удк 61:651.928:681.31:003.26:007

ІДЕОЛОГІЯ РОЗВИТКУ МЕДИЧНИХ ОСНОВ В КРИПТОГРАФІЇ - ВЧОРА ТА СЬОГОДНІ

І. М. Шупяцький

Державна служба спеціального зв'язку та захисту інформації України

В статті проаналізовано історичний розвиток криптографії з зазначенням застосування в захисті медичної інформації.

Ключові слова: ідеологія, криптографія, медицина, інформація, захист.

ИДЕОЛОГИЯ РАЗВИТИЯ МЕДИЦИНСКИХ ОСНОВ В КРИПТОГРАФИИ - ВЧЕРА И СЕГОДНЯ

И. М. Шупяцкий

Государственная служба специальной связи и защиты информации Украины

В статье проанализирована история развития криптографии с определением применения в защите медицинской информации.

Ключевые слова: идеология, криптография, медицина, информация, защита.

IDEOLOGY OF THE MEDICAL BASIS DEVELOPMENT IN THE CRYPTOGRAPHY - YESTERDAY AND TODAY

I. M. Shupiatskyi

State Service for Special Communication and Information Protection of Ukraine

The article analyzed the history of the cryptography development with the purpose to working of the protect medical information.

Key words: ideology, cryptography, medical, information, protect.

Вступ. Термін «криптографія» виник ще за часів древніх греків і перекладається він з грецької як тайнопис.

Поняття «медична безпека» обхоплює широке коло інтересів як окремих суб'єктів, так і цілих держав. У всі історичні часи суттєва увага приділялась проблемі інформаційної безпеки, забезпеченню захисту конфіденційної інформації. Недаремно великий психолог Вільям Шекспір в «Королі Лірі» мовив: «Чтоб мысль врага узнать, сердца вскрывают, а не то, что письма».

З древніх часів існували три способи захисту інформації, в тому числі медичної.

Перший спосіб використовувався через силові методи: охорона медичної документації (носія інформації) фізичними особами, його передача спеціальним кур'єром тощо.

Другий спосіб отримав назву «стеганографія» і полягав в приховуванні самого факту існування інформації (наприклад дані пацієнта). В таких випадках використовувались так звані «симпатичні чорнила». При спеціальному проявленні текст відновлювався. Один з оригінальних прикладів приховування інформації зустрічаємо в трудах древньогрецького історика Геродота. На голові раба, чисто поголеній, писали необхідне повідомлення. Коли волосся відростало, раба відправляли до адресата, який знову голив його голову і читав отримане повідомлення.

Третій спосіб захисту інформації полягає в перекручуванні смислового тексту в такий собі хаотичний набір знаків (букв алфавіту). Отримувач донесення мав можливість перекрутити його в початкове осмислене повідомлення, якщо мав «ключ» до його побудови. Саме цей спосіб захисту інформації називається криптографічним.

На думку ряду спеціалістів, криптографія за своїм віком - ровесниця єгипетських пірамід. В докумен-

тах древніх цивілізацій - Індії, Єгипту, Месопотамії - є дані про системи і способи складання шифрувальних листів.

Постановка проблеми. Використання комплексу проблемних знань криптографічного аналізу медичної інформації допоможе в вирішенні завдань, щодо неможливого розголошення медичних даних при передачі їх на відстань за допомогою сучасних технічних засобів.

В арабському світі в стародавні часи була одна з найрозвиненіших цивілізацій. Шалено розвивалась наука, арабська медицина й математика стали передовими в світі. Зрозуміло, що на тлі такого прогресу постало питання і про розвиток криптографії, джерелом якої є арабська медична наука, коли особливості лікувального процесу і різноманітні знання треба було записувати так, щоб було зрозуміло тільки лікарям. Одне з основних понять криптографії - шифр - має коріння в арабському слові «цифра». Тайнопис та його значення згадується в казках «Тисяча й одна ніч». Одна з перших великих книг, в якій ретельно описується криптографія - це праця, створена Абу Вакр Ахмед бен Али бен Вахшия ан Набати - «Книга про велике бажання людини розгадати загадки стародавньої письменності». В ній описано декілька систем шифрів, саме питання з медичної науки та інших.

В 1412 році Шехаб аль Кашкаіді написав 14-томну енциклопедію «Шауба аль Аша». В цій роботі є розділи про криптографію «Відносно хования в буквах тайних повідомлень». Дано систематичний опис різноманітних шифрів, заміни й перестановок.

Використовуючи криптографію древніх часів, брали за основу два види шифрів: заміна та перестановка.

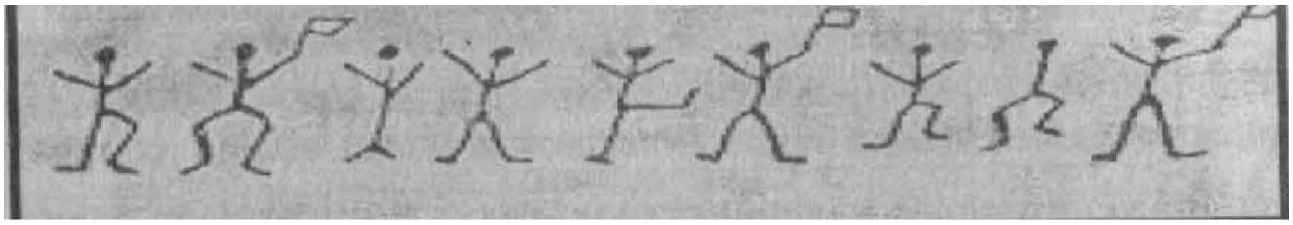
Історичним прикладом шифру заміни, є шифр Цезаря, який свого часу описав історик Стародавнього Риму - Светоній. Гай Юлій Цезар використовував в своїй переписці шифр приватного винахідника - тобто авторський. Щодо сучасної російської мови він складався таким чином. Виписували алфавіт: А, Б, В, Г, Д, Е,.... Після того під ним виписували той же алфавіт, але з циклічним зсувом на три букви вліво:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ы Ъ Ь Э Ю Я

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ы Ъ Ь Э Ю Я А Б В

При шифруванні буква А змінювалась на Г, Б змінювалась на Д, В - Е і так далі. Так наприклад слово «РИМ» переходило в слово «У Л П ». Отримувач повідомлення «У Л П» шукав ці букви в нижньому рядку і по буквах над ними відновлював отримане слово «РИМ». Ключем в шифрі Цезаря є величина зсуву другго нижнього рядка алфавіту.

В художній літературі класичним прикладом шифру є відомий шифр «Танцюючі люди» (К. Дойля). В ньому букви тексту були замінені на символічні фігурки людей. Ключем такого шифру є пози людей , що замінюють букви. Фрагмент шифрувального посланння мав наступний вигляд:



Отриманий текст: I'm here Abe Slaney» («Я тут Аб Слени»). Використано шифр простої заміни букв на фігурки людей, прапорець в руках це ознака кінця слова.

В середині ХУІ сторіччя в Італії вийшла книга математика, лікаря і філософа Дж. Кардано „О тонкостях" с дополнением „О разных вещах" де мова йде не тільки про особливості діагностування та лікування захворювань, але є розділи з криптографії. В книзі знайшли відображення нові ідеї криптографії, що використовували частини самого активного відкритого тексту в якості ключа шифру і новий спосіб шифрування, який увійшов в історію як «решітка Кардано». Для її виготовлення використовували лист твердого матеріалу (картон, пергамент, метал), що представляв собою квадрат, в якому є «вікна». При шифруванні решітка накладалась на лист паперу і букви відкритого тексту вписувались у «вікна». При використанні всіх «вікон» решітка поверталась на 90 градусів, і знову букви відкритого тексту вписувались у «вікна» повернутої решітки. Потім знову робився поворот на 90 градусів тощо. В один «захід» решітка працювала 4 рази. Якщо текст був зашифрований не повністю, то решітка ставилась в першу позицію і вся процедура повторювалась. Зрозуміло, що це не що інше, як шифр перестановки.

Головна вимога щодо решітки Кардано - при всіх обертах «вікна» не повинні попадати на одне й те саме місце в квадраті, в якому утворюється шифротекст.