net/authorsmore.php?id=1881> [in English].
 12. ND TZI 2.5-004-99 “Kryterii otsinky zakhyschenosti informatsii v komp’iuternykh systemakh vid nesanktsionovanoho dostupu” [Normative document on technical protection of information 2.5-004-99 “Criteria for assessing the security of information in computer systems from unauthorized access”]. (n.d.). Retrieved from <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342> [in Ukrainian].
 13. ND TZI 2.5-005-99 “Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhyschenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu” [Normative document on technical protection of information 2.5-005-99 “Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access”]. (n.d.). Retrieved from http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?jsessionid=5510AAB9DB971D6B6F895BBA3ECD8BAD.app1?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 [in Ukrainian].