2. Malikov, N. V., Bogdanov, N. V., Kuznetsov, A. A. (2005). The use of new computer technologies in otsenkefunktsionalnoy preparedness and functional state of an organism. Slobozhanskiynaukovo-sportivniyvisnik, 8, 237–240.

3. Vovk, V. M. (2002). Automated diagnostic systems control the physical condition of students. Pedagogika, psihologiya that health biologichni fizichnogo vihovannya problemi i Sport, 9, 82–89.

4. Sergienko, K. N. (2005). Interactive computer monitoring the level of physical development and health of school children Ukraine. Olympic Sport and Sport for All. Kiev, 280.

5. Kashuba, V., Khmelnitska, I. (2007). The Biovideo Software for Biomechanical Analysis of Human Movement. Proceedings of 12th Annual Congress of the European College of Sport Science. Jyväskylä, 67–69.

6. Landa, B. H. (2005). Methodology of comprehensive assessment of physical development and physical preparedness. Moscow: Soviet Sport, 192.

7. Izaak, S. I. (2005). Monitoring of physical development and physical preparedness. Soviet Sport, 196.

*Рекомендовано до публікації д-р техн. наук, професор Лисенко О. І.*
*Дата надходження рукопису 20.05.2015*

**Антонова-Рафі Юлія Валеріївна**, кандидат технічних наук, доцент, кафедра біобезпеки і здовов'я людини, Національний Технічний Університет України «Київський Політехнічний Інститут», пр. Перемоги, 37, м. Київ, Україна, 03056
E-mail: unes04@mail.ru
**Нікітенко Микита Віталійович**, кафедра біобезпеки і здовов'я людини, Національний Технічний Університет України «Київський Політехнічний Інститут», пр. Перемоги, 37, м. Київ, Україна, 03056
E-mail: nikitenko.nikita.v@gmail.com

**УДК 004.056**
**DOI: 10.15587/2313-8416.2015.44361**

# МОДЕЛЬ СОЦІАЛЬНОЇ КРИПТО-МЕРЕЖІ

**© М. М. Орел**

*В роботі представлена теоретична модель соціальної мережі з посиленим механізмом захисту конфіденційності. Розглянуті проблеми, які виникають при побудові такого типу мережі. Наведені методи вирішення проблем, що виникають при побудові захищеної соціальної мережі. Побудована теоретична модель соціальної мережі з посиленими методами захисту інформації на основі інформаційно-комунікаційних блоків*
***Ключові слова:*** *соціальна мережа, криптографія, конфіденційність інформації, інформаційна безпека, захист персональних даних*

*The article presents the theoretical model of social network with the enhanced mechanism of privacy policy. It covers the problems arising in the process of implementing the mentioned type of network. There are presented the methods of solving problems arising in the process of building the social network with privacy policy. It was built a theoretical model of social networks with enhanced information protection methods based on information and communication blocks*
***Keywords:*** *social network, cryptography, confidentiality of information, infoemation security, protection of personal data*

## 1. Вступ

На сьогодні соціальні мережі є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною, так і конфіденційною інформацією. Проте зі зростанням об'ємів інформації, зростає й загроза порушення однієї найважливішої властивості – конфіденційності. Кількість випадків хакерських атак значно зросла не лише на інтернет-ресурси, а й на електронні поштові скриньки журналістів і громадських активістів з метою отримати доступ до їхніх комп'ютерів і встановити контроль над листуванням, абощо? Не винятком залишаються і найпоширеніший інструмент обміну інформацією – соціальні мережі.

## 2. Постановка проблеми

Соціальні мережі стали невід'ємною частиною життя майже кожного користувача Інтернету. Їхні основні функції розширились зі звичайного обміну повідомленнями до всезагальних обговорень, Інтернет комерції, і навіть широко використовуються як основний інструмент в інформаційних війнах. Саме тому збереження конфіденційності, тобто забезпечення інформаційної безпеки в соціальних мережах, є актуальним на сьогодні.

Соціальна мережа (англ. Social network) як об'єднання соціальних позицій – соціальних акторів (люди або організації) та їх зв'язків – це основне, загальноприйняте визначення даного поняття. Соціальна мережа (математично – соціальний граф) складається з групи вузлів, якими є соціальні актори, і зв'язків між ними (соціальних взаємодій) з приводу обміну ресурсами. Таким чином, в рамках соціальної мережі соціальні актори групуються на основі подібності займаних позицій, зв'язків і

за типом ресурсів, циркулюючих між даними позиціями [1].

На даний момент існують засоби для забезпечення властивості конфіденційності інформації при обміні та зберіганні. Серед них – криптографія, технічні методи захисту інформації, організаційні методи, тощо. Проте, переважна більшість існуючих моделей мереж не враховує того фактору, що їхні сховища даних можуть бути вилучені чи викрадені під час певних фізичних атак, що спричинить чимале порушення цілісності та конфіденційності інформації, яка міститься на цих сховищах. Виходячи з даної інформації, метою дослідження є аналіз комунікаційних моделей в існуючих соціальних мережах та розробка моделі захищеної комунікації в соціальній мережі.

Для досягнення поставленої мети в дипломній роботі були та вирішені наступні завдання:

– аналіз існуючих моделей соціальних мереж та виокремлення основних інформаційно-комунікаційних блоків;

– розробка алгоритмів функціонування інформаційних блоків.

Глибока теоретична і логічна оцінка проблеми, аналіз об'єкта дослідження дозволяє забезпечити умови для створення теоретичної моделі, тобто сформулювати теоретичні положення про взаємозв'язок та взаємообумовленість її параметрів.

**2. Літературний огляд**

У статті 2011 року [2], Jan H. Kietzmann, Kristopher Hermkens, Ian P. McCarthy та Bruno S. Silvestre виділили наступні структурні елементи соціальних мереж (рис. 1).


Рис. 1. Усі компоненти соціальної мережі у вигляді "медової соти"

Ідентичність: Цей блок являє собою секцію, в якій користувач може проявити свою індивідуальність в соціальному середовищі засобів масової інформації. Це може включати в себе розкриття інформації, такої як ім'я, вік, стать, професія, місце роботи, а також інформації, яка відображує користувачів в певних відносинах.

Бесіди: Цей блок являє собою секцію, в якій користувач може спілкуватися з іншими користувачами в соціальному середовищі засобів масової інформації. Багато сайтів соціальних медіа в першу чергу призначені для полегшення бесіди серед окремих осіб та груп. Ці розмови відбуваються з різних причин. Люди твітять, пишуть блоги, і тому подібне, щоб познайомитися з однодумцями, щоб знайти справжню любов, щоб покращити свою самооцінку, або щоб бути у тренді нових ідей чи трендових темах. Інші бачать соціальні медіа як спосіб зробити їх повідомлення почутими: щодо різних гуманітарних проблем, економічних негараздів чи навіть політичних дебатів.

Обмін: Цей блок являє собою секцію, в якій користувачі обмінюються, поширюють і отримують контент. В термін «соціальний» часто вкладається поняття обміну, яке несе вирішальне значення.

Присутність : Цей блок являє собою секцію, в якій користувачі можуть знати, чи є інші користувачі доступними. Це включає в себе знання, де перебувають інші користувачі - у віртуальному світі, чи в реальному світі, і чи будуть вони доступними [2].

Стосунки : Цей блок представляє секцію, в якій користувачі можуть бути пов'язані з іншими користувачами. Двоє або більше користувачів мають деяку форму асоціації, що приводить їх до розмов, обміну об'єктами соціальності, зустрічей, або просто рахувати (вважати) один одного другом чи фаном [2].

Репутація: Цей блок являє собою секцію, в якій користувачі можуть ідентифікувати положення інших, у тому числі себе, в соціальному середовищі засобів масової інформації. Репутація може мати різні значення в соціальних медіа-платформах. У більшості випадків, репутація – це привід для довіри. Атак, як інформаційні технології не вміють досконало визначати достовірність джерел, сайти соціальних медіа покладаються на системи автоматичної обробки даних: інструменти, які автоматично, відповідно до дій користувача генерують інформацію, щоб визначити достовірність джерела [2]. Управління репутацією є ще одним аспектом і прикладом використання соціальних засобів масової інформації.

Групи: Цей блок являє собою секцію, в якій користувачі можуть створювати спільноти і субспільноти. Чим більшою стає "соціальна" мережа, тим швидше зростає кількість груп друзів, фоловерів і контактів [2].

**4. Розробка моделі соціальної мережі з посиленими механізмами захисту**

**Основні інформаційно-комунікаційні блоки соціальних мереж**

Соціальна мережа – це інтерактивний багатокористувацький веб-сайт, контент якого наповнюється самими учасниками мережі. Такий ресурс являє собою автоматизоване соціальне середовище, що дозволяє спілкуватися групі користувачів, об'єднаних спільними інтересами, слідкувати за життям користувачів.

Саме тому, проаналізувавши основні ресурси, було виділено основні інформаційні блоки, що зустрічаються у кожній соціальній мережі. Такі блоки можна назвати базовими, і вони є найбільш важливими в процесі моделювання мережі з посиленими механізмами захисту.

Далі приведений перелік інформаційно-комунікаційних блоків:

– профіль – сторінка яка містить інформацію про користувача, та, зазвичай, містить мікроблог. Профіль може переглядатись усіма користувачами мережі, яким власник профілю надав це право;

– особиста переписка – зазвичай, даний блок реалізований як засіб для комунікації між двома користувачами;

– публічні сторінки – це сторінка, в якій усі бажаючі можуть залишати свою думку під певними записами.

Згідно з даними блоками було розроблено моделі функціонування захищеної соціальної мережі.

**Принципи функціонування системи.**

Основна ідея соціальної мережі з посиленим механізмом захисту конфіденційності полягають у наступному:

- Сервер зберігає лише зашифровану інформацію. Доступ до відкритих даних має лише власник цих даних та довірені особи.
- Все шифрування відбувається на стороні клієнта.
- Для шифрування використовуються алгоритми симетричного шифрування (AES), для обміну ключами – алгоритми асиметричного шифрування (RSA).
- Публічні сторінки мають свої ключі (відкриті, закриті), які зберігаються у власника публічної сторінки, тобто у того, хто її створив.

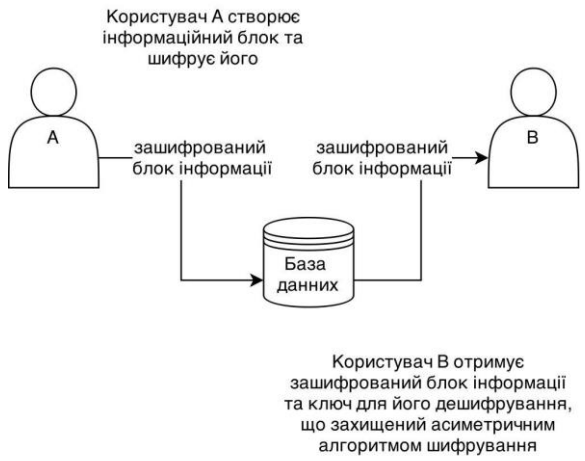


Рис. 2. Загальна схема соціальної мережі з посиленим механізмом захисту конфіденційності

Таким чином, скомпрометований сервер не буде нести загрози, тому що дані, які він зберігає,знаходяться в зашифрованому вигляді. Саме це і реалізовує принцип захищеності.

Розробка моделей відбувалась з урахуванням тих факторів, що у будь-який час (t) доступ до даних має (n) користувачів, а у будь-який інший момент (t+1) кількість цих користувачів може зрости чи зменшитись. Якщо новий користувач отримує доступ до даних у момент (t), він повинен мати також можливість переглянуті дані у моменти (t–1, t–2 …).

**Моделі функціонування інформаційно-комунікаційних блоків**

Кожен користувач системи має свій відкритий та закритий ключ {e,n}, {d,n} відповідно до алгоритму RSA, та ключ k для AES. Кожен користувач має список друзів, що являє собою список відкритих ключів тих користувачів, яким він довіряє – [$\{e_1,n_1\}$, $\{e_2,n_2\}$ … $\{e_N,n_N\}$].

Функціональний блок - профіль (Рис.3): користувач А створює профіль - Р. Шифрує профіль за допомогою ключа k та алгоритму AES, в результаті чого отримує зашифрований профіль F. Наступним кроком для кожного користувача зі списку друзів за допомогою відкритого ключа, шифрує ключ k та зберігає його та повідомлення у базу у вигляді [F, $\{RSAe_1(k), e_1\}$, $\{ RSAe_2(k), e_2\}$, … $\{RSAe_N(k),e_N)$]. При додаванні нового користувача до списку друзів, він дописує данихпрофілю новий масив $\{RSAe_L(k), e_L\}$. У випадку видалення користувача зі списку друзів , власник профілю повинен перешифрувати профіль новим секретний ключем $k_1$ та створити для кожного користувача зі списку друзів нові ключі $\{RSAe_l(k_1),e_l\}$.

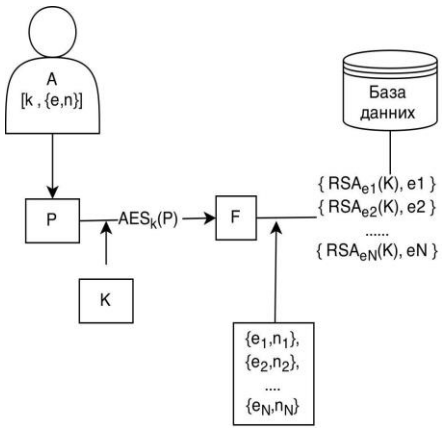


Рис. 3. Модель створення та шифрування профілю

Функціональний блок – особиста переписка. Користувач А (k, {e,n}, {d,n}) хоче написати повідомлення користувачу В ($k_1$, $\{e_1,n_1\}$, $\{d_1,n_1\}$). Користувач А генерує випадковий ключ m для конкретного повідомлення М. Шифрує повідомлення М за допомогою ключа m та алгоритму AES. Далі шифрує за допомогою свого відкритого ключа зашифровуєключ m – RSAe(m). Аналогічну операцію він проводить і за допомогою ключа $e_1$ , в результаті чого отримує $RSAe_1$ (m). Далі зберігає дані у базу у вигляді AESm(M), $\{RSAe_1(m)\}$, {RSAe(m)}. Таким чином, навіть якщо один ключ буде скомпрометований, інша частина інформації буде захищена.

Функціональний блок – публічна сторінка. Принцип реалізації механізму функціонування блоку «публічна сторінка» є близьким до «особистого профілю». Розглянемо даний механізм детальніше.

Користувач А створює публічну сторінку та додає до неї ті публічні ключі, які належать «читачам» даної сторінки. Таким чином він отримує список користувачів, які мають доступ до інформації,

яка буде публікуватись на даній сторінці. При заявці нового користувача публічної сторінки, він може відхилити запит та не додавати відкритий ключ нового користувача до системи.

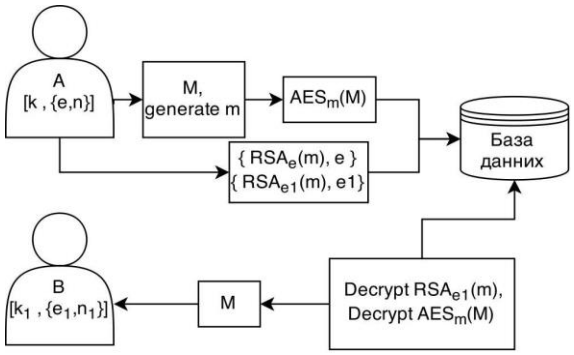


Рис. 4. Модель шифрування особистої переписки

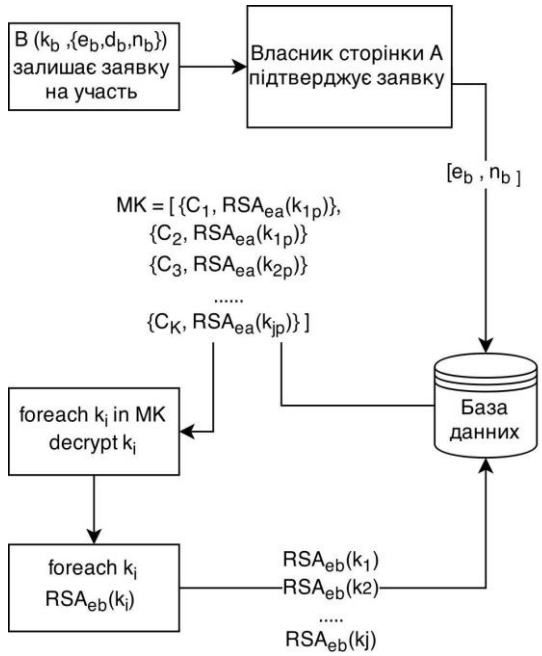


Рис. 5. Схема додавання нового користувача

При створенні публічної сторінки користувач A(k, {e,n}, {d,n}), як власник сторінки, генерує ключі для даної сторінки P($k_p$, {$e_p$,$n_p$}, {$d_p$,$n_p$}). Усі повідомлення, які він публікує на дану сторінку, він шифрує за допомогою алгоритму AES та ключа $k_p$ , та додає до повідомлення зашифрований ключ $k_p$ за допомогою алгоритму RSA кожного з користувачів його публічної сторінки, а також ключ повідомлення шифрований його відкритим ключем. Уразі видалення користувача зі списку «читачів» публічної сторінки, власник повинен згенерувати новий ключ $k_{p1}$ і надалі виконувати шифрування нових повідомлень за допомогою нового ключа. У разі додавання нового користувача B ($k_b$ , {$e_b$ , $n_b$}, {$d_b$ , $n_b$}), власник сторінки, після підтвердження заявки, повинен до усіх старих повідомлень додати наступну криптограму $RSA_{eb}(k_p)$. Це надасть змогу новому користувачеві читати повідомлення, що були створені у даній публічній сторінці до його участі в цій сторінці.

**5.Результати дослідження**

Результатами дослідження є модель захищеної соціальної мережі. Дана модель є ефективним механізмом забезпечення конфіденційності інформації під час її зберігання. Також дану модель можна використовувати під час реалізації нової соціальної мережі, а також як надлаштування над існуючою мережею. Прикладом надлаштування над існуючою мережею може бути додаток до браузеру. В такому випадку, соціальна мережа, для якої буде розроблятись додаток, буде слугувати каналом зв'язку та зберігання захищеної інформації. Для реалізації додатку потрібно використовувати ті алгоритми функціонування, що відповідають інформаційно-комунікаційному блоку.

**6. Висновки**

У ході роботи було встановлено, розглянуто та виділено основні теоретичні аспекти соціальних мереж та їх ключові особливості, проаналізовано існуючі алгоритми симетричного та асиметричного шифрування.

Модель, отримана у роботі, є новим підходом для керування потоками інформації у соціальних мережах. Дана система може бути імплементована як у існуючих системах, так і може слугувати фундаментом для нових соціальних мереж.

Дана модель має широке застосування у різних сферах, де існують інформаційні потоки, що базуються на соціальних мережах. Результатом роботи є три моделі функціонування соціальної мережі, відповідно до виділених інформаційно-комунікаційних блоків.

**Література**

1. Wasserman, S. Social Network Analysis in the Social and Behavioral Sciences. Social Network Analysis: Methods and Applications [Text] / S. Wasserman, K. Faust. – Cambridge University Press, 1994. – P. 1–27.

2. Kietzmann, H. Social media? Get serious! Understanding the functional building blocks of social media [Text] / H. Kietzmann, J. K. Hermkens, I. P. McCarthy, B. S. Silvestre // Business Horizons. – 2011. – Vol. 54, Issue 3. – P. 241–251.

3. Carrington, P. J. Models and Methods in Social Network Analysis [Text] / P. J. Carrington, J. Scott. – Cambridge University Press, 2005. doi: 10.1017/cbo978051 1811395

4. Баричев, С. Г. Стандарт AES. Алгоритм Rijndael. Основы современной криптографии [Текст] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов – Стандарт AES, 2002. – С. 30–35.

5. Hill, R. Social Network Size in Humans [Text] / R. Hill, R. Dunbar // Human Nature. – 2003. – Vol. 14, Issue 1. – P. 53–72. doi: 10.1007/s12110-003-1016-y

6. НД ТЗІ 1.1-003-99 [Текст] / Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

**References**

1. Wasserman, S., Faust, K. (1994). Social Network Analysis in the Social and Behavioral Sciences. Social Network Analysis: Methods and Applications. Cambridge University Press, 1–27.

2. Kietzmann, J. H., Hermkens, K., McCarthy, I. P., Silvestre, B. S. (2011). Social media? Get serious! Understand-

ing the functional building blocks of social media. Business Horizons, 54 (3), 241–251. doi: 10.1016/j.bushor.2011.01.005

3. Carrington, P. J., Scott, J. (2005). Models and Methods in Social Network Analysis. Cambridge, Cambridge University Press. doi: 10.1017/cbo9780511811395

4. Barychev, S. G., Goncherov, V. V., Serov, R. E (2002). AES standart. Rijndael algorithm. The foundations of modern cryptography, 30–35.

5. Hill, R. A., Dunbar, R. I. M. (2003). Social network size in humans. Human Nature, 14 (1), 53–72. doi: 10.1007/s12110-003-1016-y

6. ND TZI 1.1-003-99. Terminology in the field of information security in computer systems against unauthorized access.

*Рекомендовано до публікації д-р техн. наук Качинський А. Б.*
*Дата надходження рукопису 20.05.2015*

**Орел Марк Миколайович**, кафедра безпеки інформаційно-комунікаційних систем, Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна, 03056
E-mail: mail.ormark@gmail.com

**УДК 519.6:616.1**
**DOI: 10.15587/2313-8416.2015.44335**

# МОДЕЛЮВАННЯ РОБОТИ СЕРЦЯ НА ОСНОВІ ЧАСОВИХ ТА СПЕКТРАЛЬНИХ ХАРАКТЕРИСТИК ЕЛЕКТРОКАРДІОСИГНАЛУ

**© О. О. Юрко, Р. О. Рибніков, О. В. Курченко**

*Запропонований метод моделювання роботи серця на основі часових та спектральних характеристик. Робота присвячена вирішенню актуальної проблеми аналітичного описання спектральної щільності електрокардіосигалу на основі перерахунку несиметричних Гаусових імпульсів з часового ряду. Було апроксимовано ЕКГ-сигнал за допомогою несиметричних Гаусових імпульсів та отримано його спектр. Для ЕКГ-сигналу з патологією було побудовано фазограмму.*
***Ключові слова:*** *апроксимація, спектральна щільність, функція Гаус, електрокардіосигнал, спектр, частотна область, фазограма.*

*It is proposed the method of modeling of the heart based on temporal and spectral characteristics. The work is devoted to the decision of actual problems of analytical description of the spectral density of electrocardiosignal, based on the terms of asymmetric Gaussian pulses with time series. It was approximated ECG signal using asymmetric Gaussian pulses and obtained its spectrum. It was built phasegram for the ECG signal with the pathology*
***Keywords:*** *approximation, spectral density, Gaussian function, electrocardiosignal spectrum, frequency domain, phasegram*

## 1. Вступ

Серцево-судинні захворювання людини міцно утримують першість за основними критеріями соціальної значущості: поширеності, інвалідності та смертності. У зв'язку з чим виникає гостра необхідність у точній та сучасній діагностиці захворювань серцево-судинної системи на різних стадіях розвитку. Існує велика кількість різноманітних методів обробки кардіосигналу, такі як: вейвлет-перетворення, фрактальний аналіз компонент, метод головних компонент, методи Р.М. Баевского та інші, що дозволяють зменшити час обробки та збільшити точність результатів аналізу. Для діагностики кардіосигналу доцільно використовувати математичні моделі, які дозволяють отримати синтезовані штучні кардіосигнали з певними характеристиками.

## 2. Постановка проблеми

Мета даної роботи полягає у розробці математичної моделі спектральних характеристик ЕКГ-сигнлау для діагностики захворювань серцево-судинної системи. На основі аналізу стійкості роботи серця, але в існуючих моделях є проблема у визначенні гармонійних складових спектру для побудови передавальної функції.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– встановити зв'язок між часовими та спектральними характеристиками з незначною кількістю математичних перетворень для можливості застосування у експрес діагностиці;

– проаналізувати можливість застосування несиметричних Гаусових імпульсів для встановлення такого зв'язку;

– отримати аналітичну залежність для апроксимації спектральної щільності ЕКГ-сигналу.

## 3. Літературний огляд

Метод стандартної ЕКГ та проведення навантажувальних проб до теперішнього часу досягли певних меж своїх діагностичних можливостей для виявлення ранніх або прихованих захворювань серцево-судинної системи.