$$
\begin{array}{ll}
 & \begin{matrix} 3 & 4 & 5 \end{matrix} \\
S_1 = \{5,1\} & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
S_2 = \{4,2\} & \\
S_3 = \{4,1\} & \\
S_4 = \{3,2,1\} &
\end{array}
$$

Для перетвореної матриці стратегії S_2 та S_3 для S стають рівнозначними. Після їх об'єднання в одну стратегію матриця гри звелася до одиничної.

Таким чином, оптимальною стратегією H є ховати предмет в 3-й, 4-й або 5-й ящик з ймовірностями 1/3. Оптимальною стратегією S є застосування мішаної стратегії, в якій S_1 та S_4 вибираються з ймовірностями 1/3, а S_2 та S_3 можна змішувати в будь-якій пропорції, але так, щоб сума ймовірностей їхнього вибору складала 1/3.

Література

1. *Мазалов В.В*. Математическая теория игр / В. В. Мазалов. — СПб.: Лань, 2010. — 446 с.

2. *Петросян Л.А*. Теория игр / Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В. — СПб. : БХВ-Петербург, 2012. — 432 с.

3. *M. Osborne*. A course on game theory / M. Osborne, A. Rubinstein // The MIT Press, 1994. — 352 p.

УДК 336.1.0018

Бабинюк О. І., асистент
кафедри комп'ютерної математики та інформаційної безпеки ФІСІТ,
Київський національний економічний університет імені Вадима Гетьмана

ЗАСТОСУВАННЯ МЕТОДІВ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Щоб думку ворога дізнатися, серця розкривають,
а не те що листи.
У. Шекспір «Король Лір»

АНОТАЦІЯ. Викладено етапи розвитку становлення криптографічного захисту інформації. Висвітлено проблеми захисту даних в інформаційних системах і проблеми розподілу ключів у криптографії. Розглянуто

шляхи розв'язку проблем з використанням сучасних методів квантової криптографії та стеганографії. Описано недоліки даних технологій.

КЛЮЧОВІ СЛОВА: криптографія, криптографічні ключі, квантова криптографія, стеганографія, протоколи, одностороння функція.

АННОТАЦИЯ. Изложены этапы развития становления криптографической защиты информации. Освещены проблемы защиты данных в информационных системах и проблемы распределения ключей в криптографии. Рассмотрены пути решения проблем с использованием современных методов квантовой криптографии и стеганографии. Описаны недостатки данных технологий.

КЛЮЧЕВЫЕ СЛОВА: криптография, криптографические ключи, квантовая криптография, стеганография, протоколы, односторонняя функция.

ABSTRACT. Set out stages of the formation of cryptographic protection. Highlights the problem of data protection in information systems and key distribution problem in cryptography. The ways of solution of problems using modern methods of quantum cryptography and steganography. Disadvantages of these technologies.

KEY WORDS: cryptography, cryptographic keys, quantum cryptography, steganography, minutes, one-way function.

Вступ. Розвиток сучасного суспільства нерозривно пов'язаний зі зростанням інформаційної складової (інформаційні ресурси, інформаційні технології тощо) і, як наслідок, інформаційної безпеки. Питання інформаційної безпеки на сучасному етапі розглядаються як пріоритетні в державних структурах, у наукових закладах і в комерційних фірмах. Інформаційні системи спеціального призначення (банківські системи, силові структури тощо), будучи пріоритетними в структурі держави, не можуть залишатися в питаннях забезпечення ***інформаційної безпеки*** тільки на рівні традиційних засобів: криптографічний захист, удосконалення систем розподілу доступу, реалізація спеціальних вимог для абонентського трафіку, проведення організаційних заходів щодо посилення режиму.

Не має сенсу перераховувати всі переваги, які отримує організація, підключаючись до мережі Інтернет. Проте при цьому потрібно враховувати і негативні сторони такої акції. У загальнодоступній мережі — це можливі атаки на підключені до неї локальні мережі та комп'ютери. Загальновідомо, що щорічні збитки завдяки недостатнього захисту корпоративних інформаційних систем обчислюються десятками мільйонів доларів.

На сучасному етапі розвитку інформаційних технологій найнадійніші засоби вирішення питань забезпечення певних інтересів (державних, комерційних, особистих та ін.) дає ***криптографія***

— наука про застосування математичних методів для перетворення (шифрування) інформації з метою її захисту від незаконних користувачів. Криптографія ґрунтується на останніх досягненнях фундаментальних наук і в першу чергу — математики.

1. Історичний огляд. Проблема захисту інформації шляхом її перетворення, що виключає її прочитування сторонньою особою, хвилювала людський розум з давніх часів. Історія криптографії — ровесниця історії людської мови. Більш того, спочатку писемність сама по собі була криптографічного системою, тому що в стародавніх суспільствах нею володіли лише обрані. Священні книги Стародавніх Єгипту та Індії тому приклади.

Криптографія як прикладна наука дістала свій розвиток ще з 20 ст. до н. е. Так, наприклад, при розкопках давньої цивілізації в Месопотамії знайдено глиняні таблички, що містять тайнопис про глазурування гончарних виробів, тобто перші шифротексти носили деякий комерційний характер. Надалі стали шифруватися тексти медичного характеру, купівлі-продажу худоби та нерухомості. Подальший розвиток, підготовка та передача зашифрованих текстів отримали при веденні бойових дій. Відносна широкомасштабність воєнних заходів привела до необхідності розробки та впровадження засобів «малої механізації» для шифрування секретних повідомлень.

Багатовікова історія розвитку науки криптографії показує, що відносно донедавна вона була спрямована на побудову криптографічних систем військового призначення. Проте в останні десятиліття цей науковий напрям знайшов широке застосування практично у всіх сферах людської діяльності, виконуючи функції як криптографічного захисту електронних повідомлень від несанкціонованого сприйняття і розпізнавання, так і аутентифікації (підтвердження автентичності) прийнятих електронних повідомлень з використанням інструментарію електронного цифрового підпису.

Великий вплив на розвиток криптографії здійснили праці американського математика Клода Шеннона, які з'явилися в середині XX ст. [1]. У цих працях було закладено основи теорії інформації, а також було розроблено математичний апарат для досліджень у багатьох галузях науки, пов'язаних з інформацією.

Для того щоб доводити математичні теореми, потрібно чітко визначити об'єкти, з якими ми маємо справу. При шифруванні тексту необхідно, в першу чергу, знати, які символи можуть у ньому зустрічатися або, простіше кажучи, знати алфавіт.

На теперішній час розроблено велику кількість різноманітних методів шифрування, створені теоретичні та практичні основи їх

застосування. Більшість цих методів може бути успішно застосовано і для закритої інформації.

2. Сучасні методи криптографічного захисту. Сучасна криптографія містить чотири великі розділи:

1. Симетричні криптосистеми.
2. Криптосистеми з відкритим ключем.
3. Системи електронного підпису.
4. Управління ключами.

Основні напрямки використання криптографічних методів — передача конфіденційної інформації з каналів зв'язку (наприклад, електронна пошта), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

Для шифрування відкритих електронних повідомлень при передачі їх за відкритими загальнодоступними каналами, включаючи і канали інтернет-технологій, використовують три основні методи:

- симетричний (одноключовий) — перетворення відкритих повідомлень;
- асиметричний (двоключовий) — перетворення відкритих повідомлень (криптографія з відкритим ключем);
- комбінований — перетворення відкритих повідомлень.

Найширше втілення у відкритих мережевих комп'ютерних технологіях на сучасному етапі розробок і експлуатації криптографічних систем захисту та аутентифікації електронних документів і повідомлень отримали комбіновані криптографічні системи, що поєднують у собі переваги симетричних і асиметричних перетворень.

Метод асиметричного перетворення відкритих повідомлень реалізований у криптографічних системах з відкритим ключем. Подальшим розвитком методу асиметричного перетворення, що дістав на сучасному етапі найбільше поширення і визнаний як найперспективніший, став ідентифікований метод побудови криптографічних систем, побудований на теоретичних положеннях еліптичних кривих. Спочатку теорію побудови криптографічних систем на основі асиметричних методів необхідно розглянути в базисі криптосистем з відкритим ключем.

Вперше концепція криптографічних перетворень з відкритим ключем була запропонована Унтфілдом Діффі (Whitfield Diffie) і Мартіном Хеллманом (Martin Hellman) [8], яка була подана на Національної комп'ютерної конференції (National Computer Conference) в 1976 році. Ця ж концепція була закладена і в основу

аутентифікації електронних повідомлень (електронний цифровий підпис). Найбільшого поширення при реалізації криптографічних систем з відкритим ключем отримали методи, розроблені ще в 1978 р. трьома авторами Р. Райвест (Rivest), А. Шамір (Shamir) і А. Адлеманом (Adleman). Цей алгоритм отримав найменування по буквах прізвищ авторів — алгоритм RSA (Rivest-Shamir-Adleman).

Наступним алгоритмом криптографічних перетворень з відкритим ключем став широко застосовуваний у практичній діяльності інформаційних технологій алгоритм дискретного логарифмування Ель Гамаля. Ель Гамаль, американський учений-математик арабського походження, в 1985 р. запропонував алгоритм шифрування та електронного цифрового підпису, заснований на складності обчислення дискретних логарифмів у кінцевому полі.

У 1985 р. американськими вченими Нілом Коблиця (Neal Koblitz) і Віктором Міллером (Viktor Miller) запропоновано новий метод криптографічних перетворень з відкритими ключами — метод дискретного логарифмування в метриці еліптичних кривих [5]. З 1998 р. використання еліптичних кривих у прикладних криптографічних задачах шифрування та аутентифікації електронних повідомлень було закріплено в стандартах США ANSI X9.62 і FIPS 182-2, у 2001 р. в Російській Федерації було прийнято аналогічний стандарт на електронний цифровий підпис ГОСТ Р34.10-2001.

Основна перевага криптографічних систем, побудованих на алгоритмах перетворень у метриці еліптичних кривих, у порівнянні з методом факторизації великих чисел (розклад великих чисел на прості множники) — алгоритмом RSA і методом дискретного логарифмування (алгоритм Ель Гамаля) полягає в досягненні значно більшої криптостійкості при рівних розмірах ключів шифрування-дешифрування і однаковою криптостійкості при значно менших розмірах ключів шифрування-дешифрування. Наприклад, при однаковому рівні криптостійкості в алгоритмі RSA розміри ключів перетворення складають 1024 біт, а в алгоритмі перетворення на еліптичних кривих розміри ключів перетворення складають 160 біт, що забезпечує більшу простоту програмної та апаратної реалізації криптографічних систем захисту та аутентифікації електронних повідомлень.

3. Математичні моделі криптографії. Основними поняттями, на яких базується теорія криптографічних перетворень, є елементи модулярної алгебри: знаходження числа за модулем, операція обчислення зворотних величин за модулем, мала теоре-

ма Ферма, розширений алгоритм Евкліда для знаходження зворотних величин, алгоритм піднесення до степеня за модулем.

У багатьох криптографічних задачах для заданих чисел a та P потрібно знайти число d, що менше за P ($d<P$), щоб виконати одиничне порівняння $a \cdot d \cdot mod\ P \equiv 1$. Потрібно відмітити, що таке число d існує, якщо числа a і P взаємно прості, при цьому число d називають інверсією числа a по модулю P, та позначають як: $a^{-1} \cdot mod\ P$.

Для обчислення зворотних величин при умові, що P — просте число, що практично справедливо для всіх криптографічних задач асиметричної криптографії, використовують малу теорему Ферма:

Якщо P просте число, то інверсію числа a по модулю P можна визначити як:

$$a^{-1} \cdot (mod\ P) = a^{\varphi(P)-1} mod\ P,$$

де $\varphi(P)$ — функція Ейлера, для простих чисел $\varphi(P)=P-1$. Функція Ейлера вказує скільки в множині чисел від 0 до P є чисел взаємно простих з P.

У 1983 р. в книжці «Коди та математика» М. Н. Аршинова і Л. Є. Садовського було написано: «Прийомів тайнописі — дуже багато, і, скоріше за все, це область, де вже не має потреби придумувати ще щось суттєво нове». Проте, це була чергова велика омана щодо криптографії. Ще в 1976 році була опублікована праця молодих американських математиків У. Діффі і М.Е. Хеллмена «Нові напрямки в криптографії», яка не тільки істотно змінила криптографію, але й привела до появи і бурхливого розвитку нових напрямків у математиці. Розглянемо основні поняття «нової криптографії».

Односторонньою називається функція $F: X \rightarrow Y$, що має дві властивості:

а) існує поліноміальний алгоритм обчислення значень $F(x)$;

б) не існує поліноміального алгоритму інвертування функції F, тобто розв'язку рівняння $F(x) = y$ відносно x.

Одностороння функція суттєво відрізняється від звичайних математичних функцій завдяки обмеженням на складність її обчислення та інвертування. Існування односторонньої функції не доведено, але вивчення властивостей цього, поки що гіпотетичного об'єкту, дозволило встановити його зв'язок із іншими більш вивченими об'єктами. Вдалося довести, що проблема існування односторонньої функції еквівалентна одній з добре відомих невирішених проблем — «чи збігаються класи складнощів P і NP»?

Говорячи неформально, клас P складається із завдань з поліноміальною складністю. Більш строго, клас P — це клас мов, які розпізнаються за поліноміальний час надетермінованою машиною Тьюрінга. Якщо таку машину Тьюринга доповнити гіпотетичною здатністю «вгадування», виходить більш сильна модель — недетермінована машина Тьюрінга. Клас NP — це клас мов, які розпізнаються за поліноміальний час на недетермінованій машині Тьюрінга. Проблема збігу класів P і NP — це проблема співвідношення можливостей двох моделей обчислень: детермінована і недетермінірована машина Тьюрінга.

Іншим поняттям, ближчим до традиційної криптографії, в якій є секретний ключ, є поняття односторонньої функції з секретом. Іноді ще вживаються терміни функція з пасткою, функція потайної двері (англійська назва: one-way trap-door function).

Односторонньою функцією з секретом K називається функція $F_K: X \to Y$, яка залежить від параметра K і має три властивості:

а) при будь-якому K існує поліноміальний алгоритм обчислення значень $F_K(x)$;

б) при невідомому K не існує поліноміального алгоритму інвертування F_K;

в) при відомому K існує поліноміальний алгоритм інвертування F_K.

Про існування односторонньої функції з секретом можна сказати теж саме, що було сказано раніше про односторонні функції. Для практичних цілей у криптографії побудовано кілька функцій, які можуть виявитися односторонніми. Це означає, що для них властивість б) поки що не доведено, але відомо, що задача інвертування еквівалентна деякій важкій математичній задачі, яка давно вивчається.

На початку 1977 року американські фахівці з комп'ютерних наук Р. Рівест, А. Шамір і Л. Адлеман придумали одну таку функцію [6]. Система на основі цієї функції виявилася дуже практичною і отримала широке поширення під назвою «система RSA» по першим англійським буквах прізвищ авторів.

Опишемо систему RSA. Нехай $n = pq$, де p і q — великі прості числа, а e — деяке число, взаємно просте з $\varphi(n)$. Знайдемо число d з рівняння:

$$d \cdot e = 1 \ (\mathrm{mod}\varphi(n)).$$

Числа p, q і d будемо вважати *секретними* і позначимо секрет $K = \{p, q, d\}$. Числа n і e будем вважати *загальнодоступними*. Нескінчені множини відкритих повідомлень X і зашифро-

ваних повідомлень Y будемо вважати рівними: $X = Y = \{1, 2, ..., n\text{-}1\}$.

Функцію F_K: $X \to Y$ визначимо рівністю: $F_K(x) = x^e \pmod n$.

Властивість а) односторонньої функції з секретом для F_K наочна. Перевіримо властивість в). Для цього просто вкажемо, як при відомому K інвертувати функцію F_K: рішенням рівняння $F_K(x) = y$ буде $x = y^d \pmod n$. Для доведення наведемо необхідні викладки: $d \cdot e = \varphi(n) \cdot m + 1$, $(x^e)^d \pmod n = x^{\varphi(n)\cdot m+1} \pmod n = (x^{\varphi(n)\cdot m} \cdot x \pmod n = (1)^m \cdot x \pmod n = x$.

Властивість б) для функції F_K строго не доведено. Поки загальновизнано, що для інвертування F_K необхідно розкласти n на множники, а завдання факторизації цілих чисел належить до важких математичних завдань.

Таким чином, описану функцію F_K можна вважати з деяким припущенням односторонньої функції з секретом.

Функцію з секретом можна також використовувати для цифрового підпису повідомлень, який неможливо підробити за поліноміальний час. Розвиток і узагальнення ідей, використаних при побудові схем цифрового підпису, привело до створення великого нового напряму теоретичної криптографії — теорії криптографічних протоколів. Об'єктом вивчення цієї теорії є віддалені абоненти, які взаємодіють, як правило, по відкритих каналах зв'язку.

Подальший розвиток теорії криптографічних протоколів стимулюється їх численними практичними додатками, особливо в банківських платіжних системах, в системах електронного документообігу, в комп'ютерних мережах і т. д. Осмислення різних протоколів і методів їх побудови привело в 1985—1986 рр. до появи двох плідних математичних моделей — інтерактивної системи доказів і докази з нульовим розголошенням [9].

4. Імовірнісне шифрування. Шафі Гольдвассер (Goldwasser) і Сильвіо Мікелі (Micali) ввели поняття імовірнісного шифрування, яке є дуже цікавим різновидом криптографії з відкритим ключем. Коли певне повідомлення зашифровується за допомогою ймовірнісного шифрування, то в цьому випадку при криптоаналізі шифротекста стає однаково важко з'ясувати про повідомлення будь-якої інформації, яка дозволила б відновити весь його відкритий текст. Крім того, існує ймовірнісна схема шифрування, яка є швидшою, ніж запропонована до цього схема шифрування з відкритим ключем RSA. Подібні криптографічні системи називаються імовірнісними у зв'язку з тим, що в них шифрування повідомлень, які мають один і той же вихідний текст і шифруються

з використанням одного і того ж ключа, може в різний час привести до абсолютно різних шифр текстів.

Криптографія з відкритим ключем у значній мірі розв'язує проблему розповсюдження ключів, яка є достатньо серйозною для криптографії з секретним ключем. Однак при перехопленні шифр тексту $y = F_K(x)$ завжди стає відомою деяка інформація про відкритий текст x, оскільки криптоаналітик може обчислити без сторонньої допомоги відкриту функцію шифрування F_K для будь-якого тексту, що йому відповідає.

Задаючи довільно x^* за власним вибором, він може визначити, чи правильно, що $x = x^*$, так як це справедливо лише, якщо $F_K(x^*) = y$.

Навіть якщо визначення x із y і було б важко здійсненим завдяки знанню тільки природного алгоритму шифрування, то невідомо, як знайти, наскільки велика і яка саме повинна бути цей частковий витік інформації.

Ціллю імовірнісного шифрування є кодування повідомлень таким чином, щоб ніяке легко виконуване обчислення на основі шифр тексту не могло б дати якої б то не було інформації про відповідний відкритий текст (крім хіба що з нехтовно малою ймовірністю).

Формально система імовірнісного шифрування складається з простору ключів K і для кожного k з простору K — просторів повідомлень відкритих текстів X_k імовірнісних просторів R_k і пар функцій F_k: $(X_k \cdot R_k) > Y_k$ і $Y_k > X_k$, таких, що $D_k(F_k(xr)) = x$ для будь-якого повідомлення відкритого тексту x із X_k і випадкового числа r із R_k.

За допомогою будь-якого k із K повинні легко отримуватися ефективні алгоритми для обчислення як F_k, так і D_k , але повинен важко отримуватися будь-який ефективний алгоритм обчислення D_k при заданому лише природному алгоритмі обчислення F_k. Система імовірнісного шифрування, що використовується таким чином, дуже схожа на систему з відкритим ключем. Один раз і назавжди кожний користувач вибирає ключ k із K, який використовується для отримання обох природних алгоритмів обчислення F_k і D_k. Він робить алгоритм шифрування F_k публічно доступним і зберігає у секреті алгоритм дешифрування D_k. У тому випадку, коли інший користувач захоче надіслати йому своє повідомлення x, він знаходить F_k у довіднику, випадково обирає деяке r із R_k і обчислює шифр текст $y = F_k(xr)$. Використовуючи свій власний секретний код тільки законний отримувач зможе легко визначити x з y.

Незважаючи на значні теоретичні властивості, оригінальна система імовірнісного шифрування Гольдвассера—Мікалі мала свої недоліки: дуже велике розкриття даних, що призвело до зменшення практичного значення. Незважаючи на це, імовірнісне кодування досягло зараз такого стану, при якому схема, що існує не теперішній час, більш ефективна, ніж RSA. Для цілей секретності (але не аутентифікації) — це схема Блюма і Голдвассера є найкращою з того, що змогла запропонувати наука. Вона заснована на вірі в те, що піднесення до квадрату по модулю цілого числа Блюма є односторонньою функцією з секретом і на криптографічно сильному псевдовипадковому бітовому генераторі [4, 7].

5. Квантова криптографія. Базовим питанням криптографії є шифрування даних і аутентифікація відправника. Задача безпечної пересилки ключів може бути вирішена за допомогою квантової розсилки ключів QKD (Quantum Key Distribution). Надійність методу ґрунтується на непорушності законів квантової механіки. Зловмисник не може відвести частину сигналу з передавальної лінії, так як не можна поділити електромагнітний квант на частини. Будь-яка спроба зловмисника втрутитися в процес передачі викличе непомірно високий рівень помилок. Ступінь надійності в даній методиці вище, ніж у випадку застосування алгоритмів з парними ключами (наприклад, RSA). Тут ключ може генеруватися під час передачі по абсолютно відкритому оптичному каналу. Швидкість передачі даних при цій техніці не висока, але для передачі ключа вона і не потрібна. Квантова криптографія може замінити алгоритм Діффі—Хелмана, який у даний час часто використовується для пересилки секретних ключів шифрування по каналах зв'язку.

Перший протокол квантової криптографії (BB84) був запропонований і опублікований в 1984 р. Беннетом і Брассард. Пізніше ідея була розвинена Екертом в 1991 р. В основі методу квантової криптографії лежить спостереження квантових станів фотонів. Відправник задає ці стани, а одержувач їх реєструє. Тут використовується квантовий принцип невизначеності, коли дві квантові величини не можуть бути виміряні одночасно з необхідною точністю. Так, поляризація фотонів може бути ортогональною, діагональною або циркулярною. Вимірювання одного виду поляризації рендомізує (спосіб вибору так, щоб кожна подія мала однакову або залежну ймовірність бути вибраною) іншу складову. Таким чином, якщо відправник і одержувач не домовилися між собою, який вид поляризації брати за основу, одержувач може зруйнувати посланий відправником сигнал, не отримавши ніякої корисної інформації.

Відправник кодує дані, що відправляються, задаючи певні квантові стани, одержувач реєструє ці стани. Потім одержувач і відправник спільно обговорюють результати спостережень. Зрештою з як завгодно високою вірогідністю можна бути впевненим, що передана і прийнята кодові послідовності тотожні. Обговорення результатів стосується помилок, внесених шумами або зловмисником, і ні в найменшій мірі не розкриває вмісту надісланого повідомлення. Може обговорюватися парність повідомлення, але не окремі біти. При передачі даних контролюється поляризація фотонів. Поляризація може бути ортогональної (горизонтальної або вертикальної), циркулярної (лівої чи правої) і діагональної (45^0 або 135^0).

Як джерело світла може використовуватися світловипромінювальний діод або лазер. Світло фільтрується, поляризується і формується у вигляді коротких імпульсів малої інтенсивності. Поляризація кожного імпульсу модулюється відправником довільним чином відповідно до одним з чотирьох перерахованих станів (горизонтальна, вертикальна, ліво- або правоциркулярна).

Одержувач вимірює поляризацію фотонів, використовуючи довільну послідовність базових станів (ортогональна або циркулярна). Одержувач відкрито повідомляє відправнику, яку послідовність базових станів він використовував. Відправник відкрито повідомляє одержувача про те, які базові стану використані коректно. Усі вимірювання, виконані при невірних базових станах, відкидаються. Вимірювання інтерпретуються згідно двійковій схемі: ліво-циркулярна поляризація або горизонтальна — 0, право-циркулярна або вертикальна — 1. Реалізація протоколу ускладнюється присутністю шуму, який може викликати помилки. Помилки, що вносяться, можуть бути виявлені й усунені за допомогою підрахунку парності, при цьому один біт з кожного блоку відкидається.

6. Стеганографія. На відміну від криптографії, метою якої є приховування даних за рахунок їх шифрування, метою стеганографії є приховування самого факту передачі конфіденційних повідомлень.

Стеганографія, як молода наука про непомітне і стійке приховування даних, отримує широке застосування в галузях діяльності, які пов’язані зі збереженням і захистом інформації. Непомітність приховування даних має на увазі обов’язкове включення людини до системи стеганографічної передачі даних. Людина розглядається тут як додатковий приймач даних, що пред’являє до стеганографічної системи достатньо важко формалізовані вимоги. Саме завдяки стеганографічним інструментам захисту до-

сягається найбільший ріень стійкості до навмисних атак з метою руйнування або виявлення інформації, що приховується.

Комп'ютерна сеганографія — напрям класичної стеганографії, який заснований на особливостях комп'ютерної платформи представлення й обробки даних.

Цифрова стеганографія — напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів [10].

Як правило, дані об'єкти є мультимедіа-об'єкти (зображення, відеопотоки, аудіодані, текстури 3D-об'єктів) і внесення спотворень, що розташовані нижче від порога чутливості органів чуття середньостатистичної людини, не призводить до помітних змін. В оцифрованих даних, які спочатку мають аналогову природу, завжди присутній шум квантування, а при відтворенні цих даних з'являється додатковий аналоговий шум внаслідок нелінійних спотворень в апаратурі. Все це сприяє більшій непомітності прихованої інформації [11].

У цифровій стеганографії найбільш популярними областями вбудовування секретних повідомлень є просторові, і/або тимчасові, і/або частотні параметри цифрових аудіоконтейнерів і контейнерів-зображень. Тому дослідження допустимої модифікації параметрів контейнера і його інформаційної надмірності представляє безперечний інтерес.

На сьогодні завдання пошуку оптимальних контейнерів і методів вбудовування повністю не вирішена. Чималий внесок у розвиток стеганографії внесли вчені Японії, Швейцарії, Англії, Сполучених Штатів Америки, Сербії, України та Росії. Як правило, найефективніші стеганоалгоритми є закритими для широкого використання. Часто найстійкіші до атак алгоритми не дозволяють вбудувати достатній обсяг секретної інформації у файл-контейнер. Розробка таких алгоритмів вбудовування, які, з одного боку, підвищують стеганостійкість каналу, а з другого — зберігають обсяг переданих секретних даних, значно поліпшить якість конфіденційного каналу зв'язку.

Поряд з пошуком оптимальних параметрів контейнера і методів вбудовування, однією з актуальних завдань у даний час є виявлення факту приховування інформації [12]. Тому особливу значимість являє собою розробка нових способів і алгоритмів виявлення факту наявності вбудованих даних, а також локалізації стеганографічної вбудованої інформації у файлі-контейнері.

Висновки. Таким чином, криптографічні методи захисту інформації можна застосовувати як для захисту інформації, що об-

робляється в ЕОМ або зберігається в різного типу ЗП, так і для закриття інформації, що передається між різними елементами системи по лініям зв'язку. На теперішній час розроблено велику кількість різноманітних методів шифрування, створені теоретичні та практичні основи їх застосування. Отже, проблема використання криптографічних методів в інформаційних системах стала зараз особливо актуальна. Пояснити це можна тим, що, з одного боку, розширилося використання комп'ютерних мереж, зокрема глобальної мережі Інтернет, по яких передаються великі обсяги інформації державного, військового, комерційного і особистого характеру, що не дозволяє можливість доступу до неї сторонніх осіб. З другого боку, поява нових потужних комп'ютерів, технологій мережевих і нейронних обчислень зробило можливим дискредитацію криптографічних систем, які донедавна вважалися такими, що практично не розкривалися.

Підтвердженням актуальності криптографічних методів є те, що, номінантами премії Тьюрінга (премія Тюрінга (англ. Turing Award) — найпрестижніша премія в інформатиці, що вручається Асоціацією обчислювальної техніки за видатний науково-технічний внесок у цій галузі) за 2012 р. знову стали криптологи. Нагороду отримали Сільвіо Мікалі (Silvio Micali) і Шафі Гольдвассер (Shafi Goldwasser) за новаторські роботи з імовірнісного шифрування (у тому числі за першу вірогідну криптосистему з відкритим ключем) і роботи із застосування доказів з нульовим розголошенням у криптографічних протоколах.

Отже, квантова криптографія розвивається досить швидко, і вже існують і функціонують промислові системи КК, які починають впроваджуватися в життя і роблять її безпечнішою, забезпечуючи практично 100 % захист ключа та інформації. У найближчому майбутньому весь криптографічний захист і розподіл ключів будуть базуватися на квантово-криптографічних системах.

Література

1. *Шеннон К. Э.* Теория связи в секретных системах / К. Э. Шеннон // Работы по теории информации и кибернетике. — М. : ИЛ, 1963.

2. *Дориченко С. А.* 25 этюдов о шифрах / С. А. Дориченко, В. В. Ященко

3. *Ященко В. В.* Введение в криптографию / [под общей ред. В. В. Ященко]. — СПб.: Питер, 2001. — 288 с.

4. *Brassard J.* Modern Criptology Springer-Verlag, Berlin — Heidelberg, 1988. — 107 p.

5. *Goldwasser, S.* Mlcali, S., “Probabilistic encryption” // Journal of Computer and System Sciences, vol. 28. — 1984. — P. 270–299.

6. *Rivest, R. L., Shamir, A., Adleman, L.M.* “A method for obtaining digital signatures and public-key cryptosystems” // Communications of the ACM, vol. 21. — 1978. — P. 120–126.

7. *Blum, M., Goldwasser, S.,* “An efficient probabilistic public-key encryption scheme which hides all partial information”, Advances in Cryptology: Proceedings of Crypto 84, August 1984, Springer-Verlag,. — P. 289–299.

8. *Diffie, W., Hellman, M. E.,* “New directions in cryptography” // IEEE Transactions on Information Theory, vol. IT-22. — 1976. — P. 644-654.

9. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM J. Comput. — V. 18. — № 1. — 1989. — P. 186–208.

10. *Конахович Г.Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

11. *Johnson, N. F.* Steganography: Seeing the Unseen / Neil F. Johnson, S. Jajodia // IEEE Computer. — 1998. — № 2. — P. 26-34.

12. *Westfeld, A*. Attacks on Steganographic Systems / A. Westfeld, A. Pfitzmann // Lecture Notes In Computer Science: The Third International Workshop on Information Hiding, Dresden, Germany, September 29 — October 1, 1999 / Editor: Andreas Pfitzmann. — Springer, Germany, 2000. — P. 61-75.

УДК 681.518

Данильченко Т. В., к.т.н.,
доцент кафедри інформаційних систем в економіці,
Київський національний економічний університет імені Вадима Гетьмана

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДІАГНОСТИКИ ТА МОНІТОРИНГУ

Анотація. У статті розглянуто основні етапи побудови та реалізації системи підтримки прийняття рішень для лікування, діагностики та моніторингу хворих на тиреотоксичне серце.

Ключові слова: система підтримки прийняття рішень, лікар-користувач, лікар-експерт, база даних, база знань, алгоритм, захворювання, множина діагнозів, множина симптомів.

Annotation. The article describes the main stages of construction and implementation of decision support systems for the treatment, diagnosis and monitoring of patients with thyrotoxic heart.

Key words: decision support system, the physician-user physician expert database, knowledge base, algorithm disease, multiple diagnoses, the set of symptoms.