УДК 681.3.06(075.8)

АНОНІМНІСТЬ ЯК КРИТЕРІЙ ОЦІНКИ ЗАХИЩЕНОСТІ ПРОТОКОЛІВ СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Галина Козіна, Геннадій Нікуліщев
Запорізький національний технічний університет

Анотація: **Розглянуто три протоколи сліпого підпису. Наведено атаки на анонімність підпису. Розглянуті два протоколи сліпого підпису не забезпечують захищеність підписаного повідомлення за критерієм анонімності, одна схема стійка за цим критерієм.**
Summary: **The article is dedicated to the blind digital signature schemes. Three of them are investigated according to the anonymity breaking attacks. Two schemes are exposed to such attacks and one is secure.**
Ключові слова: **Електронний цифровий підпис, сліпий підпис, анонімність, атака.**

I Вступ

На часі разом із завданнями реалізації стандартних схем електронного цифрового підпису (ЕЦП) практичну актуальність і значущість мають реалізації інших схем, зокрема, сліпого підпису [1 – 4].

Сліпий ЕЦП дозволяє авторові документа довести його юридичну значимість, не розкриваючи власної особи. Це може знадобитися, зокрема, при проведенні електронного голосування чи розрахунку електронними грошима.

В типовій схемі сліпого підпису, як правило, приймають участь три сторони – емітент документу, підписувач та валідатор. Емітент створює документ, який має підписати підписувач. При цьому, підписувач не має знати вмісту документа та вигляду остаточного підпису, для чого емітент маскує документ за допомогою певного криптографічного перетворення. Підписувач підписує замаскований документ, а емітент на основі його підпису формує остаточний ЕЦП під документом у відкритому вигляді згідно зі схемою сліпого підпису. Валідатор перевіряє правильність підпису за допомогою відкритого ключа емітента.

Наприклад, в схемі електронного голосування як емітент виступає виборець, підписувача – дільнична виборча комісія, валідатора – центральна виборча комісія. Виборець заповнює бюлетень, маскує його, щоб зберегти конфіденційність голосу, і передає на підпис у дільничну виборчу комісію. Комісія, засвідчивши особу виборця, підписує його бюлетень, не знаючи, за кого той проголосував. Центральна виборча комісія отримує бюлетень у відкритому вигляді і перевіряє валідність підпису дільничої комісії, не знаючи при цьому, хто заповнив цей бюлетень.

Таким чином, у випадку сліпого ЕЦП до критеріїв захищеності схеми підпису додається анонімність – неможливість відстежити за підписаним документом його автора і однозначно їх пов’язати. Втім, в деяких схемах у підписувача може виявитись можливість порушити анонімність, оскільки в процесі формування остаточного підпису він обмінюється з емітентом документа додатковими параметрами, передбаченими схемою підпису. Якщо підписувач збереже ці параметри, пов’язавши їх з конкретним емітентом, а в подальшому зможе отримати доступ до документу із власним підписом у відкритому вигляді, то він зможе спробувати вирахувати його автора за допомогою збережених параметрів. Обчисливши маскуючі параметри, які використовував емітент, підписувач зможе однозначно пов’язати його з документом, що призведе до порушення анонімності. Наприклад, у схемі електронного голосування це означатиме, що буде відомо, за кого проголосував конкретний виборець.

II Схеми сліпого ЕЦП, нестійкі до порушення анонімності

Розглянемо декілька протоколів ЕЦП, в яких у підписувача є можливість здійснити атаку порушення анонімності. Стійкість всіх протоколів засновано на складності задачі знаходження дискретного логарифма на еліптичній кривій.

В усіх схемах як емітент документа виступає користувач B, який підписує в підписувача A певний документ m, $0<m<n$, так, щоб підписувач A у момент формування підпису не міг ознайомитися із вмістом документу m. Валідатором може виступити будь-хто з них, або третя особа.

Загальні параметри протоколів, відомі підписувачу і всім користувачам: основне поле $GF(p)$; еліптична крива над основним полем; базова точка P простого порядку n групи точок еліптичної кривої; функція хешування H.

Кожен протокол складається з трьох етапів: генерація ключів, формування сліпого підпису, перевірка сліпого підпису.

Генерацію ключів виконує підписувач А. Він обирає випадкове число d з діапазону $1<d<n$ і множить на нього базову точку P. Отриманий добуток – точка Q – становить відкритий ключ підписувача, а число d – закритий.

Схема 1.

Розглянемо протокол, який є модифікацією алгоритму Шнорра для еліптичних кривих.

Формування сліпого підпису починає підписувач А, обираючи одноразовий випадковий секретний ключ k з діапазону $1<k<n$, та множить його на базову точку P, отримуючи точку E. Молодші ($|n|-1$) розрядів хеш-образу $H(E)$ точки E формують число h_E, яке має бути ненульовим. Підписувач А відправляє користувачеві В значення E та h_E.

Користувач В перевіряє приналежність точки E еліптичній кривій, обирає випадкове число α з діапазону $1<\alpha<n$ та множить на нього точку E, отримуючи точку R. Молодші ($|n|-1$) розрядів хеш-образу $H(R)$ точки R формують число h_R, яке має бути ненульовим. Далі користувач В обчислює параметр β за формулою

$$\beta = \frac{h_R}{h_E} \bmod n. \tag{1}$$

За допомогою параметрів α і β, які не мають співпадати, користувач В засліплює документ m, використовуючи співвідношення

$$m' = \frac{\beta}{\alpha} m \bmod n. \tag{2}$$

Користувач В направляє значення m', яке має бути ненульовим, підписувачу А. Підписувач А обчислює підпис s' за формулою

$$s' = (h_E \cdot d \cdot m' + k) \bmod n. \tag{3}$$

Підписувач А відправляє значення s' користувачеві В, який перевіряє коректність обчисленого значення s' за формулою

$$s' \cdot P = h_E \cdot m' \cdot Q + E. \tag{4}$$

Якщо підпис s' визнається справжнім, користувач В формує підпис s під документом m за формулою

$$s = \alpha \cdot s' \bmod n. \tag{5}$$

Сліпим підписом під документом m вважається пара значень $<R, s>$.

Перевірка підпису $<R, s>$ під документом m здійснюється за допомогою відкритого ключа Q підписувача А. Молодші ($|n|-1$) розрядів хеш-образу $H(R)$ точки R формують число h_R, яке використовується у перевірочному співвідношенні

$$s \cdot P = h_R \cdot m \cdot Q + R. \tag{6}$$

Якщо співвідношення (6) виконується, то підпис вважається справжнім.

Покажемо коректність формування та перевірки сліпого підпису

$$s \cdot P = \alpha \cdot s' \cdot P = \alpha \cdot (k + h_E \cdot m' \cdot d) \cdot P = R + \beta \cdot h_E \cdot m \cdot Q = R + h_R \cdot m \cdot Q.$$

Таким чином, протокол дозволяє користувачеві В отримати під документом m підпис підписувача А, при цьому не розкриваючи підписувачу А ані вміст документу, ані вигляд підпису під ним. Інші користувачі можуть перевірити, що документ m справді підписаний підписувачем А, однак не можуть встановити його приналежність користувачеві В.

Втім, підписувач А може здійснити атаку порушення анонімності, якщо зберігатиме всі проміжні значення, які він обчислює та отримує від користувачів під час формування сліпого підпису. Зведені у базу даних, кожен запис якої міститиме ідентифікатор користувача та параметри підпису, ці значення можуть бути використані для визначення автора документа із валідним підписом підписувача А.

Отримавши документ m із підписом $<R,s>$, підписувач А має для кожного запису своєї бази даних обчислити параметр α'

$$\alpha' = \frac{s}{s'} \bmod n. \tag{7}$$

За допомогою цього параметра для кожного запису бази даних необхідно обчислити точку R' як добуток α' і точки E. Рядок, в якому відбудеться збіг R і R', міститиме ідентифікатор користувача, який надав підписувачеві А документ m для формування сліпого підпису $<R,s>$.

Таким чином, виявляється, що маскуючий параметр β є надлишковим, оскільки він ніяк не впливає на можливість підписувача порушити анонімність абонентів і не приймає участь у його розрахунках.

Приклад 1.

Нехай в протоколі використовуються наступні відкриті параметри: еліптична крива $y^2=x^3+5x+9 \bmod 59$, базова точка P=(0,3) з простим порядком n=79 ($|n|$=7). Як хеш-функція використовується MD5.

Підписувач А має асиметричну пару ключів: секретний ключ d=15 і відповідний йому відкритий ключ Q=(34, 22). Нехай підписувач А декілька разів використав свій секретний ключ для постановки сліпого підпису і накопичів базу даних, представлену в табл.1.

Таблиця 1 – База даних підписувача А (приклад 1)

№	k	E	h_E	m'	s'
B1	17	(49,32)	16	63	48
B2	3	(41, 20)	52	51	46
B3	25	(54,6)	60	16	47
B4	11	(58,48)	27	65	29
B5	40	(33,48)	34	30	14

Нехай підписувач А отримав повідомлення m=36 з підписом $<R, s>=<(49,27), 3>$. Перевіривши, що це його підпис за співвідношенням (6), для кожного з рядків бази даних з табл. 1 він проводить необхідні розрахунки за формулою (7). Розрахунки зведені в табл. 2.

Як видно з табл. 2, збіг R' з R відбувся в другому рядку, отже, автором документу є користувач В2, якому відповідає цей рядок бази даних підписувача А.

Таблиця 2 – Розрахунки підписувача А (приклад 1)

№	α'	R'	R
B1	5	(24,18)	(49,27)
B2	43	(49,27)	(49,27)
B3	32	(41,39)	(49,27)
B4	11	(54,53)	(49,27)
B5	51	(30,14)	(49,27)

Схема 2.

Розглянемо протокол, який є модифікацією алгоритму Ель-Гамаля для еліптичних кривих над простим полем.

Формування сліпого підпису починає підписувач А, обираючи одноразовий випадковий секретний ключ k з діапазону $1<k<n$, та множить його на базову точку P, отримуючи точку E. Молодші ($|n|$–1) розрядів хеш-образу $H(E)$ точки E формують число h_E, яке має бути ненульовим. Підписувач А відправляє користувачеві В значення E та h_E.

Користувач В перевіряє приналежність точки E еліптичній кривій, обирає випадкове число α з діапазону $1<\alpha<n$ та множить на нього точку E, отримуючи точку R. Молодші ($|n|$–1) розрядів хеш-образу $H(R)$ точки R формують число h_R, яке має бути ненульовим. Далі користувач В обчислює параметр β за формулою

$$\beta = \frac{h_R}{h_E} \bmod n. \tag{8}$$

За допомогою параметрів α і β, які не мають співпадати, користувач В маскує документ m, використовуючи співвідношення

$$m' = \frac{\alpha}{\beta} m \bmod n. \tag{9}$$

Користувач В направляє значення m', яке має бути ненульовим, підписувачу А. Підписувач А обчислює підпис s' за формулою (10) і направляє його користувачеві В.

$$s' = (h_E \cdot d + k \cdot m') \bmod n. \tag{10}$$

Користувач В перевіряє коректність обчисленого значення s' за формулою

$$s' \cdot P = h_E \cdot Q + m' \cdot E. \tag{11}$$

Якщо підпис s' визнається справжнім, користувач В формує підпис s під документом m за формулою

$$s = \beta \cdot s' \bmod n . \tag{12}$$

Сліпим підписом під документом m вважається пара значень $<R, s>$.

Перевірка підпису $<R, s>$ під документом m здійснюється за допомогою відкритого ключа Q підписувача А. Молодші ($|n|-1$) розрядів хеш-образу $H(R)$ точки R формують число h_R, яке використовується в перевірочному співвідношенні

$$s \cdot P = h_R \cdot Q + m \cdot R . \tag{13}$$

Якщо співвідношення (13) виконується, то підпис вважається справжнім.

Покажемо, що коректність формування та перевірки сліпого підпису дотримується:

$$s \cdot P = \beta \cdot s' \cdot P = \beta \cdot (d \cdot h_E + m' \cdot k) \cdot P = \beta \cdot h_E \cdot Q + m \cdot \alpha \cdot E = h_R \cdot Q + m \cdot R.$$

Як і попередній, цей протокол дозволяє користувачеві В отримати під документом m підпис підписувача А, при цьому не розкриваючи підписувачу А ані вміст документу, ані вигляд підпису під ним. Інші користувачі можуть перевірити, що документ m справді підписаний підписувачем А, однак не можуть встановити його приналежність користувачеві В.

Однак, цей протокол також піддається атаці порушення анонімності з боку підписувача А, за умови, якщо він зберігатиме всі обчислені та отримані від користувачів проміжні параметри у базі даних, яка дозволяє співставити їх з ідентифікатором користувача.

Якщо підписувач А отримає документ m з власним валідним підписом $<R, s>$, то він зможе визначити його автора, обчисливши для кожного запису бази даних параметри α' і β'

$$\beta' = \frac{s}{s'} \bmod n , \tag{14}$$

$$\alpha' = \frac{\beta' \cdot m'}{m} \bmod n . \tag{15}$$

За допомогою цих параметрів для кожного запису бази даних необхідно обчислити точку R' як добуток α' і точки E. Рядок, в якому відбудеться збіг R і $R,'$ міститиме ідентифікатор користувача, який надав підписувачеві А документ m для формування сліпого підпису $<R,s>$.

Приклад 2.

Нехай в протоколі використовуються наступні відкриті параметри: еліптична крива $y^2=x^3+5x+9 \ mod \ 59$, базова точка P=(0,3) з простим порядком n=79 ($|n|$=7). Як хеш-функція використовується MD5.

Підписувач А має асиметричну пару ключів: секретний ключ d=34 і відповідний йому відкритий ключ Q=(24, 18). Нехай підписувач А декілька разів використав свій секретний ключ для постановки сліпого підпису і накопичив базу даних, представлену в табл. 3.

Таблиця 3 – База даних підписувача А (приклад 2)

№	k	E	h_E	m'	s'
B1	26	(3,46)	6	14	15
B2	18	(19, 58)	43	78	22
B3	47	(3,13)	22	70	9
B4	53	(45,26)	74	53	32
B5	36	(13,41)	35	41	59

Нехай підписувач А отримав повідомлення m=19 з підписом $<R, s>$=<(35,15), 26>. Перевіривши за допомогою (13), що це його підпис, для кожного з рядків бази даних з табл. 3 він проводить необхідні розрахунки за формулами (14, 15). Розрахунки зведені в табл. 4.

Таблиця 4 – Розрахунки підписувача А (приклад 2)

№	β'	α'	R'	R
B1	7	1	(3,46)	(35,15)
B2	73	71	(13,18)	(35,15)
B3	38	61	(45,33)	(35,15)
B4	65	15	(35,15)	(35,15)
B5	54	50	(54,53)	(35,15)

Як видно з табл. 4, збіг R' з R відбувся в четвертому рядку, отже, автором документу є користувач В4, якому відповідає цей рядок бази даних підписувача А.

III Схема сліпого ЕЦП, стійка до порушення анонімності

Розглянемо ще один протокол, який є модифікацією російського стандарту ЕЦП ГОСТ Р.34-10 2001.

Формування сліпого підпису починає підписувач А, обираючи одноразовий випадковий секретний ключ k з діапазону $1<k<n$, та множить його на базову точку P, отримуючи точку E. Цю точку підписувач відправляє користувачеві В.

Користувач В обирає випадкові маскуючі параметри α та β з діапазону $1<\alpha,\beta<n$ і обчислює точку С за формулою

$$C = \alpha \cdot E + \beta \cdot P. \tag{16}$$

Користувач В обчислює величини r та r' як абсциси точок C та E відповідно. За допомогою цих величин користувач В маскує повідомлення:

$$m' = \frac{r'}{r} m\alpha \bmod n. \tag{17}$$

Користувач В направляє значення m', яке має бути ненульовим, підписувачу А. Підписувач А обчислює підпис s' за формулою (18) і направляє його користувачеві В:

$$s' = (r' \cdot d + k \cdot m') \bmod n. \tag{18}$$

Користувач В перевіряє коректність обчисленого значення s' за формулою

$$s' \cdot P = r' \cdot Q + m' \cdot E. \tag{19}$$

Якщо підпис s' признається справжнім, користувач В формує підпис s під документом m за формулою

$$s = (s' \frac{r}{r'} + \beta m) \bmod n. \tag{20}$$

Сліпим підписом під документом m вважається пара значень $<r, s>$.

Перевірка підпису $<r, s>$ під документом m здійснюється за допомогою відкритого ключа Q підписувача А. Обчислюється точка С′

$$C' = \frac{s}{m} \cdot P - \frac{r}{m} \cdot Q. \tag{21}$$

Якщо абсциса цієї точки збігається із значенням r, то підпис вважається правильним.

Покажемо, що коректність формування та перевірки сліпого підпису дотримується:

$$C' = \frac{s' \frac{r}{r'} + \beta m}{m} P - \frac{rd}{m} P = \left(\frac{(r' \cdot d + k \cdot m')r}{mr'} + \beta - \frac{rd}{m} \right) P = \left(\frac{kr'm\alpha r}{mr'r} + \beta \right) P =$$

$$= (k\alpha + \beta) P = \alpha E + \beta P = C$$

Як і попередні, цей протокол дозволяє користувачеві В отримати під документом m підпис підписувача А, при цьому не розкриваючи підписувачу А ані вміст документу, ані вигляд підпису під ним. Інші користувачі можуть перевірити, що документ m справді підписаний підписувачем А, однак не можуть встановити його приналежність користувачеві В.

Досліджемо цей протокол на анонімність.

Підписувач А, отримавши документ m з власним валідним підписом $<r, s>$, може обчислити для кожного запису бази даних параметри α' і β'

$$\alpha' = \frac{r \cdot m'}{m \cdot r'} \bmod n, \tag{22}$$

$$\beta' = \frac{s - s' \cdot \frac{r}{r'}}{m} \bmod n. \tag{23}$$

Отримавши ці значення, підписувач А має можливість для кожного запису бази даних обчислити точку C'', скориставшись рівнянням перевірки підпису (19),

$$C'' = \alpha' \cdot E + \beta' \cdot P = \frac{r \cdot m'}{m \cdot r'} \cdot E + \frac{s - s' \cdot \frac{r}{r'}}{m} \cdot P = \frac{r}{m \cdot r'} \cdot \left(s'P - r'Q\right) + \frac{s}{m} \cdot P - \frac{s' \cdot r}{m \cdot r'} \cdot P =$$

$$= \frac{s}{m} \cdot P - \frac{r}{m} \cdot Q.$$

Значення точки C'' не залежить від параметрів r', s', m' і не дає можливості вирахувати автора документа m.

Таким чином, розглянутий протокол не піддається атаці порушення анонімності з боку підписувача А, навіть за умови, якщо він зберігатиме всі обчислені та отримані від користувачів проміжні параметри у базі даних, яка дозволяє співставити їх з ідентифікатором користувача. Підписувач А не може встановити однозначної відповідності документу жодному з абонентів. Проілюструємо це на обчислювальному прикладі.

Приклад 3.

Нехай в протоколі використовуються наступні відкриті параметри: еліптична крива $y^2=x^3+5x+9 \ mod \ 59$, базова точка P=(0,3) з простим порядком n=79 ($|n|$=7). Як хеш-функція використовується MD5.

Підписувач А має асиметричну пару ключів: секретний ключ d=21 і відповідний йому відкритий ключ Q=(21, 42). Нехай підписувач А декілька разів використав свій секретний ключ для постановки сліпого підпису і накопичів базу даних, представлену в табл. 5.

Таблиця 5 – База даних підписувача А (приклад 3)

№	k	E	r'	m'	s'
B1	55	(19,1)	19	65	24
B2	19	(17, 13)	17	78	22
B3	32	(42,12)	42	47	16
B4	48	(54,53)	54	25	43
B5	23	(2,33)	2	75	29

Нехай підписувач А отримав повідомлення m=38 з підписом $<r, s>$=<22, 73>. Перевіривши за допомогою (21), що це його підпис, для кожного з рядків бази даних з табл. 1 він проводить необхідні розрахунки за формулами (22) – (23). Результати розрахунків зведені в табл. 6.

Таблиця 6 – Результати розрахунків підписувача А (приклад 3)

№	α'	β'	C''	r
B1	51	35	(22,18)	22
B2	21	71	(22,18)	22
B3	35	61	(22,18)	22
B4	41	3	(22,18)	22
B5	3	6	(22,18)	22

Як видно з табл. 6, збіг абсциси обчисленої точки C'' з r відбувся в кожному рядку, отже, підписувач А не може встановити однозначної відповідності між документом та будь-яким з абонентів.

IV Висновки

Таким чином, незважаючи на те, що схеми сліпого ЕЦП дозволяють емітенту документа отримати підпис підписувача під ним, не розкриваючи підписувачу ані вміст документу, ані остаточний вигляд підпису, деякі з них мають вразливості, які можуть привести до порушення анонімності емітента. Недоліки побудови алгоритму сліпого підпису дозволяють підписувачеві встановити однозначний зв'язок між підписаним ним документом і його емітентом. Для перевірки схеми сліпого ЕЦП за критерієм анонімності необхідно з'ясувати, чи є у підписувача можливість обчислити підпис в не замаскованому вигляді за допомогою бази даних проміжних значень, яку він створює при постановці підпису. В статті розглянуто два протоколи сліпого підпису, які не забезпечують захищеність підписаного повідомлення за критерієм анонімності, і одна схема, стійка за цим критерієм. Дослідження останньої схеми показує, що співвідношення між маскуючими параметрами необхідно обирати таким чином, щоб за ними було неможливо вирахувати автора документу, який підписується.

В подальшому авторами планується аналіз інших відомих протоколів сліпого підпису за критерієм анонімності.

Література: ***1.*** *Молдовян Н. А. Новые протоколы слепой подписи / Н. А. Молдовян, Е. В. Морозова, А. А. Костин, С. Е. Доронин // Программные продукты и системы. – 2008. – № 4. – С. 161–164.* ***2.*** *Молдовян Н. А. Новые протоколы слепой подписи / Н. А. Молдовян, П. А. Молдован // Безопасность информационных технологий. – М.:МИФИ. – 2007. – № 3. – С. 17-21.* ***3.*** *Ростовцев А. Г. Подпись "вслепую" на эллиптической кривой для электронных денег / А. Г. Ростовцев // Проблемы информационной безопасности. Компьютерные системы. – 2000. - № 1. – С. 40–45.* ***4.*** *Костин А. А. О реализации протоколов слепой подписи и коллективной подписи на основе стандартов цифровой подписи / Костин А. А, Молдован Н. А., Фаль А. М. //Материалы V1 Санкт-Петербургской межрегиональной конференции «Информационная безопасность России (ИБРР-2009). Санкт-Петербург, 28–30 октября. СПб.: СПОИСУ, 2009, с. 111.*

УДК 681.3.06

ВДОСКОНАЛЕННЯ АЛГОРИТМУ НАВЧАННЯ БАГАТОШАРОВОГО ПЕРСПЕТРОНУ, ПРИЗНАЧЕНОГО ДЛЯ РОЗПІЗНАВАННЯ МЕРЕЖЕВИХ АТАК

Ігор Терейковський
Національний технічний університет України "КПІ"

Анотація: **Обґрунтована необхідність та проведено вдосконалення математичного забезпечення алгоритму навчання багатошарового перспетрону, призначеного для розпізнавання мережевих атак на комп'ютерні системи та мережі.**
Summary: **The necessity and carried out the improvement of mathematics learning algorithm for multilayer perspetron designed to detect network attacks on computer systems and networks.**
Ключові слова: **Багатошаровий перспетрон, захист інформації, розпізнавання мережевих атак.**

Практичний досвід та аналіз публікацій [1 – 3] вказують на те, що в останнє десятиліття розпізнавання атак на інформацію комп'ютерних систем та мереж (КСМ) є однією із найбільш важливих та актуальних проблем в галузі захисту інформації. Складність проблеми обумовлена багатофакторною динамікою функціонування сучасних КСМ, великою різноваріантністю відомих та постійним виникненням нових видів атак. Тому розпізнати атаку за допомогою методів, які базуються на класичному аналізі статистики функціональних параметрів КСМ, в багатьох випадках практично неможливо. Як наслідок знаходять застосування різноманітні альтернативні математичні теорії, в тому числі і теорія штучних нейронних мереж (НМ), що довела свою ефективність в задачах аналізу багатопараметричних зашумлених даних. Однак, не зважаючи на окремі вдалі спроби та загальновизнану перспективність систем розпізнавання атак на базі НМ їх достовірність залишається не достатньою. Цим визначається актуальність досліджень щодо застосування НМ для розпізнавання атак на КСМ.

І Аналіз нейромережевих методів розпізнавання атак

Відповідно до [1 – 3] суть загальнопоширених нейромережевих методів розпізнавання атак полягає у визначенні значимих відмінностей характеристик поточного функціонування КСМ від характеристик функціонування в нормальних умовах. Відомі вдалі спроби розпізнавати за допомогою НМ віддалені мережеві атаки, комп'ютерні віруси, приховані факти передачі зашифрованих даних, спам-листи електронної пошти. При цьому типовий алгоритм застосування НМ в системах розпізнавання атак складається з наступних етапів:

– Визначається номенклатура фізичних параметрів підзахисного об'єкта, що відповідають вхідним параметрам НМ;
– проводиться попередня обробка та кодування фізичних параметрів з метою їх адаптації до НМ;
– визначається номенклатура вихідних параметрів НМ;
– розробляється система кодування вихідних параметрів НМ;
– визначається оптимальний тип архітектури НМ;
– оптимізуються параметри архітектури НМ;