УКД 621.396.13

Гаврилюк О.Г. (ВІТІ)
Бондаренко Т.В. (ВІТІ)

МЕТОДИКА ПОРІВНЯЛЬНОГО АНАЛІЗУ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЩО ПЛАНУЮТЬСЯ НА ПРИЙНЯТТЯ ДЛЯ ПОСТАЧАННЯ В ЗБРОЙНІ СИЛИ УКРАЇНИ

В роботі запропонована методика порівняльного аналізу засобів криптографічного захисту на основі методу аналізу ієрархій Т. Сааті. Даний метод аналізу ієрархій є систематичною процедурою для ієрархічного уявлення елементів, що визначають суть проблеми. Метод полягає в декомпозиції проблеми на все більш прості складові частини і подальшій обробці послідовності суджень особи, яка приймає рішення, по парним порівнянь. В результаті може бути виражена відносна ступінь (інтенсивність) взаємодії елементів в ієрархії. Ці судження потім виражаються чисельно. Метод включає в себе процедури синтезу множинних суджень, отримання пріоритетності критеріїв і знаходження альтернативних рішень.

Гаврилюк О.Г., Бондаренко Т.В. Методика сравнительного анализа средств криптографической защиты планируемого на принятие для поставки в Вооруженные силы Украины. *В работе предложена методика сравнительного анализа средств криптографической защиты на основе метода анализа иерархий Т. Саати. Данный метод анализа иерархий является систематической процедурой для иерархического представления элементов, определяющих суть проблемы. Метод заключается в декомпозиции проблемы на все более простые составляющие части и дальнейшей обработке последовательности суждений лица, принимающего решение, по парным сравнениям. В результате может быть выражена относительная степень (интенсивность) взаимодействия элементов в иерархии. Эти суждения затем выражаются численно. Метод включает в себя процедуры синтеза множественных суждений, получения приоритетности критериев и нахождения альтернативных решений.*

O. Gavryliuk, T. Bondarenko Method of comparative analysis of cryptographic protection means planned for acceptance for delivery to the Armed Forces of Ukraine. *In the work the method of comparative analysis of cryptographic protection means is proposed based on the method of analysis of the hierarchy of T. Saati. This method of hierarchy analysis is a systematic procedure for hierarchical representation of elements that determine the essence of the problem. The method consists in decomposing the problem into more simple parts and further processing the sequence of judgments of the decision maker on the basis of paired comparisons. As a result, the relative degree (intensity) of the interaction of elements in the hierarchy can be expressed. These judgments are then expressed numerically. The method includes procedures for synthesizing multiple judgments, obtaining priority criteria and finding alternate solutions.*

Ключові слова: *захист інформації, криптографія, криптографічний захист інформації, метод аналізу ієрархій***.**

Постановка проблеми в загальному вигляді. Аналіз виконання бойових завдань підрозділами та військовими частинами ЗС України показав, що забезпечення скритого управління військами (силами) в ході проведення Антитерористичних операцій повинно організовуватися з використанням засобів криптографічного захисту інформації. Планується використовувати шифрувальну та кодувальну техніку до окремого батальйону включно (у підрозділах, в яких такі засоби не передбачені, розробляються документи кодованого зв'язку). Таким чином, забезпечення захисту інформаційних ресурсів набуває все більш важливого значення. Прискорення темпів науково-технічного прогресу, результатом якого є нові технічні та електронні засоби, призвело до виникнення нових та сучасних засобів криптографічного захисту інформації.

Разом з тим, відсутність типових, застарілі зразки шифрувальної та кодувальної техніки, її знос, не дає можливість організувати зв'язок взаємодії з іншими військовими формуваннями. Різні типи криптографічного захисту приводять до комплексної надмірності та фінансових затрат.

Таким чином, задача вибору нових засобів криптографічного захисту інформації є актуальна, що підтверджує актуальність обраної тематики досліджень.

Аналіз останніх публікацій дозволяє зробити висновок, що питанням вибору засобів криптографічного захисту інформації не приділяється достатньо уваги. В той же час, відомі роботи мають певні недоліки та обмеження. Наприклад, у роботах [1, 2] акцент робиться на застосування обладнання для вузьких (конкретних) питань, наприклад використання у

системах електронного документообігу. Такий підхід значно звужує спектр можливих рішень. У роботі [3] при вирішенні завдання вибору виявляються протиріччя між „технічним" та „споживчим" поглядами на вибір обладнання через наявність у різних засобів криптографічного захисту унікальних функціональних можливостей.

Таким чином, на сьогоднішній день відсутня методика порівняльного аналізу засобів криптографічного захисту, що не дає змогу об'єктивно та упереджено здійснювати вибір виробника засобів криптографічного захисту для потреб Збройних сил України. Виходячи з цього **метою статті є** розробка методики порівняльного аналізу виробів криптографічного захисту.

Виклад основного матеріалу дослідження. Методика порівняльного аналізу полягає в одержанні зваженого показника на основі бальних оцінок низки експлуатаційно-технічних критеріїв та їх вагових коефіцієнтів, обчислених шляхом їх попарного порівняння.

Особливістю обраного методу є те, що в процесі порівняльного аналізу відбувається взаємне обговорення деякої проблеми групою людей (експертів), при цьому кожен експерт може висловлювати та модифікувати свої думки, в результаті чого обирається компромісний груповий висновок щодо певного критерію, який характеризує обговорювану проблему. В результаті описаної вище взаємодії експертів в рамках експертної групи забезпечується об'єднання думок експертів раціональним чином і як результат винесення узагальненої оцінки того чи іншого критерію відносно конкретного об'єкта порівняння.

Для досягнення мети порівняльного аналізу використовується метод експертних оцінок та проводиться ретельний аналіз перевірених технічних характеристик засобів криптографічного захисту різних виробників[4 – 7].

Вихідними даними для проведення розрахунків виступають:

перелік засобів криптографічного захисту, що підлягають оцінці;

перелік основних технічних характеристик засобів криптографічного захисту, за якими проводиться аналіз, та їх значення, отримані за результатами практичних (дослідних) випробувань;

бальні оцінки засобів криптографічного захисту, що отримані за даними експертів.

В основі методики покладено ряд **обмежень**, а саме – серед технічних характеристик засобів криптографічного захисту в якості основних застосовуються наступні:

1. Практична стійкість шифру.
2. Пропускна спроможність каналу зв'язку, що шифрується.
3. Мінімально допустима ймовірність помилки у символі в каналі зв'язку.
4. Час напрацювання на відмову.
5. Стійкість обладнання до впливу зовнішніх факторів (захищеність).
6. Відповідність алгоритму криптографічного захисту державному стандарту України (ГОСТ 28147-89).

Бальні оцінки засобів криптографічного захисту виставляються експертами за результатами практичної перевірки основних технічних характеристик;

економічний фактор (вартість обладнання) не враховується при застосуванні методики.

Особливістю методики проведення порівняльного аналізу засобів криптографічного захисту, у порівнянні з відомим методом аналізу ієрархій, є використання конкретного переліку основних технічних характеристик, які використовуються для порівняння.

Кроки методики

Методика порівняльного аналізу засобів криптографічного захисту призначена для вибору засобу криптографічного захисту за результатами порівняльних досліджень та полягає у ряд кроків.

На І кроці здійснюються заміри характеристик засобів криптографічного захисту за результатами їх випробувань. Порівняльний аналіз засобів криптографічного захисту здійснюється після перевірки всіх основних технічних характеристик засобів криптографічного захисту (див. обмеження).

Для проведення порівняльного аналізу засобів криптографічного захисту визначаються з критеріями, відносно яких будуть порівнювати засоби криптографічного захисту. Критерії порівняння доцільно обирати, виходячи з основних функціональних відмінностей технологій та їх особливостей з точки зору експлуатаційно-технічних параметрів; сервісних параметрів та інших параметрів, що перевіряються. (вибір критеріїв порівняння не входить у об'єм досліджень даної статті та потребує додаткових вишукувань).

На ІІ кроці експерти заповнюють таблицю Попарного порівняння критеріїв експертної оцінки.

В процесі порівняльного аналізу характеристик (параметрів) засобів криптографічного захисту обирається компромісний висновок щодо показників та критеріїв оцінки. В результаті описаної вище взаємодії забезпечується об'єднання думок експертів раціональним чином і як результат винесення узагальненої оцінки того чи іншого показника (критерію) відносно конкретного об'єкта порівняння – засобу криптографічного захисту.

Для одержання єдиної комплексної порівняльної оцінки засобів криптографічного захисту застосовують лінійну згортку виду:

$$Q = \sum_{i=1}^{n} K_i B_i \,, \tag{1}$$

де K_i – ваговий коефіцієнт *i*-го показника, B_i – бальна оцінка *i*-го показника.

В якості показників використовуються технічні характеристики та параметри засобів криптографічного захисту.

Вагові коефіцієнти для прийнятих показників обчислюються шляхом їх попарного порівняння. Для цього формується порівняльна матриця *A* розміром $n \times m$ елементів a_{ij}, де кожний елемент матриці є результатом зваженого експертного порівняння *i*-го та *j*-го показника. При цьому, якщо *i*-й показник вважається експертами вагомішим за *j*-й, то елемент a_{ij} має дорівнювати 2 (в свою чергу елемент a_{ji} має дорівнювати 0), а у випадку, коли *i*-й показник вважається менш вагомим ніж *j*-й, елемент a_{ij} має дорівнювати 0 (a_{ji} має дорівнювати 2). Якщо ж *i*-й та *j*-й показники вважаються рівнозначними, то елементи a_{ij} та a_{ji} повинні дорівнювати 1. Елементи головної діагоналі матриці дорівнюють 1. Приклад заповнення таблиці попарного порівняння наведено в таблиці 1.

Таблиця 1

Попарне порівняння критеріїв експертної оцінки

	1	**2**	**3**	**4**	**5**	**6**
1	1	0	2	0	2	0
2	2	1	2	2	2	0
3	0	0	1	0	0	0
4	2	0	2	1	2	0
5	0	0	2	0	1	0
6	2	2	2	2	2	1

На ІІІ кроці визначаються вагові коефіцієнти.

За результатами порівняння показників одержимо матрицю попарних порівнянь, значення елементів a_{ij} якої відображають суб'єктивний висновок стосовно важливості *i*-го показника порівняно з *j*-м у конкретних умовах експертизи.

Для визначення вагових коефіцієнтів K_i *i*-го показнику необхідно знайти суму елементів матриці кожного рядка:

$$s_i = \sum_{j=1}^{m} a_{ij}, \quad i = 1 \ldots m,$$

де *m* – кількість критеріїв.

На наступному кроці необхідно обчислити загальну суму елементів матриці *A*:

$$S_k = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} = \sum_{i=1}^{m} s_i .$$

Далі нормоване значення вагового коефіцієнта K_i *i*-го показника обчислюється за формулою:

$$K_i = \frac{s_i}{S_k}, \quad i = 1 \ldots m. \qquad (2)$$

Результати обчислення вагових коефіцієнтів за формулою (2) на основі матриці попарного порівняння та результати бального оцінювання критеріїв на основі експертних висновків для всіх об'єктів порівняння, а також пояснення щодо кожного критерію приводяться в таблиці 2. Кількість балів (мінімум 1 бал, максимум 5 балів), присвоєних кожному показнику для кожного засобу криптографічного захисту, вказаних в табл. 2, формується, спираючись на досвід фахівців (експертів) та перевірені характеристики (можливості), що перевірені на практиці та характеризують засоби криптографічного захисту порівняння. Аналіз даних, а також виконання розрахункових операцій згідно з виразом (1), дозволяють зробити висновок щодо порівняння кількох засобів криптографічного захисту і вибрати найкращий з порівнюваних.

На IV кроці проводиться бальне оцінювання показників на основі висновків експертів для всіх засобів, що порівнюються. Для цього використовуються заздалегідь визначені критерії бальної оцінки. Кількість балів, присвоєних кожному показнику для кожного засобу, формується, спираючись на досвід фахівців (експертів) та перевірені характеристики (можливості), що перевірені на практиці та характеризують засоби, що порівнюються. Приклад одержання бальних оцінок наведено в таблиці 2.

Таблиця 2

Бальна оцінка критеріїв порівняння

№ з/п	Назва критерію	Ваговий коефіцієнт, Кі	Бальна оцінка, Ві							
			1	2	3	4	5	6	7	8
1	1	0,1388889	4	4	5	4	4	5	4	5
2	2	0,25	3	3	4	4	2	5	5	5
3	3	0,0277778	3	2	1	2	2	3	4	4
4	4	0,1944444	3	1	3	3	3	3	3	3
5	5	0,0833333	3	3	1	3	3	1	3	3
6	6	0,3055556	3	4	4	3	3	4	4	3
Q			3,14	3,03	3,61	3,36	2,86	3,92	3,97	3,81

На V кроці, на основі бальних оцінок та вагових коефіцієнтів, визначаються єдині комплексні порівняльні оцінки засобів криптографічного захисту з використанням лінійної згортки (вираз 1).

На VI кроці, за результатами проведеного порівняльного аналізу та розрахованих оцінок для кожного засобу криптографічного захисту, робиться відповідний висновок, при чому кращим вважається засіб, яка отримав найбільшу комплексну оцінку.

За результатами проведеного розрахунку (див. табл. 2) можна зробити висновок, що за 6 критеріями максимальну оцінку отримав засіб №7 (Q=3,97).

Висновки

Запропонована методика може бути використана для дослідження і оцінки засобів криптографічного захисту з урахуванням основних функціональних відмінностей, технологій виготовлення та їх особливостей з точки зору експлуатаційно-технічних параметрів; сервісних параметрів та інших параметрів, що перевіряються.

Недоліками запропонованої методики вибору засобів криптографічного захисту інформації є те, що на другому та третьому кроках (етапах) методики можливе введення експертами своїх суб'єктивних оцінок щодо бальних оцінок засобів та вагових коефіцієнтів різних параметрів, за якими проводиться порівняння. В той же час, зазначені недоліки нівелюються залученням до оцінювання великої кількості експертів з достатньо високим професійним рівнем.

Оцінка засобів криптографічного захисту може проводитися як для тих, що плануються на прийняття для постачання в Збройні сили України, так і для тих, що вже використовуються в існуючій (розгорнутій) системі зв'язку.

Серед напрямків подальших досліджень слід зазначити удосконалення розробленої методики шляхом розробки пропозицій для формування критеріїв, на основі яких визначаються бальні оцінки експертів. Такий підхід дозволить знизити суб'єктивність бальних оцінок експертів та підвищити об'єктивність комплексних порівняльних оцінок засобів криптографічного захисту.

ЛІТЕРАТУРА

1. Барышкова Н. Выбор средств криптографической защиты информации для использования в системах электронного документооборота депозария / Н. Барышкова – Технология. – №4 (50), 2007. – с. 30 – 32.

2. Конявская С.В. Выбор средств криптографической защиты информации для применения в системах ЭДО. – Режим доступа: http://www/okbsapr.ru/konyavskaya _2010-1.htm.

3. Черезов К. Выбор средств криптографической защиты информации / К.Черезов – Information Security. Информационная безопасность. – № 6. – 2007. – с. 54 – 55.

4. Саати Т. Принятие решений. Метод анализа иерархий / Т.Саати – М.: Радио и связь, 1993. – 278 с.

5. Ларичев О.И. Теория и методы принятия решений / О.И. Ларичев. – М.: Логос, 2002. – 392 с.

6. Кини Р.Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. – М.: Радио и связь, 1981. – 560 с.: ил.

7. Лотов А.В., Поспелова И.И. Многокритериальные задачи принятия решений: учебное пособие. – М: МАКС Пресс, 2008. – 197 с.