http://dspace.nbuv.gov.ua:8080/dspace/bitstream/123456789/300/1/Проскудина_1.pdf, 2010 4. Сравнительный анализ функциональных возможностей систем электронных библиотек / К.А. Кудим, Г.Ю. Проскудина, В.А. Резниченко // Пробл. програмув. – 2007. – № 4. – С. 32–49. 5. DSpace open source software, -URL: http://www.dspace.org, 2010. 6. Андрухів А.І., Тарасов Д.О. Методи та засоби побудови електронного архіву у Науково-технічній бібліотеці Національного університету "Львівська політехніка" / А. Андрухів, Д. Тарасов // "Сучасні проблеми діяльності бібліотек в умовах інформаційного суспільства", наук.-практ. конф. (2009; Львів). Матеріали науково-практичної конференції "Сучасні проблеми діяльності бібліотеки в умовах інформаційного суспільства," Львів, 12 лист. 2009 р.: до 165-річчя Нац. ун-ту "Львівська політехніка" / Нац. ун-т "Львівська політехніка", Наук.-техн. б-ка ; редкол.: О.В. Шишка [та ін.]. – Л. : Вид-во Нац. ун-ту "Львівська політехніка". – 2009. – С. 37–48. 7. Тарасов, Д.О. Технологічні особливості опрацювання документів у електронній формі у бібліотеках / Д.О. Тарасов // Інформаційні системи та мережі: (зб. наук. пр.) / відп. ред. В.В. Пасічник. – Л.: Вид-во Нац. ун-ту "Львівська політехніка", 2008. – С. 229–232. – (Вісник Нац. ун-ту "Львівська політехніка"; № 610).

УДК 004.02

В.А. Висоцька, О.Р. Гарасим
Національний університет “Львівська політехніка”,
кафедра інформаційних систем та мереж

МЕТОД ВИБОРУ ОПТИМАЛЬНОГО АЛГОРИТМУ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вирішується завдання оптимізації вибору алгоритму криптографічного захисту інформації для електронного урядування в Україні за допомогою нелінійної згортки критеріїв на основі методу аналізу ієрархій з урахуванням вимог: безпека, швидкість, характеристика алгоритму. В результаті визначено оптимальний криптоалгоритм, який забезпечує цілісність та доступність інформації під час функціонування електронного урядування, автентифікацію користувачів та неможливість заперечення факту відправлення/отримання інформації.

Ключові слова: електронне урядування, криптоалгоритм, оптимізація вибору.

In the paper a task of cryptographic information security algorithm choice optimization is solving for an electronic management in Ukraine by nonlinear criteria convolution on the basis of hierarchy analysis method taking into account such requirements as safety, speed, algorithm description. As a result it was defined an optimal cryptographic algorithm, which provides integrity and availability of information during functioning electronic management, users authentication and impossibility of fact information sending/receipt denial.

Keywords: electronic management , cryptographic algorithm, optimization selection.

Вступ. Загальна постановка проблеми

Під електронним урядуванням («е-урядуванням») розуміють спосіб організації державної влади за допомогою систем локальних інформаційних мереж та сегментів глобальної інформаційної мережі, що забезпечує функціонування органів влади в режимі реального часу та робить максимально простим і доступним щоденне спілкування з ними громадян, юридичних осіб, неурядових організацій. На практиці це означає організацію управління державою та взаємодії з фізичними, юридичними особами та громадськими організаціями з максимальним використанням в органах публічної адміністрації сучасних інформаційних технологій [1]. Тобто е-урядування

передбачає, що будь-яка особа через інформаційно-комунікаційні засоби може звертатися до органів державної влади, органів місцевого самоврядування для отримання необхідної інформації, і, головне, – для одержання адміністративних послуг.

Зв'язок висвітленої проблеми із важливими науковими та практичними завданнями

Фахівці в галузі захисту інформації підкреслюють, що реальні масштаби комп'ютерної злочинності нікому не відомі, а розміри збитків вимірюються мільйонами доларів США і продовжують зростати щороку. Офіційна статистика [2] свідчить про те, що тільки 5 % «комп'ютерних» злочинів стають відомими правоохоронним органам, і приблизно за 20 % з них ведеться судове переслідування. Останнім часом і в Україні спостерігається стрімке зростання кількості злочинів, які пов'язані з втручанням у роботу автоматизованих систем. Як правило, втручання це здійснюється з метою вчинення інших, тяжчих злочинів: розкрадання майна, його вимагання під загрозою знищення чи спотворення інформації, яка опрацьовується чи зберігається в автоматизованих системах, ознайомлення з такою інформацією, її викрадення, знищення тощо. Це, своєю чергою, вимагає підвищення безпеки інфраструктури «е-урядування», чого можна, як правило, досягти застосуванням криптографічних методів захисту інформації. Державна політика України у сфері захисту інформації [3, 4, 5], що визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та забезпечується виконанням положень, зазначених у законодавстві, та положень концепції технічного захисту інформації, а також програм розвитку захисту інформації та окремих проектів.

Актуальність теми зумовлена стрімким розвитком електронного урядування в Україні та необхідністю адекватного захисту інформації, яка в ньому функціонує. Сьогодні відома велика кількість алгоритмів криптографічного захисту інформації, але завдання полягає в оптимальному їх виборі з урахуванням мінімізації витрат на впровадження, експлуатації та максимізації продуктивності, швидкодії та стійкості до атак.

Мета і завдання дослідження. Розглянуто питання оптимізації вибору алгоритму криптографічного захисту інформації для електронного урядування за допомогою нелінійної згортки критеріїв на основі методу аналізу ієрархій з урахуванням вимог: безпека, швидкість, характеристика алгоритму. Алгоритм повинен забезпечувати цілісність та доступність інформації під час функціонування електронного урядування, автентифікацію користувачів та неможливість заперечення факту відправлення/отримання інформації. Для досягнення мети були поставлені **такі завдання**:

- визначити вимоги до алгоритмів криптографічного захисту інформації для електронного урядування;
- з'ясувати можливості криптоалгоритмів;
- проаналізувати відповідність можливостей до вимог електронного урядування;
- визначити метод процесу оптимізації процесу вибору криптоалгоритму та його переваги/недоліки;
- обґрунтувати вибір методу підтримки прийняття рішення;
- встановити критерії порівняння;
- оптимізувати вибір алгоритму криптографічного захисту інформації для електронного урядування.

Аналіз останніх досліджень та публікацій

Криптографічні методи захисту інформації. Одним з напрямів захисту в інформаційних системах є криптографічний захист інформації, що передбачає використання математичних методів перетворення інформації за допомогою шифрування, вироблення імітовставки або цифрового підпису тощо. Криптографічний захист може здійснюватися в процесі передавання інформації каналами зв'язку та під час її опрацювання на робочих станціях і серверах.

До передавання інформації каналами зв'язку ставлять такі вимоги:

- забезпечення конфіденційності інформації;

- забезпечення цілісності інформації;
- автентичність сторін інформаційного обміну.

Конфіденційність інформації забезпечується симетричним (алгоритми ГОСТ 28147-89, DES, 3DES, AES, IDEA) та асиметричним (алгоритми RSA, El Gamal) шифруванням. Цілісність інформації та автентичність сторін досягається використанням хеш-функцій та технологій цифрового підпису. Сукупність технологій, що забезпечують конфіденційність та цілісність інформації при її передаванні незахищеними каналами зв'язку, отримала назву віртуальних приватних мереж (VPN – Virtual Private Network). У процесі мережевої взаємодії захист інформації, зокрема, забезпечується за допомогою протоколів SSL, SSH, S-HTTP, IPSec тощо. Автентичність сторін інформаційного обміну досягається за рахунок використання протоколів X.509, RADIUS, TACACS+ та інших. Реалізація цих технологій може здійснюватися програмними та програмно-апаратними засобами. Захист інформації на робочих станціях і серверах може реалізовуватися за допомогою шифрування на рівні файлової системи, криптографічних методів перевірки автентичності (цифрові сертифікати, одноразові паролі тощо), криптографічних засобів перевірки цілісності (контрольні суми).

Проблема захисту інформації через її перетворення, що унеможливлює її прочитання сторонніми особами, ще кілька десятиліть тому стосувалась головно військових операцій або була пов'язана зі шпигунськими історіями, а не становила предмет широкого використання. Причиною бурхливого розвитку криптографії, з одного боку, є використання комп'ютерних мереж, зокрема глобальної мережі Internet, по яких передають великі обсяги інформації державного, військового, комерційного та приватного змісту, що не допускає можливості доступу до неї сторонніх осіб, а з іншого – поява нових потужних обчислювальних засобів уможливила дискредитацію низки криптографічних систем. Без криптографії не було б стільникових телефонів, банкоматів, цифрового телебачення, Internet-платежів тощо.

Методи криптографічного захисту інформації передбачають як програмне, так і апаратне використання. Програмна реалізація шифрування є дешевою та практичнішою. Водночас апаратна реалізація продуктивніша та простіша у використанні. Сучасні криптографічні системи повинні задовольняти такі загальноприйняті вимоги:

- вихідний текст із зашифрованого тексту можна відтворити лише за допомогою ключа дешифрування;
- послідовне перебирання можливих ключів дешифрування з метою відтворення вихідного тексту потребує значного часу обчислень або великих затрат на реалізацію цих обчислень;
- інформація про алгоритм шифрування не повинна впливати на стійкість до зламування системи шифрування;
- незначна зміна ключа шифрування повинна призводити до істотних змін шифрограми одного і того самого тексту.

1. Шифрування з ключем. Алгоритм шифрування з ключем поділяють на дві великі групи – алгоритми симетричного шифрування й алгоритми асиметричного шифрування.

Методи симетричного шифрування/дешифрування – це метод, за яким ключі шифрування і дешифрування є або однаковими, або легко обчислюються один з одного, забезпечуючи спільний ключ, який є таємним.

Методи асиметричного шифрування/дешифрування – набір методів криптографічного шифрування/дешифрування, в якому використовують два ключі – таємний (приватний) і відкритий; жодний із ключів не може бути обчислений з іншого за визначений час. Таке шифрування/дешифрування ще називають шифруванням/дешифруванням з відкритим ключем.

До 70-х років минулого століття застосовували лише криптографію з симетричними криптоалгоритмами. Криптографія з асиметричними криптоалгоритмами значно молодша.

Симетричні та асиметричні криптоалгоритми мають переваги та недоліки. Симетричні криптоалгоритми порівняно з асиметричними мають більшу швидкодію та меншу довжину ключа. Асиметричне шифрування застосовують за такої організації криптосистем, коли використання симетричних алгоритмів є неможливим. А загалом порівнювати характеристики цих криптоалгоритмів було б некоректно: вони створені для розв'язування різних задач шифрування.

2. Метод симетричного шифрування. Симетричне шифрування ще називають шифруванням з таємним ключем, тобто з ключем, який обидві сторони обміну інформацією (таємно від інших користувачів) використовують для шифрування та дешифрування повідомлень. На рис. 1 наведено структурну схему шифрування з таємним ключем. Основне призначення симетричних криптоалгоритмів – шифрування великих масивів даних із великою швидкістю. Разом із тим, через необхідність наявності захищеного каналу передавання таємного ключа ці криптоалгоритми під час створення сучасних криптосистем виявляють дуже низьку гнучкість. Розрізняють дві великі групи алгоритмів симетричного шифрування: потокове шифрування та блокове шифрування.

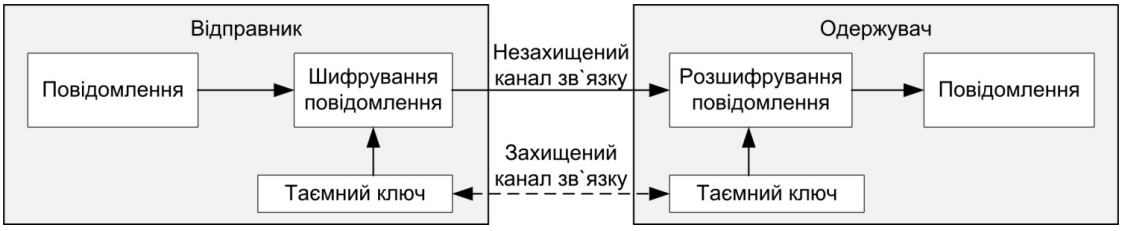


Рис. 1. Структурна схема шифрування з таємним ключем

3. Метод асиметричного шифрування. Проблему зростання обсягів шифрованої інформації у криптографії вирішують підвищенням швидкодії традиційних методів шифрування з таємним ключем. Проте застосування цих методів в умовах постійного зростання кількості учасників спільної роботи (децентралізована структура управління) й ускладнення організації взаємодії між ними, зокрема попарного обміну інформацією, виявляється неефективним. Це зумовлено тим, що зі збільшенням кількості учасників обміну інформацією квадратично зростає кількість таємних ключів. Можна показати, що для N учасників кількість таємних ключів у такій системі сягає $N(N-1)/2$. Крім того, у методах симетричної криптографії з таємним ключем ускладнене довірене узгодження таємного ключа. З метою зменшення цих недоліків було розроблено методи асиметричного шифрування з відкритим ключем. Шифрування з відкритим ключем – порівняно нова галузь криптографії. В асиметричних криптоалгоритмах для шифрування і дешифрування використовують різні ключі: для шифрування – відкриті, для дешифрування – таємні.

Асиметрична криптографія основана на ідеях В. Діффі та М. Хеллмана про шифрування з двома ключами, що стали відомими у 1976 році. Але першим алгоритмом асиметричного шифрування, що набув практичного значення, став алгоритм, який запропонували Р. Рівест, А. Шамір і Л. Адлеман у 1978 році. Він дістав назву алгоритм RSA. На рис. 2 наведено структурну схему шифрування з відкритим ключем.

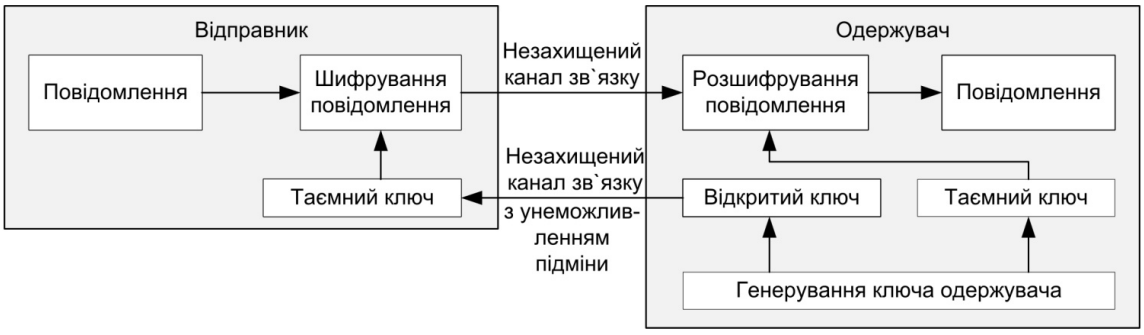


Рис. 2. Структурна схема шифрування з відкритим ключем

Математичним обґрунтуванням асиметричних криптоалгоритмів є важкооборотні (односторонні) функції. У теорії складності обчислень розглядають поняття, яке характеризує рівень складності обчислень (кількість операцій) залежно від розміру вхідних даних. Поширеними є поліноміальний та експоненційний характери залежності складності обчислень від кількості вхідних даних. В асиметричній криптографії В. Діффі та М. Хеллмана зашифроване повідомлення за наявності таємного ключа дешифровується за поліноміальний час роботи обчислювальної системи, а у разі його відсутності – за експоненційний час. Сучасна асиметрична криптографія

основана на алгоритмах Ель-Гамаля та Міллера–Коблиця. Теоретичну основу стійкості алгоритму RSA становить проблема факторизації великих цілих чисел, а алгоритмів Ель-Гамаля та Міллера–Коблиця – проблема дискретного логарифмування. Сьогодні відомі численні вразливості цих алгоритмів. Алгоритми шифрування на відкритому ключі замінили стійкіші алгоритми шифрування на еліптичних кривих, які запропонували окремо В. Міллер і Н. Коблиць у 1986 р. [6].

Виділення проблем

Алгоритми асиметричного шифрування, так само, як і симетричного, застосовують для шифрування масивів даних, але їхня швидкість значно нижча. Основне призначення асиметричних алгоритмів – забезпечення ефективного функціонування сучасних криптосистем. Саме ці алгоритми покладено в основу задач автентифікації користувачів, контролю цілісності та доступності інформації, унеможливлення відмови від авторства чи факту одержання даних тощо, зокрема, в організації електронного урядування. Найповніше ці вимоги задовольняють такі алгоритми асиметричного шифрування: Mars, RC6, Rijndael, Serpent, Twofish (табл. 1).

Таблиця 1

Вибрані для порівняння алгоритми асиметричного шифрування

Алгоритм	Розробник	Країна	Швидкодія (asm, 200M Гц)
MARS	IBM	US	8 Мбайт/с
RC6	R.Rivest & Co	US	12 Мбайт/с
Rijndael	V.Rijmen & J.Daemen	BE	7 Мбайт/с
Serpent	Universities	IS, UK, NO	2 Мбайт/с
TwoFish	B.Schneier & Co	US	11 Мбайт/с

Важливого практичного значення асиметричні криптоалгоритми набули у застосуванні систем електронно-цифрового підпису (ЕЦП). ЕЦП – цифрова послідовність, що додається до повідомлення для забезпечення цілісності інформації та підтвердження авторства і формується із застосуванням асиметричних криптосистем. У ЕЦП для формування підписаних повідомлень використовують таємний ключ, а для перевірки підпису – відкритий.

В процесі організації електронного урядування виникає проблема оптимального вибору алгоритму криптографічного захисту інформації. Кожен з великої кількості криптографічних алгоритмів має певні переваги та недоліки. Тому обсяг аналізу інформації щодо оцінення і вибору криптографічного алгоритму, який найкраще задовольняє вимоги захисту інформації в електронному урядуванні, є доволі великим. Процес вибору передбачає кількісний та якісний аналіз в процесі порівняння різних альтернатив. Із зростанням кількості критеріїв порівняння та кількості альтернатив, які можуть істотно впливати на кінцевий результат, людині зробити вибір серед такої множини варіантів (табл. 2 [7]) досить складно. Саме тому виникає необхідність використання систем підтримки прийняття рішення, що дає змогу на основі експертних оцінок оптимізувати вибір алгоритму криптографічного захисту інформації, а також не тільки виконувати якісний, кількісний аналіз, враховуючи найважливіші вимоги до алгоритмів, але і науково обґрунтувати вибір [8].

Таблиця 2

Характеристика основних асиметричних алгоритмів захисту інформації

Алгоритм шифрування	Характеристика
1	2
MARS	виконує послідовність перетворень у такій послідовності: додавання за модулем 2 з ключем як pre-whitening, 8 раундів прямого перетворення без використання ключа, 8 раундів прямого перетворення з використанням ключа, 8 раундів зворотного перетворення з використанням ключа, 8 раундів зворотного перетворення без використання ключа і віднімання ключа як post-whitening. 16 раундів з використанням ключа, який називається криптографічним ядром. Раунди без ключа використовують два 8x16-бітові S-boxes і операції складання і XOR. На додаток до цих елементів раунди з ключем використовують 32-бітове множення ключа, що залежить від даних, циклічні зрушення і додавання ключа. Як раунди перетворення, так і раунди ядра є раундами модифікованої мережі Фейштеля, в яких чверть блока даних використовується для зміни решти трьох четвертих блока даних. MARS запропонований корпорацією IBM.

Продовження табл. 2

1	2
RC6	є сім'єю алгоритмів шифрування, що параметризується, основане на мережі Фейштеля; для AES було запропоновано використовувати 20 раундів. Функція раунду в RC6 задіює змінні циклічні зрушення, які визначаються квадратичною функцією від даних. Кожен раунд також передбачає множення за модулем 32, складання, XOR і складання з ключем. Складання з ключем також використовується для pre- і pos-whitening. RC6 був запропонований лабораторією RSA.
Rijndael	є алгоритмом, що використовує лінійно-підстановлювальні перетворення і складається з 10, 12 або 14 раундів залежно від довжини ключа. Блок даних, що обробляється з використанням Rijndael, ділиться на масиви байтів, і кожна операція шифрування є байт-орієнтованою. Функція раунду Rijndael складається з чотирьох шарів. У першому шарі для кожного байта застосовується S-box розмірністю 8x8 біт. Другий і третій шари є лінійними перетвореннями, в яких рядки розглядаються як зміщені масиви і стовпці перемішуються. У четвертому шарі виконується операція XOR байтів підключа і кожного байта масиву. У останньому раунді перемішування стовпців опущене. Rijndael запропонований Joan Daemen (Proton World International) і Vincent Rijmen (Katholieke Universiteit Leuven).
Serpent	є алгоритмом, що використовує лінійно-підстановлювальні перетворення і складається з 32 раундів. Serpent також визначає некриптографічні початкову і завершальну перестановки, які полегшують альтернативний режим реалізації, так званий bitslice. Функція раунду складається з трьох шарів: операція XOR з ключем, 32 паралельних застосувань одного з восьми фіксованих S-boxes і лінійне перетворення. В останньому раунді шар XOR з ключем замінений на лінійне перетворення. Serpent запропонований Ross Anderson (University of Cambridge), Eli Biham (Technion) і LarsKnudsen (University of California San Diego).
Twofish	є мережею Фейштеля з 16 раундами. Мережа Фейштеля модифікована з використанням однобітних ротацій. Функція раунду впливає на 32-бітові слова, використовуючи чотири залежних від ключа S-boxes, за якими слідують фіксовані максимально видалені окремі матриці в GF(28), перетворення псевдо-Адамара і додавання ключа. Twofish був запропонований Bruce Schneier, John Kelsey і Niels Ferguson (Counterpane Internet Security, Inc.), Doug Whiting (Hi/fn, Inc.), David Wagner (University of California Berkley) і Chris Hall (Princeton University).

Формулювання мети

Методика і критерії порівняння. Для електронного урядування визначальними є такі критерії порівняння: надійне виконання алгоритму як в апаратному, так і програмному виконанні; швидке генерування та узгодження ключів, їх використання; мінімальне використання оперативної пам'яті; стійкість до атак; гнучкість; висока пропускна здатність. Отже, визначимо основні критерії порівняння алгоритмів криптографічного захисту інформації для електронного урядування: безпека; швидкість; загальні параметри алгоритму.

Критерій «безпека» є найважливішим чинником під час оцінювання і порівняння таких можливостей, як стійкість алгоритму до криптоаналізу, дослідження його математичної основи, випадковість вихідних значень алгоритму і відносна безпека порівняно з іншими алгоритмами.

Критерій «швидкість» є наступним важливим критерієм оцінювання, який характеризує обчислювальну ефективність на різних платформах, вимоги пам'яті, час, затрачений на шифрування та дешифрування, швидкість реагування на атаки.

Загальні параметри алгоритму. Третім пріоритетним критерієм оцінки алгоритмів для електронного урядування є характеристика алгоритму, під якою розуміють: гнучкість, технічні засоби, придатність програмного забезпечення і простоту алгоритму. Гнучкість означає здатність алгоритму до:

- управління ключем, зведення розмірів до мінімуму;
- безпечного й ефективного функціонування в різних типах програмного середовища;
- здійснення хешування алгоритму, можливість забезпечення додаткових криптографічних послуг.

Виконання цих вимог необхідне для того, щоб в електронному урядуванні технічні засоби і програмне забезпечення підтримували реалізацію вибраного криптоалгоритму. В табл. 3 наведено порівняльну характеристику п'яти криптоалгоритмів за визначеними критеріями порівняння [9].

Таблиця 3

Порівняльна характеристика п'яти криптоалгоритмів

№ з/п	Категорія	Serpent	Twofish	MARS	RC6	Rijndael
1	Криптостійкість	+	+	+	+	+
2	Запас криптостійкості	+ +	+ +	+ +	+	+
3	Швидкість шифрування при програмній реалізації	-	+ -	+ -	+	+
4	Захист від атак під час виконання і використання потужності	+	+ -	-	-	+
5	Захист від атак за необхідної потужності на процедуру розширення ключа	+ -	+ -	+ -	+ -	-
6	Захист від атак за використовуваної потужності для реалізації у смарт-картах	+ -	+	-	+ -	+
7	Можливість паралельних обчислень	+ -	+ -	+ -	+ -	+
8	Можливість розширення ключа «на льоту»	+	+	+ -	+ -	+ -

Криптостійкість алгоритмів є достатньою — під час досліджень не було виявлено жодних атак, що реально реалізовувалися, на повноцінних версіях алгоритмів. У цьому випадку криптоаналітики, зазвичай, досліджують варіанти алгоритмів з усіченою кількістю раундів, або з деякими внесеними змінами, незначними, але які послаблюють характеристики алгоритму. Під запасом криптостійкості розуміють співвідношення повної (передбаченої в специфікаціях алгоритмів) кількості раундів і максимального з тих варіантів, проти яких діють будь-які криптоаналітичні атаки. Наприклад, за допомогою диференціально-лінійного криптоаналізу розкривається 11-раундовий Serpent, тоді як в оригінальному алгоритмі виконуються 32 раунди. Запас криптостійкості у Rijndael і RC6 дещо нижчий, ніж у решти алгоритмів.

З характеристики алгоритмів видно, що всі вони підтримують розширення ключа «на льоту» (тобто підключі можуть генеруватися безпосередньо в процесі шифрування – за необхідністю), проте тільки Serpent і Twofish підтримують таку можливість без будь-яких обмежень.

Під наявністю варіантів реалізації (гнучкість) мається на увазі можливість по-різному реалізовувати будь-які операції алгоритму з оптимізацією під конкретні цілі. Найпоказовішими в цьому сенсі є згадані раніше варіанти процедури розширення ключа алгоритму Twofish, що дають змогу оптимізувати реалізацію алгоритму залежно, передусім, від частоти зміни ключа.

Аналіз отриманих наукових результатів

Математична модель процесу оптимізації вибору алгоритму криптографічного захисту інформації для електронного урядування. Один із підходів призначення «мір вагомості» кінцевому набору n порівнюваних об'єктів на основі матриці парних порівнянь був запропонований Т. Сааті [10]. Надалі цей підхід оформився в цілий розділ прийняття рішень за наявності одного, а також декількох критеріїв [11] – [14] та отримав назву методу аналізу ієрархій (The analytic Hierarchy Process, AHP), скорочено MAI. Нині MAI увійшов в теорію та практику багатокритеріального вибору. Кількість статей прикладного характеру, в яких MAI застосовується для розв'язання найрізноманітніших прикладних багатокритеріальних задач, перевищила тисячу вже десять років тому. На основі MAI був розроблений та набув поширення всесвітньо визнаний пакет програм EXPERT CHOICE, MPRIORITY та СППР «ВЫБОР». Відповідно до MAI експертами формується так звана матриця парних порівнянь A, а шуканий вектор міри $w = \left(w_1, w_2, ..., w_n \right)^T$ обчислюється як власний вектор цієї матриці, що відповідає максимальному власному значенню. Такий спосіб визначення вектору міри через порушення на практиці властивості сумісності (consistency) [15–18] матриці парних порівнянь не є обґрунтованим.

Пояснимо сказане. Добре відомо, що вектор міри w є власним вектором сумісності (в деяких джерелах використовується назва повністю сумісної) матриці A, що відповідає її максимальному власному значенню n. Тим самим, у разі сумісної матриці вектор міри є вказаним власним вектором. Але при формуванні відповідно до МАІ експертами матриці парних порівнянь розраховувати на її сумісність не варто. Про це відомо усім, хто знайомий з МАІ. Це означає, що на практиці доводиться мати справу з іншою ситуацією (моделлю), якій відповідає несумісна матриця. Однак відповідно до МАІ вектор міри знову пропонується знаходити як власний вектор (несумісної) матриці парних порівнянь, причому цей власний вектор відповідає власному значенню, яке вже не дорівнює (а строго більше) n. В загальній літературі по МАІ не існує (принаймні у наш час) доказу того, що шуканий вектор міри повинен бути власним вектором несумісної матриці, що відповідає її максимальному власному значенню, більшому за n. З цієї причини розглянутий метод неможливо назвати обґрунтованим, він являє собою визначений евристичний підхід, логіка якого полягає в рекомендації діяти точно так в ситуаціях, які можуть сильно відрізнятися від тих, для яких встановлена справедливість цих дій. Це означає, що застосування МАІ практично завжди містить деяку «модельну» помилку розрахунку вектора міри (не враховуючи похибок суто обчислювального характеру) і, якщо ця помилка велика, то застосування МАІ стає просто невиправданим. Тому вводиться спеціальний числовий показник «***індекс сумісності***» (consistency index), що характеризує ступінь довіри до отриманих за допомогою МАІ результатам. Цей індекс трактується як своєрідна міра відхилення вихідної несумісної матриці від деякої сумісної. Як вказує Т. Сааті [15], за достатньо малого значення індексу сумісності матриця парних порівнянь «близька» до деякої матриці з нульовим значенням цього індексу (тобто до деякої сумісної матриці). Тим самим, і результат застосування МАІ у вигляді вектора міри є до деякої міри «близьким» до результату, отриманого на основі цієї сумісної матриці. Якщо ж індекс сумісності перевищує «порогове» значення, то зробити висновок про близькість вказаних матриць неможливо, тому і застосовувати МАІ в таких випадках не рекомендується. Проте необхідно відзначити, що за значенням індексу сумісності можна лише опосередковано робити висновки про величину результативної «модельної» помилки; точно вона ніколи та ніким не може бути визначена. Така специфіка цього евристичного підходу.

МАІ неодноразово критикували різні автори, переважно за невиконання властивості зберігання ранжування рішень при видаленні одного із можливих рішень [18]. У цьому випадку пропонується переглянути інші дві важливі складові методу.

По-перше, процедуру формування матриці парних порівнянь пропонується істотно спростити, вимагаючи від експерта відомостей не про всі елементи цієї матриці, що розташовані вище (або нижче) від головної діагоналі, а лише про визначені «базисні» елементи, на основі яких потім легко та без помилок обчислювального характеру знаходять шуканий вектор міри. Вибір конкретного «базисного» набору відповідає тій або іншій схемі порівняння об’єктів, яку можна вибирати з метою отримання найнадійніших результатів від експерта. В загальному запропонований варіант виявляється значно простішим, ніж початковий метод як на стадії формування матриці A, так і в процесі обчислення вектора міри. Крім того, він повністю позбавлений «модельної» помилки, про яку було сказано вище, оскільки оснований на сумісній матриці A.

По-друге, відповідно до принципу Едворта–Парето під час розв’язання багатокритеріальних задач застосування лінійної згортки критеріїв можливе лише за певних достатньо обмежених припущень. У зв’язку з цим, замість лінійної пропонується використовувати згортку у вигляді функції мінімуму, що міститься в теоремі Ю. Б. Гермейєра [19, 20], застосування якої є обґрунтованим для найширшого класу багатокритеріальних задач вибору зі скінченною множиною можливих рішень. Отриманий в результаті перегляду метод розв’язання багатокритеріальних задач названий спрощеним варіантом МАІ на основі нелінійної згортки критеріїв.

Обґрунтування вибору MAI. Завдання прийняття рішення має два основні різновиди:

- завдання вибору (вибрати або відкинути декілька варіантів з групи можливих);
- завдання розподілу ресурсів (кожен з цих варіантів враховується відповідно до його пріоритету).

Зазначимо, що у реального процесу прийняття рішення існують супутні проблеми, які успішно вирішуються за допомогою методу аналізу ієрархій.

Можливості методу аналізу ієрархій. Метод аналізу ієрархій – методологічна основа для розв'язання завдань вибору альтернатив за допомогою їх багатокритеріального ранжування.

Основне застосування методу – підтримка ухвалення рішень за допомогою ієрархічної композиції завдання і ранжування альтернативних рішень. Маючи на увазі цю обставину, необхідно перерахувати можливості методу.

1. *Метод дає змогу проаналізувати проблему.* Проблема прийняття рішення подається у вигляді ієрархічно впорядкованих:
    - головній меті (головного критерію) ранжування можливих рішень;
    - декількох груп (рівнів) однотипних чинників, що так або інакше впливають на рейтинг;
    - групи можливих рішень;
    - системи зв'язків, що вказують на взаємний вплив чинників та рішень.

Передбачається, що для всіх перерахованих «вузлів» вказують їхні взаємні впливи один на одного (зв'язки один з одним).

2. *Метод дає змогу збирати дані з проблеми.* Відповідно до результатів ієрархічної декомпозиції модель ситуації ухвалення рішення має кластерну структуру. Набір можливих рішень і всі чинники, що впливають на пріоритети рішень, ділять на порівняно невеликі групи – кластери. Розроблена в методі аналізу ієрархій процедура парних порівнянь дає змогу визначити пріоритети об'єктів, що входять в кожен кластер. Для цього використовується метод власного вектора. Отже, складна проблема збору даних ділиться на декілька простіших, які вирішуються для кластерів.
3. *Метод дає змогу оцінити суперечність даних та мінімізувати їх.* З цією метою в методі аналізу ієрархій розроблено процедури узгодження. Зокрема, є можливість визначати найсуперечливіші дані, що дає змогу виявити найменш з'ясовані ділянки проблеми і організувати ретельніше вибіркове обдумування проблеми.
4. *Метод уможливлює синтез проблеми ухвалення рішення.* Після того як виконано аналіз проблеми і зібрані дані за всіма кластерами, за спеціальним алгоритмом розраховують підсумковий рейтинг – набір пріоритетів альтернативних рішень. Властивості цього рейтингу дають змогу здійснювати підтримку прийняття рішень. Наприклад, ухвалюється рішення з найбільшим пріоритетом. Крім того, метод дає змогу побудувати рейтинги для груп чинників, що допомагає оцінювати важливість кожного чинника.
5. *Метод дає змогу організувати обговорення проблеми, сприяє досягненню консенсусу.* Думки, що виникають при обговоренні проблеми прийняття рішення, самі можуть в цій ситуації розглядатися як можливі рішення. Тому метод аналізу ієрархії можна застосувати для визначення важливості урахування думки кожного учасника обговорення.
6. *Метод дає змогу оцінити важливість обліку кожного рішення і важливість обліку кожного чинника, що впливає на пріоритети рішень.* Відповідно до формулювання завдання ухвалення рішення величина пріоритету безпосередньо пов'язана з оптимальністю рішення. Тому рішення з низькими пріоритетами відкидаються як невпливові. Як зазначено вище, метод дає змогу оцінювати пріоритети чинників. Тому, якщо при вилученні деякого чинника пріоритети рішень змінюються, такий чинник можна вважати невпливовим для цього завдання.
7. *Метод дає змогу оцінити стійкість прийнятого рішення.* Рішення, яке приймається, можна вважати обґрунтованим лише за умови, що неточність даних або неточність структури моделі ситуації прийняття рішення істотно не впливають на рейтинг альтернативних рішень.

Ефективність застосування методу. Якщо для прийняття рішень досить використовувати тільки об’єктивні дані, то в сенсі точності та швидкості отримання результату переважати можуть інші методи (наприклад, методи оптимізації цільового критерію).

Метод може бути занадто громіздким для прийняття рішення в простих ситуаціях, через те що для збору даних необхідно багато парних порівнянь. Проте, якщо розглядається масштабна проблема і ціна наслідку неправильного рішення висока, необхідним є адекватний інструментарій. Метод аналізу ієрархій дає змогу поділити складну проблему на ряд простих, виявити суперечності.

У завданнях прийняття стратегічних рішень часто доводиться спиратися швидше на досвід і інтуїцію фахівців, ніж на наявні об’єктивні дані. В цьому випадку результати, які отримані методом аналізу ієрархій, можуть бути реалістичнішими, ніж результати, одержані іншими методами.

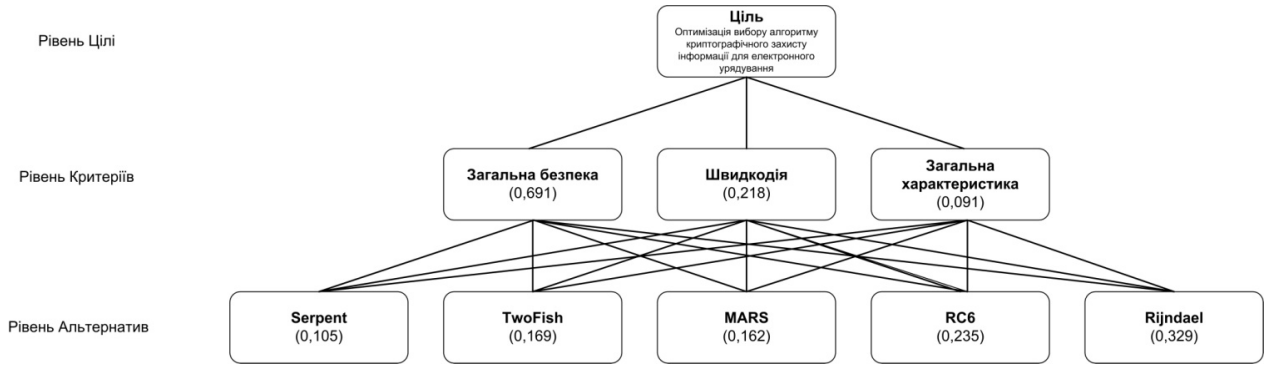
Рейтинги можливих рішень отримують на основі «прозорих» принципів. Тому вони можуть бути переконливішими, ніж інформація для підтримки прийняття рішення, одержана за допомогою моделей типу «чорної скриньки». У таких моделях вхідна інформація про проблему перетвориться на вихідну інформацію про прийняття рішення за «непрозорими» принципами і структура ситуації прийняття рішення не розкривається. Метод аналізу ієрархій не вимагає спрощення структури завдання, що є апріорним відкиданню деяких ознак. Тому він ефективніше за інші аналітичні інструменти дає змогу враховувати вплив всіляких чинників на вибір рішення.

Складання структури моделі прийняття рішення може бути громіздким процесом. Проте, якщо вона складена, то може потім багаторазово використовуватися. Залишається лише коректувати цю структуру і наповнювати її даними. При цьому вирішення типових завдань може бути поставлене на потік. Отже, застосування методу стає ефективнішим. А тепер розглянемо конкретний приклад оптимізації вибору алгоритму криптографічного захисту інформації для електронного урядування спрощеним методом аналізу ієрархій на основі нелінійної згортки критеріїв [14].

Програмні засоби процесу вибору номенклатури елементів захисту. Як було зазначено вище, для оптимізації процесу вибору алгоритму криптографічного захисту інформації для електронного урядування використовуватимемо програмну систему СППР «ВЫБОР».

Оптимізація вибору алгоритму криптографічного захисту інформації для електронного урядування методом аналізу ієрархій на основі нелінійної згортки критеріїв.

Результати обчислення наведені на рис. 3, 4, у табл. 4.



Загальна узгодженість ієрархії = 0.018

Рис. 3. Ієрархія: алгоритми криптографічного захисту інформації для електронного урядування

Таблиця 4

Результати обчислень

Фактори (Міра)		**Serpent (0.105)**	**TwoFish (0.169)**	**MARS (0.162)**	**RC6 (0.235)**	**Rijndael (0.329)**
1	2	3	4	5	6	7
Вузол		**Загальна безпека**				
Міра		0.691				
Матриця попарних порівнянь	№	1	2	3	4	5
	1	1,000	0,500	0,500	0,500	0,333
	2	2,000	1,000	1,000	1,000	0,500
	3	2,000	1,000	1,000	1,000	0,500
	4	2,000	1,000	1,000	1,000	0,500
	5	3,000	2,000	2,000	2,000	1,000
Характеристика матриці		λ_{max} = 5.007 ІЗ = 0.002 ВУ = 0.002				
Вузол		**Швидкодія**				
Міра		0.218				
Матриця попарних порівнянь	№	1	2	3	4	5
	1	1,000	0,500	0,500	0,250	0,333
	2	2,000	1,000	1,000	0,333	0,500
	3	2,000	1,000	1,000	0,333	0,500
	4	4,000	3,000	3,000	1,000	2,000
	5	3,000	2,000	2,000	0,500	1,000
Характеристика матриці		λ_{max} = 5.032 ІЗ = 0.008 ВУ = 0.007				
Вузол		**Загальна характеристика**				
Міра		0.091				
Матриця попарних порівнянь	№	1	2	3	4	5
	1	1,000	2,000	4,000	1,000	0,500
	2	0,500	1,000	3,000	0,500	0,333
	3	0,250	0,333	1,000	0,250	0,200
	4	1,000	2,000	4,000	1,000	0,500
	5	2,000	3,000	5,000	2,000	1,000
Характеристика матриці		λ_{max} = 5.052 ІЗ = 0.013 ВУ = 0.012				

ІЗ – індекс узгодженості, ВУ – відношення узгодженості;
якщо ІЗ та ВУ ≤ 0.1, тоді міра узгодженості на задовільному рівні.

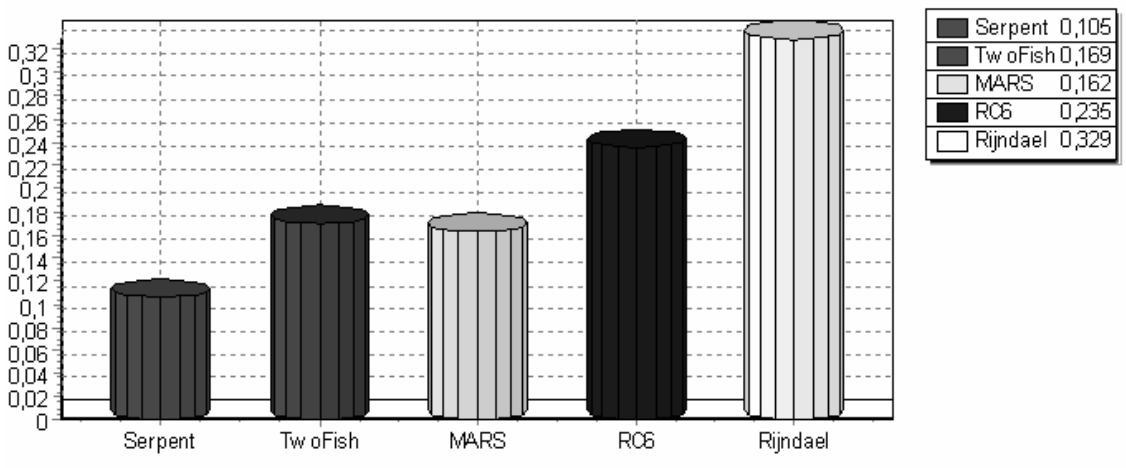


Рис. 4. Діаграма результату

Висновки і перспективи подальших наукових розвідок

Відповідно до критеріїв оцінки алгоритмів криптографічного захисту інформації для застосування в електронному урядуванні рекомендується вибирати алгоритм, який за інтегральним показником є найефективнішим.

Критерій «безпека» має найбільший пріоритет і здійснює найбільший вплив на отримані результати, а критерії «швидкість» і «характеристика алгоритму» є вторинними щодо «безпеки». Керуючись необхідністю забезпечення надійної безпеки алгоритмів від атак, можна сказати, що щодо безпеки MARS, Serpent і Twofish мають високий рівень захисту, але RC6 і Rijndael мають вищий і надійніший захист. RC6 і Rijndael загалом демонструють швидкість шифрування і дешифрування, вищу за середню для 128-бітних ключів, але щодо 32-бітних платформ RC6 має найбільшу швидкість. MARS має середню швидкість виконання цих дій. Для Twofish час, затрачений на шифрування і дешифрування, відрізняється, але в обох випадках рівень є вищим за середній. Serpent показав найнижчий показник порівняно з іншими алгоритмами.

Rijndael потребує невеликих затрат оперативної пам'яті і відповідно є найкращим за обмежених можливостей. Serpent також забезпечує належний рівень шифрування та дешифрування за малої оперативної пам'яті. RC6 має невелику оперативну пам'ять, що є позитивним в обмеженому просторі, але має недолік при безперервній здатності обчислення підключів для дешифрування, – високу вимогу до оперативної пам'яті щодо інших алгоритмів. MARS не задовольняє вимоги за обмеженого середовища та вимагає додаткових ресурсів.

Serpent і Rijndael мають найкращу апаратну продуктивність для обох способів зворотного і незворотного зв'язку. Serpent має найвищу продуктивність в незворотному зв'язку, Rijndael пропонує найкращу ефективність роботи у зворотному зв'язку. RC6 і Twofish мають середню продуктивність, і обидва алгоритми можуть виконуватись компактно. MARS має високі вимоги і загалом його продуктивність є нижча від середнього рівня. Під час атак на виконання добре себе проявили алгоритми Rijndael і Serpent, швидко виявляючи і запобігаючи їм. Довше і з більшою складністю виконує Twofish, а RC6 і MARS з найбільшою затратою часу і труднощам протидіють атакам. Twofish, MARS і RC6 потребують мало додаткового простору, щоб здійснювати шифрування та дешифрування. Хоч Rijndael у цьому аспекті поступається за швидкістю, але може розділяти деякі технічні засоби.

Twofish підтримує безперервне обчислення, підрахунок підключів як для шифрування, так і для дешифрування. Serpent також підтримує безперервний підрахунок підключів як для шифрування, так і для дешифрування; проте процес дешифрування вимагає одного додаткового обчислення підрахунку. Алгоритм Rijndael підтримує безперервне обчислення підключів для шифрування, але вимагає попереднього одноразового виконання повного ключового списку до ранішого дешифрування зі специфічним ключем. MARS має особливі характеристики, які є схожими до Rijndael, але додатково навантажує ресурс на MARS виконання. RC6 підтримує безперервне обчислення підключів тільки для шифрування. Кожен з алгоритмів забезпечує надійну захищеність і має певні переваги у деяких галузях порівняно з іншими. Методом аналізу ієрархій на основі нелінійної згортки критеріїв було досліджено і математично обгрунтовано вибір алгоритму Rijndael, як такий, що найкраще задовольняє вимоги захисту інформації в електронному урядуванні.

1. Про електронне урядування [Електронний ресурс]. – Режим доступу: http://e-gov.org.ua/node/13. 2. Душейко Г.О. Деякі питання розкриття та розслідування злочинів у сфері комп'ютерної інформації [Електронний ресурс] / Г.О. Душейко, М.О. Сергатий Режим доступу: http://www.bezpeka.com/ru/lib/spec/art66.html. 3. Закон України. Про захист інформації в автоматизованих системах (Відомості Верховної Ради (ВВР), 1994, № 31. – С. 286) (Вводиться в дію постановою ВР №81/94-ВР від 05.07.94, ВВР, 1994, № 31. – С. 287). 4. Закон України. Про державну таємницю.

№ 1079-XIV 21 вересня 1999 року. 5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення [Текст]. – К.: Держстандарт України, 1996. – 20 с. 6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с. 7. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (second Edition) [Text] / B. Schneier. – N.Y.: John Wiley & Sons, Inc., 1996. – 758 p. 8. Ногин В.Д. Принятие решении в многокритериальной среде: количественный подход [Текст] / В.Д. Ногин. – М. : Физматлит, 2002. 9. Алгоритмы симметричного шифрования. Ч. 3. Разработка Advanced Encryption Standart (AES) [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/department/security/networksec/4/5.html. 10. Saaty T. L. An eingenvalue allocation model for prioritization and planning [Text] / T. L. Saaty // Energy Management and Policy Center. – University of Pennsylvania, 1972. 11. Саати Т. Аналитическое планирование. Организация систем [Текст] / Т. Саати. – М.: Радио и связь, 1991. 12. Саати Т. Принятие решений. Метод анализа иерархий [Текст] / Т. Саати. – М.: Радио и связь, 1989. 13. Saaty T. L. Multicriteria Decision Making. The Analytic Hierarchy Process: Planning. Priority Setting. Resource Allocation [Text] / T.L. Saaty. – University of Pittsburgh, RWS Publications, 1990. 14. Yu P.L. Multiple Criteria Decision Making: Concepts, Techniques, and Extensions [Text] / P.L. Yu. – Plenum Press, N.Y., 1985. 15. Андрейчиков А.В. Анализ, синтез, планирование решений в экономике [Текст] / А.В. Андрейчиков, О.Н. Андрейчикова. – М.: Финансы и статистика, 2001. 16. Ларичев О.И. Теория и методы принятия решений [Текст] / О.И. Ларичев. – М.: Логос, 2000. 17. Ногин В.Д. Применение линейной алгебры в принятии решений [Текст] / В.Д. Ногин, С.В. Чистяков. – СПб.: СПбГТУ, 1998. 18. Подиновский В.В. Парето-оптимальные решения многокритериальных задач [Текст] / В.В. Подиновский, В.Д. Ногин. – М.: Наука, 1982. 19. Гермейер Ю.Б. Введение в исследование операций [Текст] / Ю.Б. Гермейер. – М.: Наука, 1971. 20. Карманов В.Г. Моделирование в исследовании операций [Текст] / В.Г. Карманов, В.В. Федоров. – М.: Тема, 1996.