УДК 004.056.55:616.1

В. І. РУЖЕНЦЕВ, Г. С. ДОБРОРОДНЯ, О. В. ВИСОЦЬКА, Т. А. КУЛІШ

Харківський національний університет радіоелектроніки, Україна

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ВИЗНАЧЕННЯ ТЯЖКОСТІ СТАНУ ПАЦІЄНТІВ З СЕРЦЕВО-СУДИННИМИ ПАТОЛОГІЯМИ

Робота присвячена організації захисту інформації в інформаційній системі визначення тяжкості стану пацієнтів із серцево-судинними патологіями. Розглянуто методи захисту інформації, які застосовуються в системах подібного типу. Проаналізовано та обґрунтовано вибір блочного симетричного шифрування ДСТУ 7624:2014 для захисту даних в інформаційній системі визначення тяжкості стану пацієнтів із серцево-судинними патологіями. Цей алгоритм забезпечує високий рівень стійкості від атак, а також швидкість програмної реалізації. Наявність запропонованої криптообробки знижує ймовірність викрадення даних пацієнта.

Ключові слова: *захист інформації, алгоритм, шифрування, патологія, дані.*

Вступ

Патологія серцево-судинної системи лідирує в структурі смертності, летальності та інвалідизації пацієнтів [1]. У країнах Європейського союзу показник смертності від захворювань системи кровообігу становить від 214 до 493 випадків на 100 тис. населення, в США – до 315 випадків на 100 тис. населення [2].

В [1] показано, що ще однією проблемою в медицині є коморбідність патологій, значення показників яких необхідно враховувати під час діагностики даної групи пацієнтів.

Дослідження, які спрямовані на визначення тяжкості стану пацієнтів із серцево-судинними патологіями, вимагають обліку великого обсягу інформації, тому виникає потреба в автоматизації цього процесу. Важливим елементом будь-якої інформаційної системи (ІС), що пов'язана з медичними даними пацієнтів, є організація захисту даних, які в ній знаходяться.

Відповідно до закону України «Основи законодавства України про охорону здоров'я» від 19.11.1992 № 2801-XII стаття 40 «Лікарська таємниця» медичні працівники та інші особи, яким у зв'язку з виконанням професійних чи службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та його результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків.

Актуальність теми забезпечення інформаційної безпеки в медицині підтверджується тим, що в більшості медичних установ питання захисту інформації не розглядаються.

Тому організація захисту інформації в ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями, до яких відносяться такі захворювання як ішемічна хвороба серця, гіпертензія, інсульт та інші захворювання, є актуальним завданням.

1. Постановка проблеми і аналіз останніх джерел і публікацій

Проаналізувавши загрози безпеки персональних даних [3] можна виділити наступні загрози для ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями:

- загрози, що призводять до порушення конфіденційності даних (копіювання або розголошення), при реалізації яких не здійснюється безпосередній вплив на зміст інформації;

- загрози, що призводять до несанкціонованого, в тому числі випадкового, впливу на зміст інформації, в результаті якого здійснюється зміна персональних даних.

Забезпечення конфіденційності та цілісності при обробці, зберіганні і використанні медичних даних в ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями дозволить істотно знизити ймовірність виникнення зазначених загроз [4].

На сьогоднішній день поширення набули різноманітні медичні ІС. Відома система «Монитор здоровья», яку розроблено на базі хмарних технологій. Система забезпечує захищений доступ до інформації з будь-якого місця і пристрою. Дані

про пацієнта через інтернет надходять до лікаря або в медичний заклад [5].

Існує система медичного електронного моніторингу, використовуючи яку пацієнти носять електронні браслети – датчики медичних параметрів. Інформація з електронних браслетів передається на стаціонарний або мобільний контрольний пристрій. Мобільний контрольний пристрій або смартфон використовують канали бездротового зв'язку для передачі інформації і приймачі для моніторингу місця розташування пацієнта. Центр моніторингу обмінюється отриманою інформацією з територіальними медичними закладами, які обладнані автоматизованими робочими місцями користувачів (АРМК). Через АРМК здійснюється доступ медичних працівників до інформації про стан здоров'я пацієнтів. Також центр моніторингу обмінюється даними з зовнішніми організаціями (страхові компанії, державні контрольні органи), які також обладнані АРМК. Доступ до медичної інформації здійснюється відповідно до наданих прав доступу [6].

Відомий сервіс з контролю здоров'я – ONDOC. Дані пацієнта інтегровані з електронною амбулаторною картою. Вся інформація зберігається на сервері в знеособленому вигляді. Сервіс використовує симетричний метод шифрування за стандартом AES 128 і двухфакторну авторизацію по SMS. Також для збереження даних система регулярно проводить їх резервне копіювання [7].

Відома система прихованої передачі інформації на базі хаотичних генераторів з запізненням, для забезпечення прихованої передачі даних медичних ІС і медичного обладнання. Система здійснює потокове кодування інформації з малою затримкою та може використовуватися для приховування каналу передачі інформації від медичного обладнання [8].

Питанням розробки цифрового реєстру для запису медичних даних зайнялася компанія DeepMind. Платформа отримає назву Verifiable Data Audit («Верифицируемый контроль над данными»). Першими користувачами системи стануть лікарні, британська Національна служба охорони здоров'я (NHS), а потім і самі пацієнти. Будь-яка взаємодія з даними пацієнта буде записуватися в реєстрі з використанням криптографічних перетворень. Verifiable Data Audit не буде децентралізованою. Систему регулюватимуть медичні установи і оператори по роботі з даними. Для захисту реєстру передбачається використовувати «деревоподібне хешування» (дерево Меркле) [9, 10].

Усі розглянуті системи є складними. Вони є спеціалізованими і багатофункціональними, вимагають постійної підтримки в обслуговуванні (хмарні технології), що робить їх дуже дорогими і обмежує їх застосування і експлуатацію в широкому колі медичних установ.

З ускладненням методів обробки даних і збільшенням кількості технічних засобів [11-13] все більше виникає необхідність в розробці нових або вдосконаленні вже існуючих методів захисту даних.

Використання криптографічних методів дозволяє забезпечити конфіденційність і цілісність даних. Для перевірки цілісності даних в криптографії використовуються хеш-функції. Хеш-функція перетворює послідовність байтів довільного розміру в послідовність байтів фіксованого розміру [14]. Якщо дані зміняться, то і число, що генерується хеш-функцією, теж зміниться. Забезпечення конфіденційності можливо здійснити за допомогою застосування шифрування даних, прочитати які можливо тільки при наявності відповідного ключа.

Існує симетричне і асиметричне шифрування даних. Перший спосіб шифрування передбачає наявність одного і того ж криптографічного ключа для шифрування і розшифрування даних. Другому способові характерна наявність відкритого ключа, який передається по незахищеному каналу і використовується для перевірки електронного підпису та шифрування повідомлення, і закритого ключа, який використовується для генерації електронного підпису і розшифрування повідомлення. Практичне застосування отримали обидва способи шифрування. Однак існують особливості кожного із способів шифрування. Алгоритми симетричного шифрування, як відомо, мають дуже високу продуктивність і швидкодію. Також можна відзначити, що криптографія з симетричними ключами дуже стійка, що робить практично неможливим процес дешифрування без знання ключа. Оскільки для шифрування і дешифрування використовується один і той же ключ, при використанні таких алгоритмів потрібні дуже надійні механізми для розподілу ключів. Що стосується асиметричного шифрування, то можна відзначити його складність в реалізації. У схемі шифрування з відкритим ключем неможливо обчислити процедуру дешифрування, знаючи процедуру шифрування. Таким чином, слід зазначити, що алгоритм асиметричного шифрування сильно програє симетричним з точки зору часу шифрування і розшифрування даних.

Симетричне шифрування даних можливо двома способами: блоковим і потоковим. Потокові алгоритми виконують шифрування вхідного потоку

побайтно або побітно. На основі симетричного ключа виробляється ключова послідовність (гамма-послідовність), яка складається за модулем два (операція xor) з вхідним потоком. Потокові шифри, як правило, більш продуктивні ніж блокові і використовуються для шифрування мови, мережевого трафіку і інших даних з заздалегідь невідомою довжиною. При досить частій зміні ключа для генерування гами-послідовності потокові шифри забезпечують достатню стійкість. Від поточних шифрів робота блочного відрізняється обробкою біт групами за одну ітерацію. Блокові криптосистеми розбивають текст повідомлення на окремі блоки і потім здійснюють перетворення цих блоків з використанням ключа. На відміну від поточних алгоритмів. які орієнтовані на апаратну реалізацію, блокові алгоритми призначені для програмної реалізації. До переваг блокових шифрів відносять схожість процедур шифрування і розшифрування, які відрізняються лише порядком дій. Це спрощує створення пристроїв шифрування, так як дозволяє використовувати одні і ті ж блоки в ланцюгах шифрування і дешифрування.

Таким чином, проаналізувавши всі переваги кожного із способів шифрування, рішення поставлених завдань необхідно здійснити за допомогою симетричного алгоритму блочного шифрування.

Метою роботи є розробка підсистеми захисту інформації із використанням симетричного алгоритму блочного шифрування для ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями.

2. Розробка структурної схеми ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями

ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями (рис.1) складається з медичної та технічної підсистеми. До медичної підсистеми відносяться лікар і пацієнт с серцево-судинною патологією. Лікар безпосередньо може впливати на процес діагностики і коригувати його. Взаємодія між пацієнтом і лікарем є діалог при огляді першого.

Технічна підсистема складається з наступних елементів: модуля реєстрації інформації, модуля обробки інформації, БД, модуля аналізу даних, модуля формування звіту і блоку виведення інформації.

Модуль реєстрації інформації представлений апаратно-програмним комплексом, який реєструє електрокардіографічний сигнал, а також дані огляду, анамнезу та обстежень пацієнта.

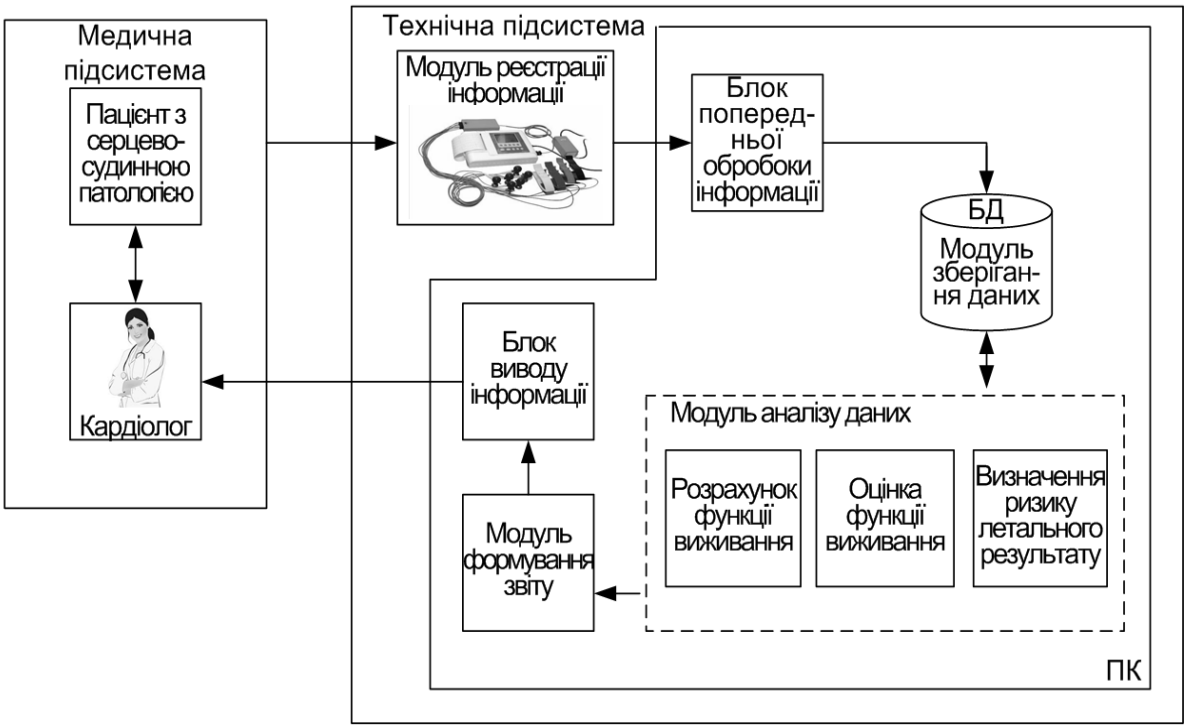

Рис. 1. Структурна схема ІС

Модуль обробки інформації служить для попередньої обробки сигналу, яка полягає в фільтрації сигналу і кодуванні інформації про пацієнта. Всі дані про пацієнта зберігаються в базі даних (БД).

У модулі аналізу відбувається визначення тяжкості стану пацієнтів із серцево-судинними патологіями з використанням необхідних даних, які надійшли з БД, розраховується і оцінюється функція виживання для хворих, а також визначається ризик летального результату у хворих з інфарктом міокарда. Для визначення стану пацієнта використовуються метод Каплана-Мейєра і регресійна модель Кокса.

Інформація про результати діагностики надходить в блок зберігання даних, а потім в модуль формування звіту. Висновок про стан пацієнта можна переглянути в блоці виведення інформації. Після отриманих даних лікар призначає відповідне лікування.

В результаті розгляду структурної схеми ІС (рис. 1) можна зробити висновок, що найбільш уразливими місцями є вхід і вихід інформації з БД. Інформація про пацієнта зберігається в БД тривалий час, що збільшує ймовірність загрози викрадення даних. Для зниження ймовірності загрози викрадення даних під час зберігання необхідно здійснити шифрування і дешифрування інформації в зазначених раніше місцях (рис. 2).

3. Розробка підсистеми захисту інформації в ІС визначення тяжкості стану пацієнтів із серцево-судинними патологіями

Існує велика кількість блокових симетричних шифрів. Найбільш розповсюдженим в світі є AES, однак в Україні в 2015р. був прийнятий стандарт ДСТУ 7624:2014, який відповідає сучасним вимогам до цього типу алгоритмів.

Алгоритм шифрування згідно ДСТУ 7624:2014 схожий з AES, який заснований на алгоритмі Rijndael. Особливість шифрування згідно ДСТУ 7624:2014, на відміну від AES, полягає в використанні різних S-блоків (використовуються 4 різних S-блока), згенерованих випадковим чином, замість однакових S-блоків, і в застосуванні поперемінного складання з цикловими підключами по модулю 2 і по модулю 2^{64}. Також шифру характерне лінійне перетворення, яке виконується за допомогою матриці МДР коду розміру 8×8 над полем GF (2^8). Дана операція покращує криптографічні властивості шифру. У таблиці 1 наведено кількість циклів N_r в залежності від довжини ключа N_k і розміру блоку N_b.

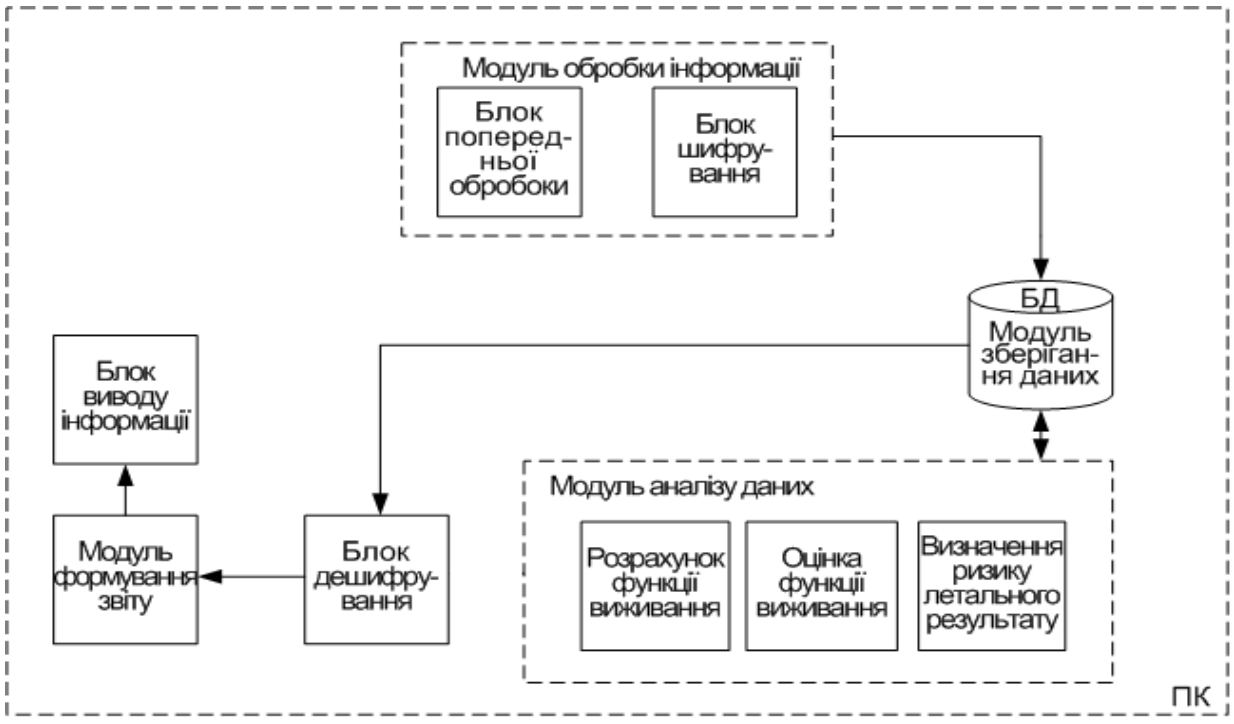

Рис. 2. Структурна схема персонального комп'ютера (ПК)
з позначеними блоками шифрування і дешифрування даних

Таблиця 1

Параметри шифру

Key length Block size	128 (N_k=2)	256 (N_k=4)	512 (N_k=8)
128 (N_b=2)	10	14	–
256 (N_b=4)	–	14	18
512 (N_b=8)	–	–	18

Основними етапами шифрування (рис. 3) є:

– процедура забілювання, яка виконується за допомогою додавання з початковим підключом по модулю 2^{64};

– введення циклових підключів з використанням операції побітового складання по модулю 2 в циклах від першого до N_r-1;

– перетворення ShiftRows і MixColumns;

– застосування чотирьох різних S-блоків в рамках перетворення SubBytes.

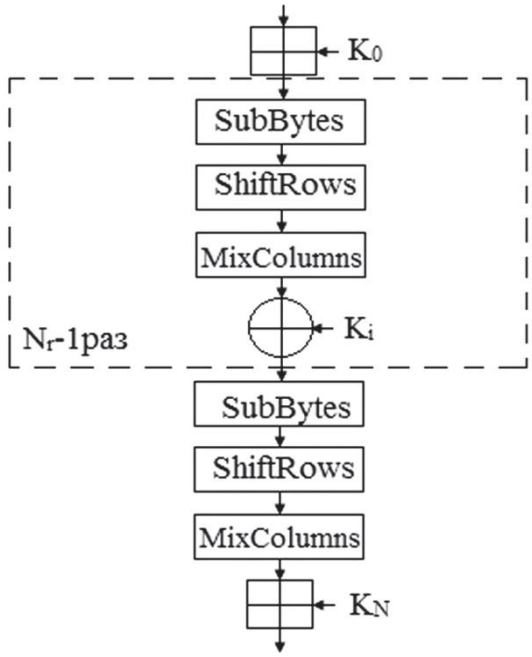

Рис. 3. Схема шифрування інформації

В ході перетворення ShiftRows проводиться рівномірний розподіл байтів кожної 64-бітної колонки серед інших колонок. Це досягається шляхом циклічного зсуву рядків стану вправо на різну кількість байтів в залежності від розміру блоку.

В ході перетворення MixColumns виконується послідовна обробка всіх колонок поточного стану. Кожна 8-байтна колонка розглядається як поліном над полем GF (28) з 8 термами, а в ході перетворення виконується множення цього поліному по модулю x8+1 на фіксований поліном c(x), де

$$c(x)=\{01\}x^7+\{05\}x^6+\{01\}x^5+\{08\}x^4+$$
$$+\{06\}x^3+\{07\}x^2+\{04\}x+\{01\}.$$

У перетворенні SubBytes використовується 4 різних підстановки «байт-в-байт», причому для байтів одного рядка поточного стану шифру використовується одна і та ж підстановка, що покращує статистичні властивості, підвищує рівень стійкості до диференціального і лінійного криптоаналізу. При розшифруванні використовуються зворотні версії перерахованих перетворень.

Під час шифрування з використанням алгоритму використовується N_r+1 циклових ключів k_i (i = 0,1 .., N_r), кожен довжиною 64×N_b біт. Розмір відкритого шифртексту збігається з розміром циклового ключа.

При виконанні операції розгортання ключа виконується три основних етапи:

1) формування проміжного ключа K_t довжиною 64×N_b біт;

2) формування циклових ключів k_{2i} (з парними індексами);

3) формування циклових ключів k_{2i} (з непарними індексами).

Розгортання ключів показано на рис. 4.

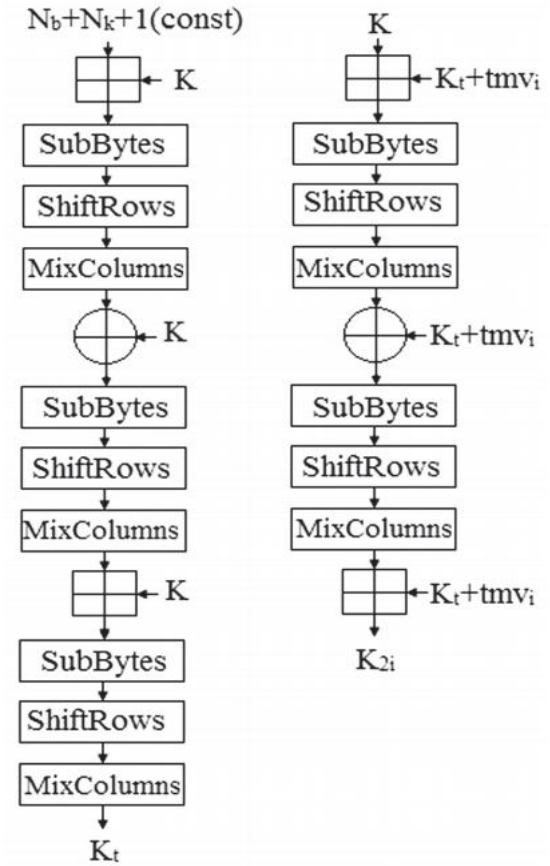

Рис. 4. Схема розгортання ключів

Проміжний ключ K_t, який збігається за розміром з довжиною блоку відкритого тексту, має довжину $64\times N_b$. Він формується на основі ключа шифрування K довжиною $64\times N_k$ біт. При цьому використовується перетворення, які також були включені в побудову циклових функцій. При формуванні K_t застосовуються три цикли шифрування. Вхідною інформацією для перетворення є двійкові числа, які визначаються розміром блоку і довжиною ключа. Цикловими ключами є ключі шифрування, у разі, якщо ключ довше блоку, використовується його молодша і старша половини. Вихідним значенням перетворення є проміжні ключі K_t.

При формуванні циклових ключів ключ шифрування K подається на двоциклове перетворення. Воно складається з операції забілювання і операції *Add64RoundKey*.

Результатом обробки проміжного ключа K_t є цикловий ключ. Ця операція виконується за допомогою функції *Add64RoundKey*, яка полягає в додаванні K_t по модулю 2^{64} з другим аргументом. Другий аргумент представлений двійковим значенням, яке залежить від індексу циклового ключа (змінна tmv_i), який формується. Розмір tmv_i дорівнює довжині блоку. Формування константи відбувається при повторенні байтів 0x01, 0x00 (в 16-му поданні) до заповнення стану.

Модифікація змінної tmv_i відбувається при формуванні циклового ключа з парними індексами. Ця операція виконується за допомогою функції *ShiftLeft*, яка обробляє послідовність 64-бітних слів. Кожне слово стану $(w_0, w_1, ..., w_{N_b-1})$ з кожним циклом перетворення логічно зсувається вліво на 1 біт, тобто $w_i = 2\ w_i \pmod{2^{64}}$.

На виході двоциклового перетворення формуються циклові ключі з парними індексами. Ця операція виконується за допомогою функції *Rotate*, яка обробляє стан як послідовність 64-бітних слів $(w_0, w_1, ..., w_{N_k-1})$, виконуючи циклічний зсув і повертаючи стан $(w_1, ..., w_{N_k-1}, w_0)$.

Циклові ключі з парними індексами подаються у вигляді байтового рядка. Потім відбувається циклічний зсув вліво на $2N_b+3$ байта і знову подається у вигляді стану, який використовується як цикловий ключ з непарним індексом, тобто $k_{2i+1} = k_{2i} <<< (2N_k+3)$. Байтовий рядок $b_0, b_1, \ldots, b_{8N_b-1}$ після перетворення має вигляд $b_{2N_b+3}, b_{2N_b+4}, \ldots, b_{8N_b-1}\ b_0, b_1, \ldots, b_{2N_b+2}$.

Константа, яка визначає зсув вліво циклового ключа з парним індексом залежить від розміру блоку. Ця залежність наведена в табл. 2 [15].

Таблиця 2

Залежність константи від розміру блоку

Розмір блоку, біт (байт)	Зсув вліво (байт)
128 (16)	7
256 (32)	11
512 (64)	19

Висновок

Основною загрозою для розроблюваної системи є несанкціонований доступ, розкрадання, зміна медичної інформації про пацієнтів, тому в якості ефективного алгоритму захисту даних був обраний симетричний алгоритм блочного шифрування на етапі запису та зчитування інформації з БД. В якості блочного симетричного шифрування було обрано ДСТУ 7624:2014. Цей алгоритм забезпечує високий рівень стійкості від атак, вибір довжини ключа і блоку даних, а також високу швидкість програмної реалізації на сучасних платформах. Реалізація запропонованих заходів, а саме наявність криптообробки інформації при її записі і вилученні з бази даних, знижує ймовірність викрадення інформації. При цьому швидкодія системи дещо знижується, однак для користувача системи буде непомітна.

Література

1. Колесникова, Е. В. Современный пациент с заболеванием печени и патологией сердечно-сосудистой системы: какой выбор сделать? [Текст] / Е. В. Колесникова // Сучасна гастроентерологія. – 2014. – № 2 (76). – С. 85-94.

2. Мониторирование сердечно-сосудистой заболеваемости, смертности и их факторов риска в разных регионах мира (проект ВОЗ MONICA) [Текст] / Научно-исследовательский институт терапии и профилактической медицины, Всемирная организация здравоохранения ; под ред. Ю. П. Никитина. – Новосибирск : Гео, 2016. – 699 с.

3. Федеральная служба по техническому и экспортному контролю. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс] / Федеральная служба по техническому и экспортному контролю. – 69 с. – Режим доступу: http://csr43.ru/files/ZI/FSTEK-baz-model-ugroz.pdf. – 15.02.2008.

4. Stankovski, T. Coupling functions enable secure communications [Text] / T. Stankovski, P. V. E. McClintock, A. Stefanovska // Physical Review X. – 2014. – № 4. – 9 p. DOI: 10.1103/PhysRevX.4.011026

5. Ринтех «Монитор здоровья» [Электронный ресурс]. – Режим доступу: http://www.rintech.ru/serv/detail.php?ID=114. –25.09.2015.

6. Зараменских, Е. П. Интеллектуализация обработки информации в системе электронного медицинского мониторинга [Текст] / Е. П. Зараменских, Е. А. Исаев, Н. Л. Коровкина // Математическая биология и биоинформатика. – 2016. – №2. – С. 288-298.

7. Сервис из Санкт-Петербурга открыл бесплатные возможности для российских клиник [Электронный ресурс]. – Режим доступу: https://www.dp.ru/a/2015/12/08/Servis_iz_Sankt-Peterburg. – 21.12.2015.

8. Система скрытой передачи данных в медицинских информационных системах, основанная на хаотической синхронизации генераторов с запаздывающей обратной связью [Текст] / Д. Д. Кульминский, А. С. Караваев, В. И. Пономаренко, М. Д. Прохоров // Бюллетень медицинских Интернет конференций. – 2014. – №7. – С. 971-974.

9. DeepMind создаст систему записи медицинских данных на блокчейне [Электронный ресурс]. – Режим доступу: https://hightech.fm/2017/03/10/blockchan_health_records. – 10.03.2017.

10. Condliffe, J. DeepMind's New Blockchain-Style System Will TrackHealth-Care Records [Text] / J. Condliffe // MIT Technology Review. – 2017. – № 5(18). – P. 1-8

11. Enabling secure and resource-efficient blockchain networks with VOLT [Text] / S. Setty, B. Soumya, Z. Lidong, M. L. Roberts, R. Venkatesan // MSR Technical Report. – 2017. – № 38. – P. 1-15

12. High-speed high-security signatures [Text] / D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, B.-Y. Yang // Journal of Cryptographic Engineering. – 2012. – № 2(2). – P. 77–89.

13. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies [Text] / J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten // SoK: InProceedings of the IEEE Symposium on Security and Privacy. – 2015. – P. 104–121.

14. Целостность информации [Электронный ресурс]. – Режим доступу: http://wikisec.ru/MediaWiki/index.php?title=%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8. –26.09.2017.

15. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України [Текст] / Р. Олійников, І. Горбенко, О. Казимиров, В. Руженцев, Ю. Горбенко // Захист інформації. – 2015. – № 2. – С. 142-157.

References

1. Kolesnikova, E. V. Sovremennyi patsient s zabolevaniem pecheni i patologiei serdechno-sosudistoi sistemy: kakoi vybor sdelat'? [A modern patient with liver disease and cardiovascular pathology: what choice should I make?]. *Suchasna hastroenterolohiya – Modern Gastroenterology*, 2014, no. 2 (76), pp. 85-94.

2. Nauchno-issledovatel'skiy institut terapii i profilakticheskoy meditsiny, Vsemirnaya organizatsiya zdravookhraneniya *Monitorirovanie serdechno-sosudistoy zabolevaemosti, smertnosti i ikh faktorov riska v raznykh regionakh mira (proekt VOZ MONICA)* [Monitoring of cardiovascular morbidity, mortality and risk factors in different regions of the world (WHO MONICA project)]. Novosibirsk, Geo Publ., 2016. 699 p.

3. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska)* [The basic model of threats to the security of personal data when processing them in information systems of personal data (extract)]. Available at: http://csr43.ru/files/ZI/FSTEK-baz-model-ugroz.pdf (accessed 15.02.2008).

4. Stankovski, T., McClintock, P.V.E., Stefanovska, A. Coupling functions enable secure communications. *Physical Review X,* 2014, no. 4. 9 p.

5. *Rintekh «Monitor zdorov'ya»* ["Health Monitor"]. Available at: http://www.rintech.ru/serv/detail.php?ID=114 (accessed 25.09.2015).

6. Zaramenskikh, E. P., Isaev, E. A., Korovkina N. L. Intellektualizatsiya obrabotki informatsii v sisteme elektronnogo meditsinskogo monitoringa [Intellectualization of information processing in the system of electronic medical monitoring]. *Matematicheskaya biologiya i bioinformatika – Mathematical biology and bioinformatics, 2016, no. 2, pp. 288-298.*

7. Servis iz Sankt-Peterburga otkryl besplatnye vozmozhnosti dlya rossiiskikh klinik [Service from St. Petersburg has opened free opportunities for Russian clinics]. Available at: https://www.dp.ru/a/2015/12/08/Servis_iz_Sankt-Peterburg (accessed 21.12.2015).

8. Kul'minskii, D. D., Karavaev, A. S., Ponomarenko, V. I., Prokhorov, M. D. Sistema skrytoi peredachi dannykh v meditsinskikh informatsionnykh sistemakh, osnovannaya na khaoticheskoi sinkhronizatsii generatov s zapazdyvayushchei obratnoi svyaz'yu [The system of hidden data transmission in

medical information systems, based on the chaotic synchronization of generators with delayed feedback]. *Byulleten' meditsinskikh Internet konferentsii – Bulletin of Medical Internet Conferences,* 2014, no. 7, pp. 971-974.

9. *DeepMind sozdast sistemu zapisi meditsinskikh dannykh na blokcheine* [DeepMind will create a system for recording medical data on blokcheyne]. Available at: https://hightech.fm/2017/03/10/blockchan_health_ records (accessed 10.03.2017).

10. Condliffe, J. DeepMind's New Blockchain-Style System Will TrackHealth-Care Records. *MIT Technology Review,* 2017, vol. 5(18), pp. 1-8.

11. Setty, S., Soumya, B., Lidong, Z., Roberts, M. L., Venkatesan, R. Enabling secure and resource-efficient blockchain networks with VOLT. *MSR Technical Report*, 2017, vol. 38, pp. 1-15.

12. Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., Yang, B.-Y. High-speed high-security signatures. *Journal of Cryptographic Engineering,* 2012, no. 2(2), pp. 77–89.

13. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., Felten, E. W. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *SoK: InProceedings of the IEEE Symposium on Security and Privacy,* 2015, pp. 104–121.

14. *Tselostnost' informatsii* [Integrity of information]. Available at: http://wikisec.ru/MediaWiki/index.php?title=%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8 (accessed 26.09.2017).

15. Oliynykov, R., Horbenko, I., Kazymyrov, O., Ruzhentsev, V., Horbenko, Yu. Pryntsypy pobudovy i osnovni vlastyvosti novoho natsional'noho standartu blokovoho shyfruvannya Ukrayiny. *Zakhyst informatsiyi – Ukrainian Information Security Research Journal,* 2015, no. 2, pp. 142-157.

Поступила в редакцию 30.09.2017, рассмотрена на редколлегии 22.11.2017

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОПРЕДЕЛЕНИЯ ТЯЖЕСТИ СОСТОЯНИЯ ПАЦИЕНТОВ С СЕРДЕЧНО-СОСУДИСТЫМИ ПАТОЛОГИЯМИ

В. И. Руженцев, А. С. Доброродняя, Е. В. Высоцкая, Т. А. Кулиш

Работа посвящена организации защиты информации в информационной системе определения тяжести состояния пациентов с сердечно-сосудистыми патологиями. Рассмотрены методы защиты информации, которые применяются в системах подобного типа. Проанализирован и обоснован выбор блочного симметричного шифрования ДСТУ 7624:2014 для защиты данных в информационной системе определения тяжести состояния пациентов с сердечно-сосудистыми патологиями. Этот алгоритм обеспечивает высокий уровень устойчивости от атак, а также скорость программной реализации. Наличие предложенной криптообработки снижает вероятность хищения данных пациента.

Ключевые слова: защита информации, алгоритм, шифрование, патология, данные.

ORGANIZATION OF INFORMATION PROTECTION FOR INFORMATION SYSTEM OF DETERMINATION STATE OF SEVERITY OF THE PATIENTS WITH CARDIOVASCULAR PATHOLOGY

V. I. Ruzhentsev, H.S. Dobrorodnia, O. V. Vysotska, T. O. Kylish

The work is devoted to the organization of information protection in the information system for determining the severity of the condition of patients with cardiovascular pathologies. The analysis of threats to the security of personal data of patients was carried out. A conclusion is drawn about the threats to the information system being developed. To prevent these threats, it is necessary to ensure confidentiality, as well as the integrity of information about the patient. This can be done using cryptographic methods. Medical informational systems and methods which used in them are considered. The shortcomings of the above medical informational systems and methods of information protection are highlighted. The choice of block symmetric encryption of DSTU 7624: 2014 for data protection was analyzed and justified for the information system to determination state of severity of the patients with cardiovascular pathologies. A structural diagram of the information system is formed and its main modules are described. The main stages of encryption using the "Kalina" algorithm (DSTU 7624: 2014) are described. The scheme is presented and the main stages of key unfolding are described. The considered encryption algorithm DSTU

7624: 2014 provides a high level of resistance against attacks, as well as the speed of software implementation, allows you to select the length of the key and data block. The listed advantages of encryption with the use of the algorithm "Kalina" allow you to use it when encrypting medical and biological information, both long-term storage, and in situations where the speed of encryption is not critical. The presence of the proposed cryptography reduces the probability of theft of patient data in the information system for determining the severity of the condition of patients with cardiovascular pathologies.

Keywords: information protection, algorithm, encryption, pathology, data.

Руженцев Віктор Ігорович – канд. техн. наук, доц. каф. безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: viktor.ruzhentsev@nure.ua.

Доброродня Ганна Сергіївна – аспірант каф. біомедичної інженерії, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: hanna.dobrorodnia@nure.ua.

Висоцька Олена Володимирівна – д-р техн. наук, проф. каф. біомедичної інженерії, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: olena.vysotska@nure.ua.

Куліш Тетяна Анатоліївна – студент каф. біомедичної інженерії, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: tredex.tatyana@gmail.com.

Ruzhentsev Victor – PhD, Assossiate Professor of Dept. of Information Technology Security, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, e-mail: viktor.ruzhentsev@nure.ua.

Dobrorodnia Hanna – PhD student of Dept. of Biomedical engineering, Kharkov National University of Radio Electronics, Kharkiv, Ukraine, e-mail: hanna.dobrorodnia@nure.ua.

Vysotska Olena – Doctor of Engineering Sciences, Professor of Dept. of Biomedical engineering, Kharkov National University of Radio Electronics, Kharkiv, Ukraine, e-mail: olena.vysotska@nure.ua.

Kulish Tetyana – student of Dept. of Biomedical engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, e-mail: tredex.tatyana@gmail.com.