УДК 004.9

Сергій Володимирович Любарський

ЗАСТОСУВАННЯ МЕТОДУ ЕКСПЕРТНОГО ОЦІНЮВАННЯ ДЛЯ ОБҐРУНТУВАННЯ ВИБОРУ ПЕРЕВАЖНОЇ МОДЕЛІ КРИПТОГРАФІЧНОГО ЗАХИСТУ SOAP-ПОВІДОМЛЕНЬ В АРХІТЕКТУРІ WEB-СЕРВІСІВ

Постановка проблеми. Аналіз останніх досліджень і публікацій

В Україні формується інформаційне суспільство, яке передбачає становлення і в подальшому домінування нових технологічних механізмів, що ґрунтуються на масовому використанні інформаційно-комунікаційних технологій, засобів обчислювальної техніки і телекомунікацій в усіх напрямках розвитку суспільства. Технологія Web, на сьогодняшній день, – це новий виток розвитку Інтернету, на якому основна ставка робиться на розвиток онлайн-сервісів, спрощення процесу отримання інформації та роботи з нею.

Протягом останніх декількох років можна спостерігати якісні зміни, які зазнає World Wide Web. Від сукупності серверів, що містять статичні документи з посиланнями один на одного, сучасний Web практично неможливо уявити без інтерактивних Web-додатків, які обробляють і поміщають в бази даних різнобічну інформацію, динамічно генерують сторінки на скриптових мовах по запиту користувача і, таким чином, обслуговують ту чи іншу сферу діяльності людини, використовуючи при цьому широкий спектр технологій (CGI, ISAPI, ASP, JSP і т. і.).

Взаємна інтеграція цільових завдань різних організацій і установ, що відбувається зараз у всьому світі, неминуче тягне за собою появу технологій і стандартів інтеграції обслуговуючих їх додатків і корпоративних інформаційних систем. Найбільш популярною технологією такої інтеграції в даний час слід назвати новітню технологію ASP.NET, що була запропонована компанією Microsoft [1]. ASP.NET забезпечує обмін даними у форматі XML (eXtensible Markup Language) за протоколом SOAP (Simple Object Access Protocol) і створення Web-сервісів, які застосовують подібний обмін даними.

Стек технологій, який реалізує архітектуру Web-сервісів [2], представлений на рисунку 1.

В рамках представленої архітектури стандарт UDDI відповідає за публікацію та пошук сервісів, стандарт WSDL – за опис їхніх інтерфейсів. Саме на протокол SOAP покладено завдання на передачу фактичних "корисних" даних.

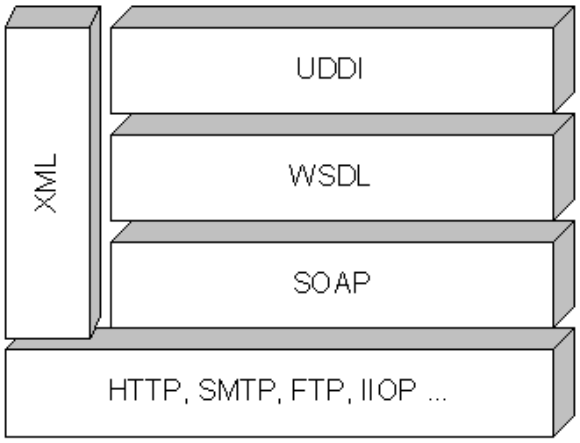

Рис. 1. Стек технологій архітектури веб-сервісів

Фактично SOAP (від англ. Simple Object Access Protocol, простий протокол доступу до об'єктів) – протокол обміну структурованими повідомленнями в розподіленому обчислювальному середовищі. Спочатку SOAP призначався в основному для реалізації віддаленого виклику процедур (RPC). Зараз протокол використовується для обміну довільними повідомленнями у форматі XML, а не тільки для виклику процедур.

Основна особливість SOAP-повідомлень полягає у тому, що вони відповідають структурі одностороннього з'єднання (запиту). Іншими словами вони передаються від відправника до адресата. Однак ці повідомлення комбінуються таким чином, що в результаті відповідають структурі як запиту так і відповіді.

Оскільки в архітектура Web-сервісу базується на відкритих Internet-стандартах, то для мереж спеціального призначення передача конфіденційної (корпоративної) інформації за посередництвом відкритих SOAP-повідомлень є неприпустимою. Порушення безпеки комп'ютерних системи спеціального призначення розглядається як інцидент безпеки інформаційно-аналітичного процесу управління мережами

спеціального призначення через втрату конфіденційності, цілісності, доступності інформаційних ресурсів [3]. Саме тому актуальним є підхід до вирішення проблеми шифрування інформації даних, які передаються по мережі спеціального призначення, для забезпечення конфіденційності інформації.

Для організації безпеки XML-даних в SOAP-повідомленнях необхідно застосовувати до нього, або до окремих його елементів, наприклад SOAP-тіла, деякого алгоритму шифрування.

Шифрування – це свого роду зміна повідомлення за допомогою певних алгоритмів та методів, тобто криптографічний захист даних. Алгоритми шифрування мають передбачати зворотні механізми розшифрування даних для приведення інформації в той варіант представлення даних, який був до шифрування. Найчастіше шифрування та розшифрування, або дешифрування проводиться за допомогою так званих ключів. В залежності від того, які саме використовуються ключі алгоритми, шифрування даних поділяються на:

асиметричні алгоритми шифрування;

алгоритми шифрування з симетричними ключами, або симетричні алгоритми шифрування.

Швидкість шифрування та розшифрування залежить не тільки від алгоритму, але й від кількості даних, які підлягають шифруванню. Тому постає питання щодо шифрування не всього SOAP-повідомлення, а лише окремих елементів чи даних, котрі містять конфіденційну інформацію.

У відповідності з специфікацією безпеки "XML − Encryption Syntax and Processing" до основних методик шифрування даних XML-формату відносяться:

шифрування всього XML;

шифрування будь-якого окремого елемента XML;

шифрування тільки змісту XML.

При цьому кожна з цих методик має свої особливості реалізації, ступінь закриття даних, а також кількість ресурсів, які необхідно витратити на її реалізацію (таблиця 1).

Порівняльний аналіз показує, що кожна з цих методик має свої переваги і недоліки і повинна застосовуватися в залежності від типу даних, які підлягають захисту, їх обсягу, поставленого завдання та особливостей структури дерева SOAP-повідомлення, що передається в мережах спеціального призначення.

Отже, при виборі тієї або іншої методики шифрування (моделі криптографічного захисту) необхідно провести її оцінку, і визначити в якому випадку кожна з цих методик буде найбільш переважною на підставі обраних показників.

Це, в свою чергу, обумовлює звернутися до аналітичного апарату вирішення багатокритеріальних задач на основі експертного оцінювання, де в якості порівняльних альтернатив слід визначити алгоритми блочного шифрування.

Таблиця 1

Порівняння методик шифрування даних *SOAP*-повідомлення

Критерій/ Методика	Шифрування всього SOAP-повідомлення	Шифрування елементу структури SOAP-повідомлення	Шифрування вмісту структурного елементу SOAP-повідомлення
Труднощі реалізації.	Не потрібно проведення попереднього аналізу структури XML.	Необхідно попередньо проводити аналіз даних і структури SOAP-повідомлення для виділення тільки тих елементів структури, які містять інформацію, яка підлягає захисту.	Необхідно попередньо проводити аналіз даних і структури SOAP-повідомлення для виділення тільки тих елементів структури, які містять інформацію, яка підлягає захисту.
Ресурси	Вимагає великих витрат часу, оскільки зашифровується все повідомлення, що особливо відчутно при шифруванні повідомлень великого обсягу	Не великий час шифрування оскільки зашифровується лише обмежене число елементів структури SOAP-повідомлення.	Не великий час шифрування оскільки зашифровується лише обмежене число елементів структури SOAP-повідомлення.
Зручність для користувача	Доступ до даних SOAP-повідомлення неможливий, для роботи з інформацією цього повідомлення необхідно його розшифрувати.	Можлива робота і частковий доступ користувачів до інформації в SOAP-повідомленні	Можлива робота і частковий доступ користувачів до інформації в SOAP-повідомленні.
Ступінь закриття даних	Зашифроване все інформаційне повідомлення.	Зашифровані і закриті тільки ті структурні елементи *XML*, які підлягають захисту	Зашифровані тільки дані, що містяться в елементах структури SOAP-повідомлення.

Формулювання мети статті. Виклад основного матеріалу

Вибір методу розв'язування багатокритеріальної задачі, як у класичній, так і в нечіткій постановці визначається тим, в якому вигляді представлена експертна інформація щодо переваг показників. Якщо представлено експертну інформацію про ступінь або важливість переваги показників та визначені їхні вагові коефіцієнти, то методом розв'язування багатокритеріальної задачі вважається метод результуючого показника.

При вирішенні завдання вибору переважної моделі криптографічного захисту SOAP-повідомлень за багатьма показниками виникає практичне питання – вибір методу оцінки коефіцієнтів важливості.

Аналіз дозволяє визначити основні фактори, що впливають на вибір методу оцінки коефіцієнтів важливості:

фізична сутність завдань управління і відносини між ними. Завдання управління визначаються виходячи з аналізу процесу функціонування системи. Далі необхідно визначити ступінь взаємозв'язку між завданнями, що впливають на метод оцінки їхньої важливості;

складність проведення експертизи й трудомісткість одержання експертної інформації;

ступінь погодженості думок фахівців. Ступінь погодженості думок, у першу чергу, залежить від кількості залучених експертів і рівня їхньої кваліфікації. У той же час, на неї впливає й метод оцінки важливості;

трудомісткість обробки експертних даних. Цей фактор не є головним при сучасному рівні розвитку обчислювальної техніки.

Урахування вищенаведених факторів дозволяє на практиці вибрати раціональний варіант методу оцінки коефіцієнтів важливості.

Найбільше поширення одержали методи Уея, Сааті й Коггера. Найбільш простим методом визначення коефіцієнтів важливості є метод власних векторів Уея.

Метод ґрунтується на даних матриці попарних порівнянь

$$A = \left\| a_{jk} \right\|,\ a_{jk} \in \{-1, 0, 1\}, \qquad (1)$$

де $a_{jk} = -1$ означає перевагу показника a_k над показниками a_j, $a_{jk} = 0$ – рівноцінність a_k і a_j, $a_{jk} = 1$ – перевагу показника a_j над a_k.

Через незручність роботи з негативними числами матрицю попарних порівнянь можна представити як ненегативну матрицю

$$A^+ = \left\| a_{jk} \right\|,\ a_{jk} \in \{0, 1, 2\}, \qquad (2)$$

де числа $\{0, 1, 2\}$ мають вищезазначений зміст.

Склавши числа по кожному з рядків матриці, будемо мати числові характеристики важливості показників, а розділивши їх на загальну суму, одержимо коефіцієнти важливості показників

$$\lambda_j = \frac{\sum_{k=1}^{n} a_{jk}^+}{\sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}^+}, \qquad (3)$$

де з формули (3) витікає умова

$$\sum_{j=1}^{n} \lambda_j = 1. \qquad (4)$$

Упорядкуємо показники якості моделей криптографічного захисту (МКЗ) за важливістю (таблиця 2).

Таблиця 2

Вихідні дані методу ранжування

Рейтингова шкала	Показники якості МОІБ:
0 – перевага C_i над C_j; 1 – рівноцінність C_i і C_j; 2 – перевага C_j над C_i.	C_1 – розмір ключа; C_2 – довжина блоку; C_3 – кількість циклів; C_4 – кількість циклів на раунд; C_5 – кількість раундів; C_6 – швидкість шифрування; C_7 – патентність.

Здійснюємо ранжування семи показників якості МКЗ.

Таблиця 3

Матриця ранжування

C_{ij}	C_{i1}	C_{i2}	C_{i3}	C_{i4}	C_{i5}	C_{i6}	C_{i7}	$\sum$
C_{j1}	1	0	2	2	1	2	2	10
C_{j2}	2	1	2	2	2	1	2	12
C_{j3}	0	0	1	0	0	2	2	5
C_{j4}	0	0	2	1	1	2	2	8
C_{j5}	1	0	2	1	1	2	2	9
C_{j6}	0	1	0	0	0	1	0	2
C_{j7}	0	0	0	0	0	2	1	3

Розраховуємо значення матриці за формулою (3):

$C_1 = \frac{10}{49} = 0{,}204$; $C_2 = \frac{12}{49} = 0{,}244$;

$C_3 = \frac{5}{49} = 0{,}102$; $C_4 = \frac{8}{49} = 0{,}163$;

$C_5 = \frac{9}{49} = 0{,}183$; $C_6 = \frac{2}{49} = 0{,}043$;

$C_7 = \frac{3}{49} = 0{,}061$.

$C_1 = 0{,}204$; $C_2 = 0{,}244$; $C_3 = 0{,}102$; $C_4 = 0{,}163$; $C_5 = 0{,}183$; $C_6 = 0{,}043$; $C_7 = 0{,}061$.

Показники впорядковані наступним чином:

$$C_2 > C_1 > C_5 > C_4 > C_3 > C_7 > C_6 .$$

Проведемо групову експертну оцінку МКЗ по заданих показниках якості. Для отримання експертних даних, що характеризують ступінь відповідності МКЗ заданим критеріям, була створена група з п'яти експертів.

Застосовується метод парних порівнянь на основі наступних вихідних даних (таблиця 4).

Таблиця 4

Вихідні дані методу парних порівнянь

Рангова шкала:	Методи інформаційної безпеки:
0 – перевага a_i над a_j 1 – рівноцінність a_j і a_i 2 – перевага a_j над a_i	a_1 – DES (Data Encryption Standart); a_2 – IDEA (International Decryption Encryption Algorithm); a_3 – Blowfish; a_4 – AES (Advanced Encryption Standard); a_5 – ГОСТ 28147-89.

На основі парних порівнянь альтернатив МКЗ за заданим показником якості від кожного експерта отримані такі нижченаведені дані:

Експерт 1

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	1	0	1	1	2	5
a_{j2}	2	1	1	1	2	7
a_{j3}	1	1	1	1	1	5
a_{j4}	1	1	1	1	2	6
a_{j5}	0	0	1	0	1	2

Експерт 2

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	1	1	0	0	2	4
a_{j2}	1	1	1	1	0	4
a_{j3}	2	1	1	1	2	7
a_{j4}	2	1	1	1	2	7
a_{j5}	0	2	0	0	1	3

Експерт 3

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	1	0	1	1	2	5
a_{j2}	2	1	2	1	2	8
a_{j3}	1	0	1	1	1	4
a_{j4}	1	1	1	1	2	6
a_{j5}	0	0	1	0	1	2

Експерт 4

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	1	0	1	1	2	5
a_{j2}	2	1	1	1	2	7
a_{j3}	1	1	1	0	2	5
a_{j4}	1	1	2	1	1	6
a_{j5}	0	0	0	1	1	2

Експерт 5

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	1	1	1	1	1	5
a_{j2}	1	1	1	1	2	6
a_{j3}	1	1	1	1	1	5
a_{j4}	1	1	1	1	2	6
a_{j5}	1	0	1	0	1	3

Підсумовуючи отримані дані від кожного експерта, одержуємо матрицю за конкретним показником якості:

МКЗ	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	$\sum$
a_{j1}	5	3	6	4	9	27
a_{j2}	7	5	8	5	9	34
a_{j3}	4	2	5	6	8	25
a_{j4}	6	5	4	5	8	28
a_{j5}	1	1	2	2	5	11

Розраховуємо значення матриці за формулою (3):

$$a_1 = \frac{24}{125} = 0{,}192 ; \qquad a_2 = \frac{32}{125} = 0{,}256 ;$$

$$a_3 = \frac{26}{125} = 0{,}208 ; \qquad a_4 = \frac{31}{125} = 0{,}248 ;$$

$$a_5 = \frac{12}{125} = 0{,}096 .$$

І так далі аналогічним порядком по всіх показниках якості МКЗ.

Усереднюємо значення вагових коефіцієнтів по кожному показнику якості, результати зводимо у таблицю 5.

Виходячи з результатів розрахунків та обраних показників якості, пропонується використання методу шифрування SOAP-повідомлення за алгоритмом симетричного блочного шифрування AES [4].

У симетричних блокових шифрах, на відміну від потокових, обробці підлягають групи елементів відкритого тексту (блоки даних). Під час такого шифрування кожен блок даних, який обробляється, по-перше, піддається

перетворенню декілька раундів, що, в свою чергу, спричинює лавинний ефект.

По-друге, кожен елемент блоку даних залежить від всіх елементів цього ж блоку.

Таблиця 5

Матриця обчислення підсумкових ваг альтернатив

	C_{j2}	C_{j5}	C_{j4}	C_{j3}	C_{j7}	C_{j6}	C_{j1}	W(i)
	0,261	**0,217**	**0,174**	**0,130**	**0,087**	**0,087**	**0,043**	
a_{j1}	(0,070+0,077+0,070+0,069+ +0,087)/5=0,074	0,156	0,367	0,050	0,331	0,236	0,162	0,180
a_{j2}	(0,356+0,241+0,272+0,260+ +0,330)/5=0,292	0,302	0,097	0,337	0,232	0,165	0,417	0,255
a_{j3}	(0,133+0,115+0,105+0,117+ +0,171)/5=0,128	0,156	0,097	0,116	0,059	0,232	0,176	0,132
a_{j4}	(0,382+0,490+0,497+0,490+ +0,345)/5=0,441	0,317	0,097	0,186	0,305	0,308	0,162	**0,285**
a_{j5}	(0,043+0,049+0,040+0,045+ +0,063)/5=0,048	0,063	0,323	0,267	0,059	0,052	0,075	0,130

Етап, що передбачає підраховування підсумкової ваги кожної з альтернатив і визначення найкращої альтернативи.

$$W = \max_{i}(W(i)) \Rightarrow a_{rat}.$$
$$W(i) = \sum_{j=1}^{m} a_{ij} \cdot A(j), \quad (5)$$

де m – кількість показників, $m = \overline{1, q}$, i – кількість альтернатив, $i = \overline{1, n}$, A(j) – функція, що повертає j-й за важливістю показник, $j = \overline{1, l}$.

Підсумкова вага першої альтернативи (a_{j1}) обчислюється наступним чином:

W(1) = (0,074 * 0,261) + (0,156 * 0,217) + (0,367 * 0,174) + (0,050 * 0,130)+ (0,331 * 0,087) + (0,236 * 0,087) + (0,162 * 0,043) = 0,180.

Підсумкова вага першої альтернативи (a_{j2}) обчислюється наступним чином:

W(2) = (0,292 * 0,261) + (0,302 * 0,217) + (0,097 * 0,174) + (0,337 * 0,130)+ + (0,232 * 0,087) + (0,165 * 0,087) + (0,417 * 0,043) = 0,255.

Підсумкові ваги інших альтернатив підраховуються за аналогією, результати занесені у таблицю 5.

Симетричні шифри застосовують для зберігання конфіденційних даних на фізичних носіях та шифрування інформації під час її передавання через комп'ютерні мережі.

Однак, якщо безпосередньо використовувати будь-який симетричний блоковий шифр без застосування додаткових криптографічних перетворень, то у процесі шифрування буде наявний ряд недоліків. Зокрема в таких випадках неможливо приховати структуру інформації, яка захищається за рахунок того, що під час шифрування використовуються блоки фіксованого розміру та один і той же самий секретний ключ. Тому, з метою усунення негативних властивостей процесу шифрування і залежно від галузі, застосовують ряд базових режимів блокового шифрування, які стандартизовані Національним інститутом стандартизації та технологій (National Institute of Standards and Technology):

ECB (Electronic Code Book) – електронна кодова книга;

CBC (Cipher Block Chaining) – зчеплення блоків по шифротексту;

CFB (Cipher Feed Back) – зворотне завантаження шифротексту;

OFB (Output Feed Back) – зворотне завантаження вихідних даних.

Отже, алгоритм блокового симетричного шифрування AES може використовуватися в одному з наступних п'яти режимів: ECB, CBC, CFB, OFB, режим "лічильника".

Для вибору найбільш переважного режиму застосування алгоритму для реалізації на багатопроцесорних системах пропонується розглянути наступний набір критеріїв:

можливість розпаралелювання процедури шифрування (розшифрування). Даний критерій означає можливість шифрування (розшифрування) двох і більше блоків одночасно;

простота реалізації, що означає, що при шифруванні і розшифруванні використовується тільки шифрувальне перетворення AES, а розшифрувальне не використовується;

можливість попередніх обчислень. Даний критерій означає, що можна почати обчислення до надходження відкритого тексту.

Далі наведена таблиця 6 оцінки застосування кожного з режимів шифрування за вищенаведеними критеріями.

Таким чином, відповідно до проведеного аналізу для розроблення паралельної версії алгоритму нами був обраний режим "лічильника".

Таблиця 6

Оцінка режимів застосування алгоритму AES

Критерій	ECB	CBC	CFB	OFB	Режим „лічильника”
Можливість розпаралелювання процедури шифрування	+	-	-	-	+
Можливість розпаралелювання процедури розшифрування	+	+	-	-	+
Простота реалізації	+	-	+	+	+
Можливість попередніх обчислень	-	-	-	+	+

Висновки

Актуальність дослідження ґрунтується на унеможливленні передачі конфіденційної інформації в архітектурі з Web-сервісами корпоративного призначення на основі існуючих стандартів, що носять відкритий характер.

В мережевих архітектурах на основі Web-сервісів за технологією .NET об’єктом захисту інформації виступає структура інформаційного повідомлення обміну даними за протоколом SOAP.

Для організації захищеного обміну SOAP-повідомленнями, необхідно інтегрувати в модулі інтерпритації інформаційного SOAP-повідомленнями методи криптографічного захисту даних.

Отже, рішення задачі вибору переважної моделі криптографічного захисту SOAP-повідомленнями полягало у визначенні переважності показників якості моделей криптографічного захисту та оцінці кожної з альтернатив за відповідними показниками для виявлення найбільш переважної з них. В якості такого методу було запропоновано метод парних порівнянь на основі експертного оцінювання.

Відмінність даного методу від існуючих полягає в застосуванні відкритих експертних оцінок та зменшенні неузгодженості думок експертів. Також метод враховує якісний та кількісний характер показників якості моделі.

Результати розрахункового прикладу дозволили запропонувати застосувати метод шифрування SOAP-повідомлення за алгоритмом симетричного блочного шифрування AES, котрий має забезпечити необхідний ступінь криптозахищеності інформаційного повідомлення на основі обраних показників якості.

Література

1. Мэтью Мак-Дональд Microsoft ASP.NET 4.0 с примерами на C# 2010 для профессионалов. / Мэтью Мак-Дональд, Адам Фримен, Марио Шпушта // 4-е издание. – М.: Вильямс, 2011. – 1024 с.
2. Шелякин П.Ю. Архитектура, ориентированная на сервисы / Шелякин П.Ю., Садыков С.С., Андрианов Д.Е. // Обработка информации: методы и системы: сб. научных статей. – М.: Горячая линия – Телеком, 2003. – С. 205–209.
3. Закон України. Про захист інформації в інформаційно-телекомунікаційних системах. [Електронний ресурс] / Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.
4. Зензин О.С. Стандарт криптографической защиты – AES. Конечные поля / О.С. Зензин, М.А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2002. – 176 с.

В статье рассматривается алгоритм решения задачи обеспечения безопасного информационного обмена сообщениями по протоколу SOAP (Simple Object Access Protocol) в распределенной клиент-серверной архитектуре Web-сервисов на основе применения метода экспертного оценивания.

Ключевые слова: Web-сервіс, SOAP-повідомлення, шифрування.

The article considers the algorithm for ensuring safety information messaging protocol SOAP (Simple Object Access Protocol) in a distributed architecture Web-services on basis of the expert evaluation method.

Key words: Web-service, SOAP-message, encryption.