КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.3.6387
УДК 004.056.5:004.75

Смірнов Сергій Анатолійович
кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

Поліщук Людмила Іванівна
старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-5093-1581
pli_80@ukr.net

Смірнова Тетяна Віталіївна
кандидат технічних наук
Центрально український національний технічний університет, Кропивницький, Україна
OrcID:0000-0001-6896-0612
sm.tetyana@gmail.com

Конопліцька-Слободенюк Оксана Костянтинівна
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-9981-5194
ksuha80@gmail.com

Смірнов Олексій Анатолійович
доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

МЕТОД ФОРМУВАННЯ АНТИВІРУСНОГО ЗАХИСТУ ДАНИХ З ВИКОРИСТАННЯМ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ МЕТАДАНИХ

Анотація. У даній статті розроблено метод антивірусного захисту даних у ТКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи. Він призначений для рішення проблематики, яка полягає в тому, що з метою підвищення ефективності використання засобів антивірусного захисту даних і мінімізації наслідків подібних кіберзлочинів, своєчасне виявлення і локалізація комп'ютерних вірусів є вкрай важливим і разом з тим складним завданням. Основними складовими методу, що пропонується в даній роботі, є: алгоритми формування множини маршрутів передачі метаданих, метод контролю ліній зв'язку ТКС, моделі системи нейромережних експертів безпечної маршрутизації. Відмінною рисою алгоритмів формування множини маршрутів передачі метаданих є показники оптимізації і обмеження, що вводяться, для безпечної маршрутизації. Новизна методу контролю ліній зв'язку ТКС полягає в обліку «скомпрометованих» біт даних спеціальних сигнатур, що передаються у хмарні антивірусні системи. Це дозволить знизити ймовірність маніпуляцій метаданими, які передаються в вузли програмного сервера. Особливістю розробленої системи нейромережних експертів є комплексність використання нейронних мереж типу АРТ і багатошарового персептрону для рішення завдання безпечної маршрутизації, що дозволить підвищити точність ухвалення правильного рішення про несанкціонований доступ до волоконно-оптичних ліній зв'язку.

Ключові слова: телекомунікаційні системи; антивірусний захист; обробка метаданих; хмарні антивірусні системи.

ISSN 2663 - 4023

1. ВСТУП

1.1 Постановка завдання дослідження

Останнім часом все більшою небезпекою є хакерські атаки, проведені за допомогою шкідливого програмного забезпечення (комп'ютерних вірусів). Саме цей вид комп'ютерної злочинності досягнув широкої популярності і використовується для реалізації різних загроз інформаційній безпеці.

Рівень забезпечення антивірусної безпеки є наслідком ефективності відповідних методів і засобів захисту даних. Для досягнення даної мети існує безліч різних підходів (сигнатурний, евристичний), методик (статична, динамічна і ін.) і технологій (стаціонарні, хмарні і ін.) аналізу. Розробляються і використовуються спеціальні методи безпечного кодування і керування трафіком ТКС. Однак, як показали дослідження, ряд істотних недоліків не дозволяє ефективно використовувати сучасні засоби антивірусного захисту даних у повному обсязі.

Виникає протиріччя між розширенням спектру злочинного програмного забезпечення, підвищенням рівня кіберзлочинності в ТКС, станом основних технологій антивірусного захисту, що існують і жорсткими вимогами до інформаційної безпеки.

Постановка проблеми. З метою підвищення ефективності використання засобів антивірусного захисту даних і мінімізації наслідків подібних кіберзлочинів, своєчасне виявлення і локалізація комп'ютерних вірусів є вкрай важливим і разом з тим складним завданням.

Аналіз останніх досліджень і публікацій. Дана проблема широко розглядається в роботах [1-4]. Однак, дані дослідження не повною мірою охоплюють технічні і технологічні можливості хмарних обчислювальних технологій, а також питання сполучення даних технологій з існуючими протоколами керування в ТКС.

Мета статті. У такий спосіб необхідно розробити метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих, який повинен містити в собі наступні складові:

1. Алгоритми формування множини маршрутів передачі метаданих.

1.1. Вибір алгоритму пошуку найкоротших шляхів між вузлами в ТКС.

1.2. Алгоритм формування базової множини маршрутів передачі метаданих.

1.3. Алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер.

2. Метод контролю ліній зв'язку телекомунікаційної системи.

3. Модель системи нейромережних експертів безпечної маршрутизації.

3.1. Система обробки і формування початкового стану маршрутів ТКС.

3.2. Розробка асоціативного блоку нейромережних експертів.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

2.1 Алгоритми формування множини маршрутів передачі метаданих

Аналіз процесу функціонування телекомунікаційної системи, а також дослідження процесів формування, передачі і обробки метаданих у хмарних антивірусних системах [5], дозволили визначити щільність розподілу ймовірностей часу передачі хеш-файлу метаданих у хмарні антивірусні системи, а також обробки і доставки команд передачі керування, сформувати і математично формалізувати знання про зміни і характер поводження основних ймовірнісно-тимчасових показників якості обслуговування в телекомунікаційній системі.

ISSN 2663 - 4023

Як було вказано в [6], обмін метаданими між програмним клієнтом і сервером, у загальному випадку, здійснюється через транзитні маршрутизатори, послідовність яких на шляху від відправника до одержувача визначимо як маршрут [7-16].

Нехай $\Re = \{V_n | \, n \in 1, N\}$ – множина маршрутизаторів у ТКС, V_n – n-й маршрутизатор, $N = |\Re|$ – кількість маршрутизаторів, $\Im = \{\theta_\xi \, | \, \xi \in 1, \Theta\}$ – множина каналів зв'язку в ТКС, де θ_ξ – ξ-й канал зв'язку, Θ – кількість каналів зв'язку в ТКС, $|Z|$ – потужність множини *Z*.

Інформаційні пакети метаданих для аналізу програмному серверу можуть бути передані по одному з маршрутів, що становлять множину $\aleph = \{ \eta_s \, | \, s \in 1, M \}$, де $\eta_s = \{ \theta_{s,c} \, | \, \theta_{s,c} \in \Im; \quad c \in 1, \Theta \}$ – s-*й* маршрут, $s \in 1, M$, $|\eta_s| = \Psi_s$, M – кількість маршрутів, $\theta_{s,c}$ – канал зв'язку з номером *c*, що належить s-*му* маршруту, Ψ_s – кількість каналів зв'язку на s-*му* маршруті.

Формування множини $\aleph$ маршрутів являє собою складний ітераційний процес, що складається в виконанні декількох алгоритмів:

– алгоритм пошуку найкоротших шляхів між вузлами в ТКС;

– алгоритм формування базової множини маршрутів передачі метаданих;

– алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер.

2.1.1 Вибір алгоритму пошуку найкоротших шляхів між вузлами в ТКС

Проведені дослідження показали, що рішення завдання пошуку найкоротших шляхів лежить у площині рішення загального завдання маршрутизації метаданих у хмарні антивірусні системи. Тому однією з необхідних умов для вибору базового алгоритму пошуку найкоротших шляхів є мінімізація обчислювальної складності, що багато в чому задається числом операцій порівняння.

Проведені дослідження і аналіз відомих алгоритмів пошуку найкоротших шляхів [7-10, 17-18] показали, що одним з найбільш оперативних алгоритмів, що відповідають заданим вимогам (*O(n2^n)*) є алгоритм D'Esopo-Pape.

Ефективність цього алгоритму підтверджується з однієї сторони результатами досліджень [18], а з іншої сторони результатами експериментів, проведених за допомогою імітаційної моделі.

Зовнішній вигляд інтерфейсу основного програмного компоненту (основного поля) імітаційної моделі наведено на рис. 1.

У ході моделювання виконувалися імітаційні процедури функціонування ТКС із різною топологією і кількістю вузлів $\overline{N}$ від 100 до 2000. Вага окремих ліній зв'язку відповідала можливій залишковій пропускній здатності реальних каналів зв'язку.

На рис. 2 наведено результати дослідження відомих алгоритмів пошуку найкоротших шляхів у вигляді графіків залежності кількості операцій порівняння від кількості вершин графа. Із графіків рис. 2 видно, що алгоритм D'Esopo-Pape має переваги в порівнянні з відомими алгоритмами Дейкстри і Беллмана-Форда [17].

Для підтвердження вірогідності отриманих результатів були проведені розрахунки, що відповідають умовам моделювання:

– ступінь зв’язності мережі вибиралася випадковим чином у рамках діапазону: від 5 до 10;

– кількість експериментів на кожному з етапів, що характеризується кількістю вузлів ТКС $\overline{\overline{N}} = 100$.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

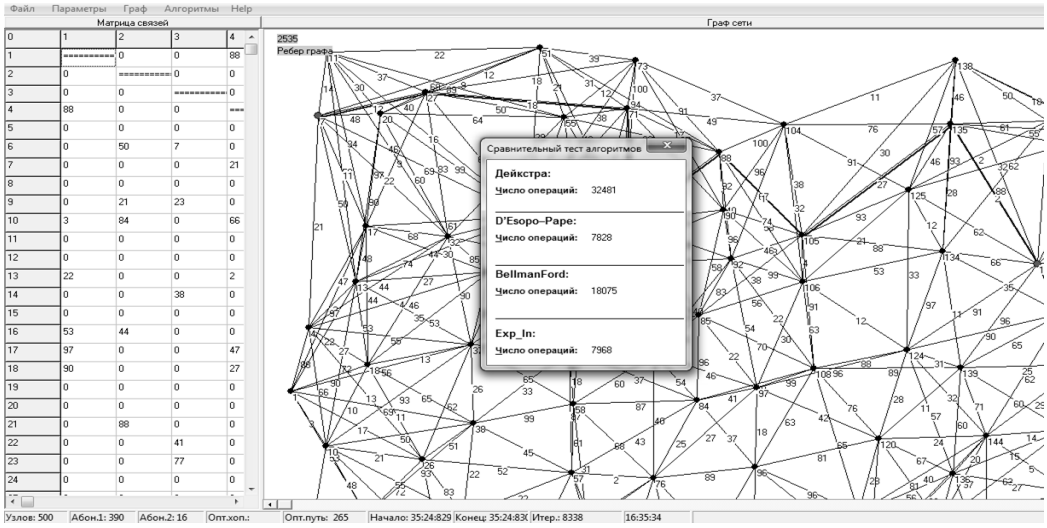

Рис. 1. Зовнішній вигляд інтерфейсу основного програмного компоненту імітаційної моделі ТКС

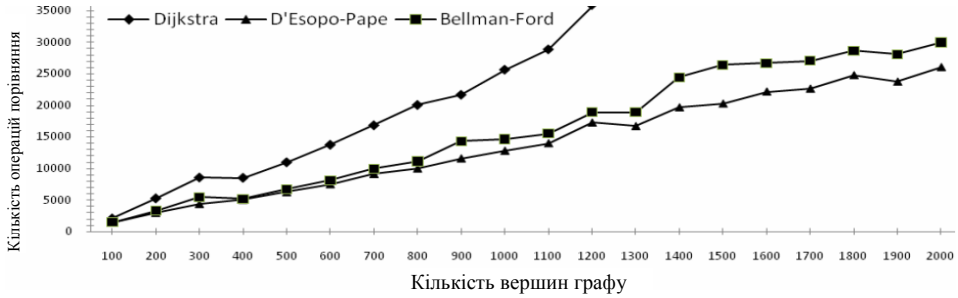

Рис. 2. Графіки залежності кількості операцій порівняння від кількості вершин графа для різних алгоритмів пошуку найкоротших шляхів

Висунута в статті гіпотеза про нормальний розподіл випадкової величини кількості операцій порівняння в алгоритмах була перевірена за критерієм згоди χ^2 Пірсона [19]:

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i ,$$

де k – кількість розрядів (інтервалів) статистичного ряду,

P_i^* і P_i – «статистична» і теоретична ймовірності «влучення» величини середньої кількості операцій порівняння в і-*й* розряд.

Проведена перевірка довела правдоподібність гіпотези про те, що величина кількості операцій порівняння розподілена за нормальним законом.

Отримано оцінки $w(\vec{\xi})^{(i)}$ математичного очікування і $\hat{D}_{w(\vec{\xi})^{(i)}}$ дисперсії ($\hat{\sigma}_{w(\vec{\xi})^{(i)}}$ середньоквадратичного відхилення) випадкової величини кількості операцій порівняння $w(\vec{\xi})^{(i)}$ [20]:

ISSN 2663 - 4023

$$\widehat{w}(\vec{\xi})^{(i)} = \frac{\sum_{i=1}^{k} \widehat{w}(\vec{\xi})^{(i)}}{\mathrm{N}^*}; \quad D_{w(\vec{\xi})^{(i)}} = \frac{\sum_{i=1}^{k} \left(w(\vec{\xi})^{(i)} - \widehat{w}(\vec{\xi})^{(i)}\right)^2}{N^* - 1}; \quad \widehat{\sigma}_{w(\vec{\xi})^{(i)}} = \sqrt{\widehat{D}_{w(\vec{\xi})^{(i)}}}.$$

Скориставшись відомим виразом для розрахунку довірчої ймовірності відхилення відносної частоти від постійної ймовірності в незалежних випробуваннях, отримане в результаті експерименту значення прогнозованої кількості операцій порівняння «не відхилиться» від математичного очікування $\widehat{w}(\vec{\xi})^{(i)}$ більш ніж на 1:

$$P\left(\left|\widehat{w}(\vec{\xi})^{(i)} - w(\vec{\xi})^{(i)}\right| < 1\right) = 2\Phi(1/\widehat{w}(\vec{\xi})^{(i)}),$$

де Ф – функція Лапласа вигляду $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt$ [5], [32].

Проведене імітаційне моделювання показало, що для всіх досліджуваних видів даних довірча ймовірність того, що значення статистичної величини $w(\vec{\xi})$ «не відхилиться» від математичного очікування $w(\vec{\xi})$ більш ніж на 1 дорівнює: $P \approx 0{,}98$.

Високий ступінь збігу результатів імітаційного моделювання підтверджують вірогідність результатів аналізу алгоритмів пошуку найкоротших шляхів.

Таким чином, можна відзначити доцільність використання алгоритму D'Esopo-*Pape* у якості базового при пошуку найкоротших шляхів між вузлами в ТКС.

2.1.2 Алгоритм формування базової множини маршрутів передачі метаданих

Для знаходження множини маршрутів, що виключають «петлі», у розглянутому алгоритмі використовуються процедури, наведені на рис. 3.

Нехай програмний клієнт хмарної антивірусної системи інстальований на деякому вузлі i, щодо якого існують множини:

- $U = \{u_\alpha \mid \aleph(u_\alpha) \subset \aleph\}$ – рівнів ієрархії на дереві припустимих маршрутів;
- $\aleph_{баз} = \bigcup_{u_\alpha=1}^{|U|} \aleph(u_\alpha)$ – шуканих шляхів передачі метаданих;
- $\aleph_{вб} \subset \aleph_{баз}$ – множина маршрутів передачі метаданих, обраних з множини $\aleph_{баз}$ для підвищення безпеки,

де u_α – номер рівня ієрархії.

Висунуті припущення, а також основні процедури розглянутого алгоритму формування базової множини маршрутів передачі метаданих дозволяють сформулювати оптимізаційне завдання підвищення оперативності передачі метаданих у межах множини маршрутів $\aleph_{вб}$:

$$T_{mc}(\aleph_{вб}) \to min; \quad (1)$$

$$|U| = \{u_\alpha \mid \aleph(u_\alpha) \subset \aleph\}; \quad (2)$$

$$\aleph_{баз} = \bigcup_{u_\alpha=1}^{|U|} \aleph(u_\alpha), \; |U| \geq 1, \; |U| < \max_{\eta_m \in \aleph} |\eta_m|; \quad (3)$$

$$\aleph_{вб} = \bigcup_{u_\alpha=1}^{|U|} \aleph_{баз}(u_\alpha); \quad (4)$$

ISSN 2663 - 4023

$$P_{без} \geq P_{без_{доп}} . \quad (5)$$

де $P_{без_{доп}}$ – припустима ймовірність безпечної передачі даних.

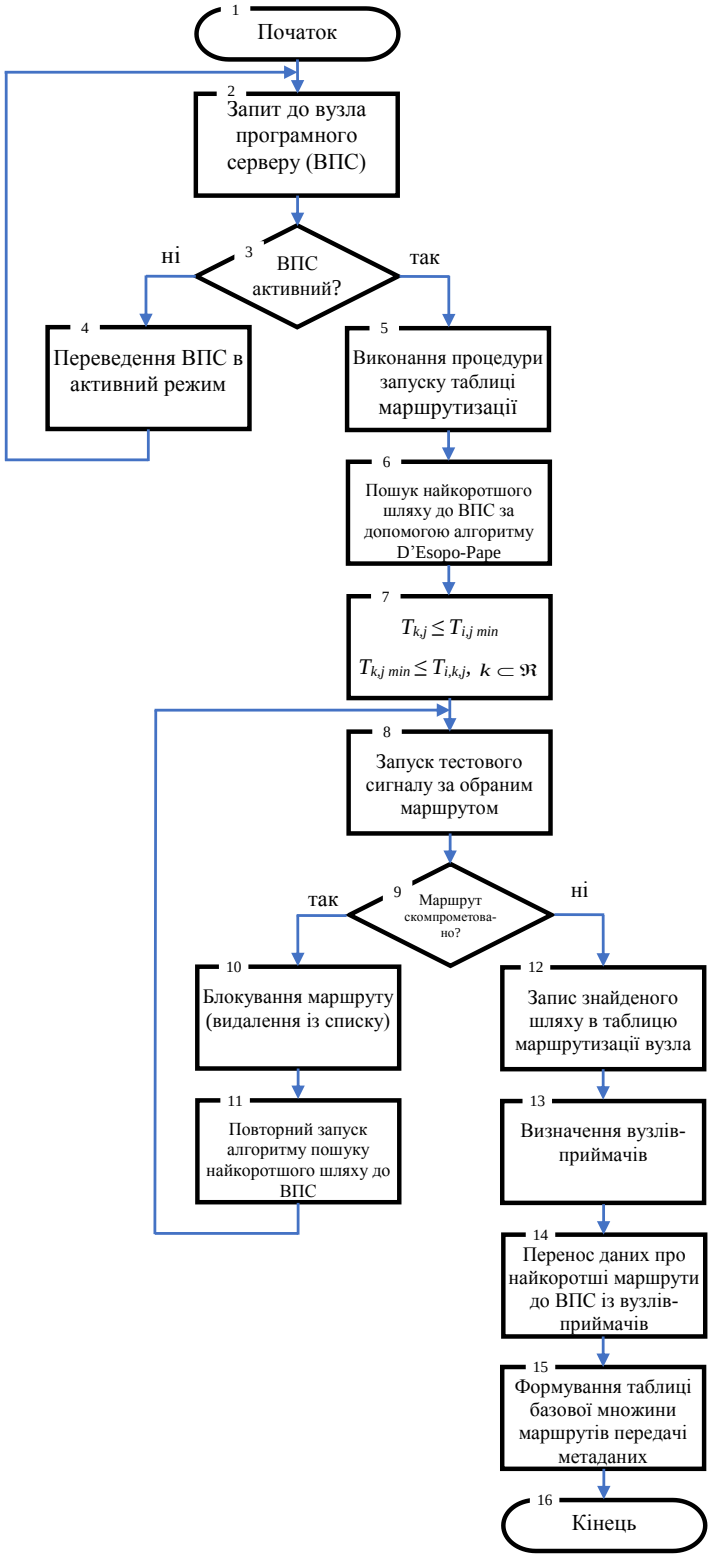

Рис.3 Структурна схема алгоритму формування базової множини маршрутів передачі метаданих

У тому випадку, якщо не знайдено жодного розподілу з множини $\aleph_{вб}$, що задовольняє обмеженню (5), необхідно розширити $\aleph_{вб}$ шляхом його об'єднання з множиною маршрутів наступного рівня ієрархії відповідно до (1) – (4).

Варто відмітити, що при рішенні поставленого завдання формування базової $\aleph_{баз}$ множини маршрутів передачі метаданих відомими алгоритмами пошуку найкоротших шляхів [17] у більшості практичних випадків доводиться зіштовхуватися із проблемою «зациклення» даних у знайдених шляхах («петель»). Це призводить до збільшення часу передачі інформаційних пакетів, а найчастіше і їхній втраті.

Уникнути «петель» можна ввівши обмеження (умова постійної відсутності «петель»), що наведені у вигляді виразів:

$$T_{k,j} \le T_{i,j\,\min}; \tag{6}$$

$$T_{k,j\,\min} \le T_{i,k,j},\ k \subset \Re, \tag{7}$$

де $T_{k,j\,\min}$ – найкоротша «відстань» (мінімальний час передачі інформаційних пакетів) від вузла *k* до адресата *j*; $T_{i,k,j}$ – «відстань» (час передачі інформаційних пакетів) від вузла *i* до адресата *j* через вузол *k*.

Ця умова перевіряється на кроці 7 розглянутого алгоритму.

На відміну від відомих алгоритмів [17], які не враховують можливість компрометації (у результаті кібератаки) маршрутів, у розробленому алгоритмі цей фактор врахований (кроки 7-11). Основні процедури формування і перевірки тестового сигналу, що посилається в лінію зв'язку, розглянуті в підрозділі 2.

Після того як сформована базова $\aleph_{баз}$ множина маршрутів передачі метаданих необхідно проводити постійний моніторинг каналів зв'язку і адаптивно змінювати таблиці базової множини маршрутів у випадку аномальних змін у показниках тестових сигналів. Для рішення цього завдання призначений алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер.

2.1.3 Алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер

Безпосереднє використання всієї знайденої множини $\aleph_{баз}$ шляхів передачі метаданих алгоритмом, що запропонований у попередньому підрозділі, не завжди можливо і виправдано. Це стає особливо очевидно у випадку високої пропускної здатності хоча б декількох з наявних каналів зв'язку, що здатні забезпечити виконання вимог при передачі метаданих у вузли програмного сервера. Розширення такої множини призводить до збільшення таблиць маршрутизації вузлів зв'язку, ускладненню процесу розподілу даних і, як наслідок, до зниження вірогідності передачі і інформаційної безпеки. Тому виникає необхідність у знаходженні такої множини маршрутів, використання якої в умовах обмежень, що накладаються, дозволить забезпечити максимально можливу інформаційну безпеку, тобто в моніторингу каналів зв'язку і виборі із всієї знайденої множини $\aleph_{баз}$ шляхів якоїсь (оптимальної) сукупності $\aleph_{вб}$ маршрутів.

Сучасні вимоги до якості наданих послуг у ТКС задаються в параметричному вигляді, системою обмежень:

$$\left\{P_{иск} \le P_{иск_{доп}},\ Q_c \ge Q_{доп},\ T \le T_{доп}, P_{без} \ge P_{без_{доп}}\right\},$$

ISSN 2663 - 4023

де $P_{иск_{доп}}$ – припустима ймовірність перекручування інформаційних пакетів у процесі передачі; $Q_{доп}$ – припустима ймовірність приймання інформаційного пакету за час T, що не перевищує припустимий.

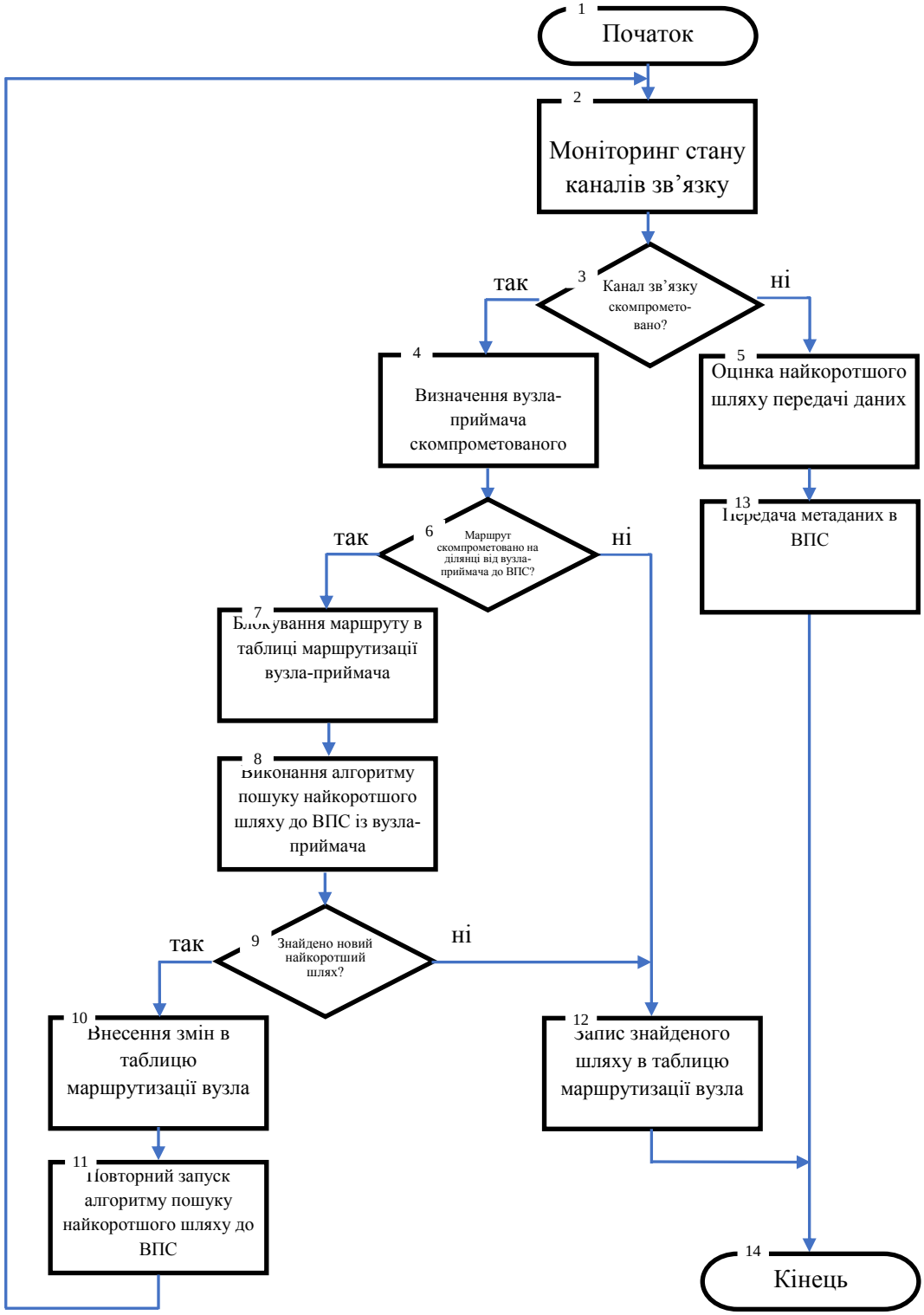

Рис. 4. Структурна схема алгоритму безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер

У той же час, в умовах підвищеної кібербезпеки при передачі і обробці метаданих у хмарних антивірусних системах, імовірність $P_{без}$ безпечної передачі даних є одним з визначальних показників. При цьому, завдання безпечної маршрутизації даних трансформується в приватне оптимізаційне завдання вигляду:

$$\left\{P_{без} \to max, \quad при \quad P_{иск} \le P_{иск_{доп}},\ T \le T_{доп},\ Q_c \ge Q_{доп}\right\}. \qquad (8)$$

У таких умовах алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер можна зобразити у вигляді рис. 4.

Характерною рисою алгоритму є можливість постійного моніторингу і обліку характеристик каналів зв'язку ТКС на маршрутах у вузол програмного сервера (кроки 2-7).

Саме тому одним із основних завдань безпечної маршрутизації є визначення і облік характеристичних параметрів ліній зв'язку, що визначають можливість кібератаки і несанкціонованого доступу в ТКС.

2.2 Розробка й дослідження методу контролю ліній зв'язку телекомунікаційної системи

Дослідження процесу обслуговування інформаційних пакетів метаданих у багатопротокольному маршрутизаторі ТКС показали, що основними його елементами, що впливають на ймовірнісно-тимчасові показники якості обслуговування є: комутатор, депакетизатор, блок керування маршрутизатором, запам'ятовуючий пристрій (буфер пам'яті) і аналізатор ліній зв'язку (див. рис. 5.) [20].

Відмінною рисою даного маршрутизатора є включення до його складу аналізатору ліній зв'язку і асоціативного блоку нейромережних експертів, побудованого на основі нейронної мережі АРТ-1. Зазначені блоки виконують завдання моніторингу каналу зв'язку і керування процесом маршрутизації в умовах можливих злочинних підключень.

У запропонованому алгоритмі безпечної маршрутизації такі блоки передбачається використовувати в кожному вузлі зв'язку (ВЗ) телекомунікаційної системи. Для того щоб маршрутизатор міг функціонувати, необхідно сформувати інформацію про стан з'єднань, що виходять із даного вузла.

Кожному з'єднанню привласнюється певний вектор параметрів, компоненти якого характеризують певну складову фізичного з'єднання.

Одними з найважливіших параметрів, які необхідно враховувати при виборі подальшого шляху маршрутизації інформації, є тип каналу зв'язку, його пропускна спроможність і функціональна безпека.

Для деяких каналів зв'язку характеристики, що використовуються для вибору маршрутів при передачі метаданих у хмарні антивірусні системи, наведені в табл. 1 [21]. Параметри пропускної спроможності і функціональної безпеки набувають значень в інтервалі від 0 до 1, які характеризують тип каналу і кабелю зв'язку в порівнянні з параметрами, обраними в якості еталонних і які мають максимальне значення пропускної спроможності і функціональної безпеки.

Формування навчальної вибірки для системи експертів відбувається шляхом аналізу лінії зв'язку, що використовуються в розглянутій локальній мережі. Вторгнення може бути здійснене шляхом прямого приєднання до каналу зв'язку і зчитуванні інформації за допомогою технічних засобів. Внаслідок цього повинна бути можливість визначення спроб підключення до каналу.

Варто помітити, що основна небезпека подібного роду злочинних вторгнень доводиться на неконтрольовані ділянки ТКС, тобто ділянки глобальних і регіональних мереж, у яких найчастіше використовуються канали типу Е-1 і Е-2.

Проведені дослідження показали, що в цей час, незважаючи на високу вартість і складність, існує принципова можливість приєднання до волоконно-оптичної лінії зв'язку (ВОЛЗ) і несанкціонованого доступу до даних, що передаються зазначеними каналами зв'язку. Способи несанкціонованого доступу можна класифікувати за двома групами (див. рис. 6).

ISSN 2663 - 4023

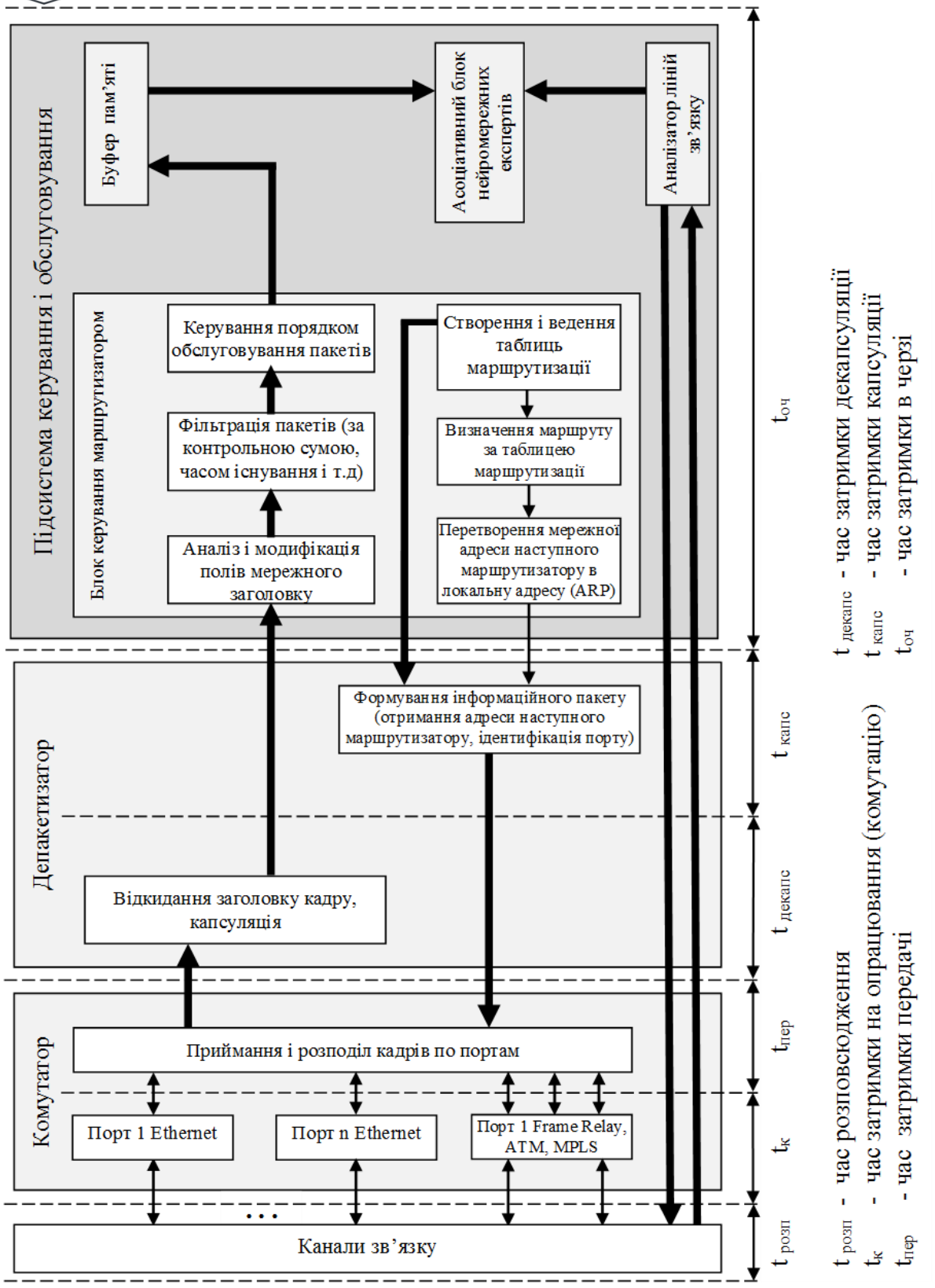

Рис. 5. Структурна схема багатопротокольного маршрутизатору

Таблиця 1

Характеристики, що використовуються для вибору маршрутів при передачі метаданих у хмарні антивірусні системи

Аналізована характеристика				
Пропускна спроможність			Функціональна безпека	
Тип каналу	Швидкість передачі	Параметр пропускної спроможності	Тип кабелю	Параметр функціональної безпеки
Ethernet	10 Мбіт/с	0,8	Коаксіальний кабель	
Ethernet	100 Мбіт/с	0,9	«Товстий» коак. кабель	0,31
Ethernet	1000 Мбіт/с	0,95	«Тонкий» коак. кабель	0,22
Канал Т-1	1,544 Мбіт/с	0,45	Телевізійний кабель	0,15
Канал Т -2	6,312 Мбіт/с	0,61	Кручена пара	
Канал Т-3	44,736 Мбіт/с	0,85	Екранована	0,6
Канал Т-4	274 Мбіт/с	0,93	Неекранована	0,5
Канал 56	56 Гбіт/с	0,33	Волоконно-оптичний	
Канал Е-2	8,488 Гбіт/с	0,65	Багатомодовий	0,8
Канал Е-1	2,048 Тбіт/с	0,55	Одномодовий	1,0

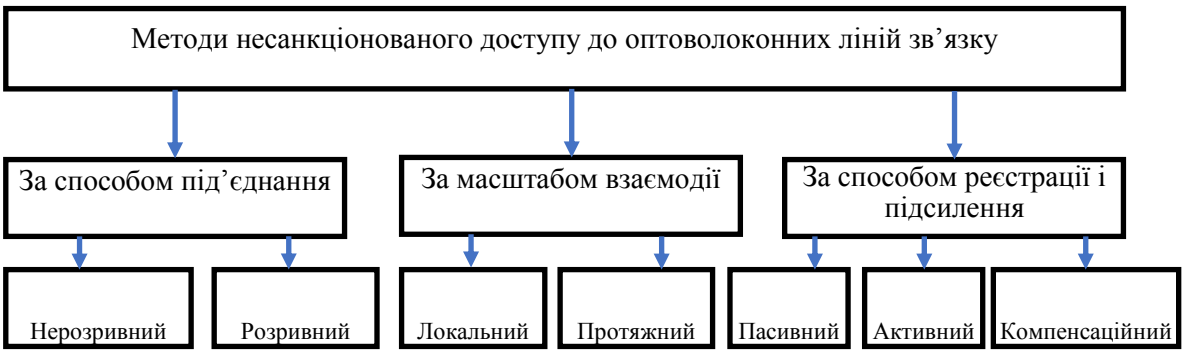

Рис. 6. Способи несанкціонованого доступу до ВОЛЗ

Найнебезпечнішими, з погляду знімання метаданих, що передаються на програмні сервери (аналізатори метаданих) є розривні способи несанкціонованого доступу. Використовуючи даний спосіб, зловмисник має широкий спектр можливих впливів на хмарну антивірусну систему в цілому, починаючи від простого перехоплення, закінчуючи підміною метаданих. Пристрої розривного несанкціонованого доступу дозволяють здійснювати більш надійне знімання даних. Але розривне підключення вимагає тимчасового відключення ліній зв'язку, що може провокувати сигналізацію про наявність злочинного вторгнення (незважаючи на можливі спроби зловмисників маскування такої атаки).

Більш непомітним за можливим виявленням, звичайно, є безрозривний спосіб приєднання. У цьому способі для знімання сигналу використовується випромінювання, що виникає природно в результаті розсіювання світла на муфтах, з'єднувачах, пристроях введення і виведення оптичної потужності, самому оптичному волокні. При цьому можливо використання пасивних, активних і компенсаційних способів реєстрації даних.

Пасивні способи мають високу скритність, тому що практично не змінюють параметрів поширення випромінюваного сигналу у ВОЛЗ. Однак цей спосіб має недоліки, пов'язані з низькою чутливістю. Тому для перехоплення метаданих зловмисники можуть використовувати ділянки, на яких рівень бічного випромінювання

підвищений. Навіть після формування стаціонарного розподілу поля у волокні невелика частина розсіяного випромінювання все-таки проникає за межі оболонки й може бути каналом витоку переданих метаданих.

Можливі причини випромінювання і розсіювання у ВОЛЗ і, відповідно, атак несанкціонованого доступу до ВОЛЗ наведені на рис. 7.

Як показали дослідження, активні способи дозволяють отримати сигнал більшої потужності і, відповідно підвищити ефективність атаки несанкціонованого доступу до ВОЛЗ. Однак при цьому відбувається зміна параметрів (потужності) сигналу, який поширюється по ВОЛЗ, що також полегшує можливість виявлення атаки.

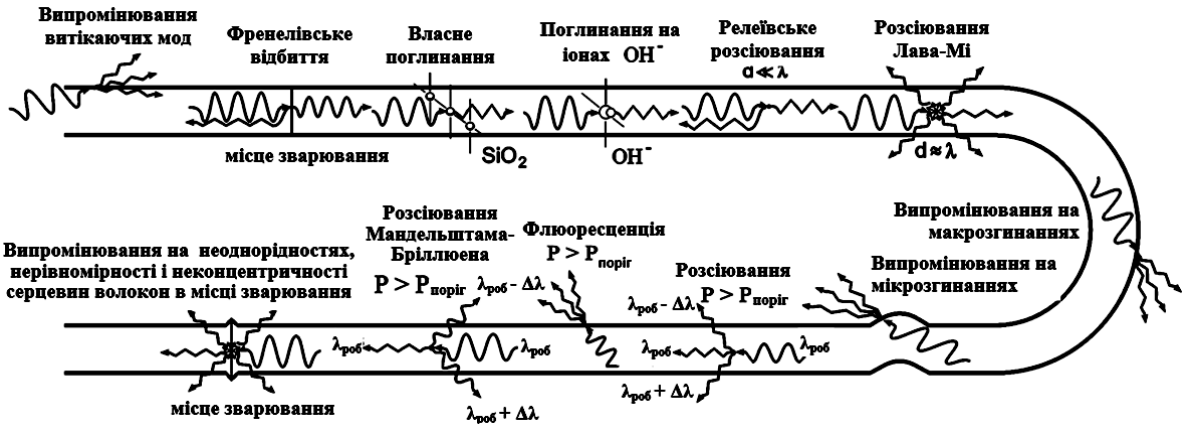

Рис. 7. Причини несанкціонованого доступу до ВОЛЗ

Аналіз способів знімання даних з ВОЛЗ показав, що для виконання даної операції на фізичному рівні будь-якої ділянки, можна використовувати локальний вплив на його волоконні світловоди. При такому впливі змінюються їхні оптичні властивості, що й призводить до «витікання» сигналу. Методів впливу на волокно можна перелічити декілька:

- згинання волокна;
- зміна діаметру волокна (наприклад, шляхом тиску)
- мікрозгинання волокна;
- акустичний вплив на волокно;
- вплив хімічними реактивами.

Проведені дослідження показали, що із цих методів одним з найбільш ефективних для зловмисників є метод згинання волокна (дозволяє організувати спрямоване виведення випромінювання). Змінюючи радіус згинання волокна, зловмисник може досягнути зняття таких величин оптичної потужності, яких йому буде цілком достатньо для перехоплення метаданих.

Однак, варто відмітити, абсолютно непомітним цей метод не є. Оскільки потужність відводиться примусово, то підключення викликає зниження рівня потужності на прийомній стороні лінії. Тому основним методом виявлення цього способу несанкціонованого доступу є контроль над рівнем потужності на прийомній стороні. Якщо пристрій контролю виявляє її зниження, то він робить висновок про наявність несанкціонованого доступу до ВОЛЗ і може ухвалити рішення щодо перенаправлення метаданих на програмні сервери за іншим маршрутом.

Проведені дослідження показали, що апаратура, розташована на стороні програмного сервера контролю і аналізу метаданих у хмарних антивірусних системах,

ISSN 2663 - 4023

крім основних своїх функцій повинна містити в собі систему контролю і виявлення несанкціонованого доступу. До завдань цієї системи повинні входити: спостереження за станом ВОЛЗ, контроль прийнятого сигналу і передача його в інтелектуальний асоціативний блок нейромережних рішень, у якому і приймається рішення про наявність несанкціонованого доступу до ВОЛЗ.

Аналіз літератури [22] показав, що основними показниками ефективності, що використовуються при рішенні поставлених завдань є:

- імовірність виявлення – $P_{вияв}$;
- імовірність помилкового спрацьовування – P_n;
- обсяг інформації, що перехоплюється порушником – k (біт).

Якщо значення цих показників лежать у рамках припустимих порогів, то дана система є ефективною.

Проведемо аналіз функціонування розглянутої телекомунікаційної системи хмарного антивірусного захисту і з'ясуємо фактори, що впливають на її ефективність.

Позначимо через s_0 стан ВОЛЗ під час відсутності несанкціонованого доступу, а через s_1 – стан ВОЛЗ при даному злочинному впливі. Завданням аналізатора ліній зв'язку (див. рис. 5) є визначення моменту зміни стану ВОЛЗ.

З роботи [21] відомо, що сигнал, який надходить на вхід приймача хмарної антивірусної системи, являє собою послідовність біт, відображених у вигляді імпульсів світла. Параметрами цих імпульсів є їхня тривалість, рівень оптичної потужності, а також функція розподілу цієї потужності. Підключення до лінії зовнішніх несанкціонованих пристроїв, викликає зміни в цих параметрах. Прийнята оптична потужність знизиться, відповідно, зміниться і її розподіл.

Апаратура детектування в приймачі хмарної антивірусної системи працює з досить потужними оптичними сигналами, і тому співвідношення «сигнал/шум» для неї буде більшим. Емпірично, у тестовому режимі нескладно провести аналіз його роботи в умовах обміну метаданими і команд передачі керування програмному клієнтові, і знайти залежність між зміною прийнятої оптичної потужності і імовірностями виявлення і помилкового спрацьовування.

Варто помітити, що системи аналізу (аналізатори) переданого сигналу є одними із простих діагностичних систем. На прийомній стороні (серверної частини) хмарного антивірусу аналізується минулий сигнал. У випадку проведення кібератаки (несанкціонованого доступу) відбувається фіксація змін потужності сигналу.

Одним з основних недоліків подібного роду систем є відсутність даних про координату (часової характеристики) аномалії, що з'явилася. Це підвищує ймовірність помилкових спрацьовувань у системі. На рис. 8 наочно ілюструється дана ситуація.

З появою аномалії оптична потужність знижується, і математичне очікування величини Z стає рівним $\lambda_1^{(y)}$, а її дисперсія – $\frac{\sigma_1 y^2}{N}$.

Як видно із графіка рис. 8, поряд із правильним виявленням злочинних вторгнень у лінії зв'язку, використання одного аналізатора без додаткових «інтелектуальних» засобів виявлення допускає ситуацію помилкового виявлення або пропуску аномалій. Це може відбутися, якщо рівень потужності сигналу стане менше (або більше) порогового значення γ під впливом будь-яких об'єктивних факторів (наприклад, старіння устаткування).

ISSN 2663 - 4023

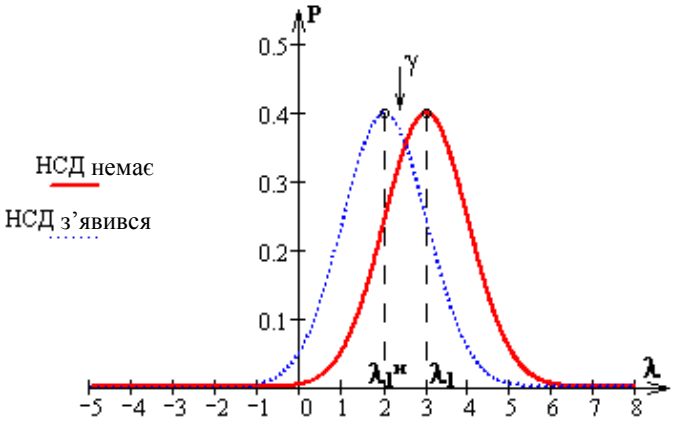

Рис. 8. Графік розподілу ймовірності для оптичної потужності на легальному приймачі при наявності і відсутності аномалії

У роботі [23] для розрахунку ймовірностей помилкового виявлення або пропуску аномалій пропонується використовувати вираз:

$$P_{ло} = \frac{1}{\sqrt{2\pi}\,\frac{\sigma_1}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1)^2}{2\sigma_1^2/N}}\, dz\,, \tag{9}$$

$$P_{прол} = \frac{1}{\sqrt{2\pi}\,\frac{\sigma_1^{н}}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1^{н})^2}{2(\sigma_1^{н})^2/N}}\, dz\,, \tag{10}$$

де $\lambda_1^{н}$ і $\left(\sigma_1^{н}\right)^2$ – математичне очікування і дисперсія випадкових величин y_i при наявності несанкціонованого доступу.

Для усунення зазначеного недоліку розіб'ємо передані дані на безліч ділянок однакової тривалості N біт. При цьому досліджуємо величину y_i – параметр рівня сигналу в і-*й* момент часу.

Нехай дана випадкова характеристика відповідає нормальному закону розподілу:

$$P(y_i) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{\frac{-(y-\lambda_i)^2}{2\sigma_i}}\,, \tag{11}$$

де λ_i, σ_i – математичне очікування і дисперсія випадкової величини y_i відповідно.

Суму величин y_i, обумовлених в аналізаторі ліній зв'язку для всіх y_i, що відповідають позитивним імпульсам, позначимо як Z і зрівняємо з порогом γ:

$$Z = \frac{1}{N}\sum_{j=1}^{N} y_j\,, \tag{12}$$

де N – інтервал аналізу.

За результатами такого порівняння в системі нейромережевих експертів приймається рішення про наявність несанкціонованого доступу. Якщо атака не виявляється, то цей процес повторюється для наступного інтервалу N.

Statechart-діаграма, що ілюструє даний процес, наведена на рис. 9. На цій діаграмі визначається стан аналізатора ВОЛЗ у процесі передачі метаданих.

З діаграми видно, що послідовність біт даних, які передаються, розбивається на ділянки однакової тривалості N біт $(N_1 \ldots N_5)$. У деякий момент часу (стан 2) проходить атака несанкціонованого доступу до ВОЛЗ. Цей момент доводиться на деякий біт ділянки N_2. Система повинна прийняти рішення, що починаючи із цього біта, всі інші себе скомпрометували (змінили параметри). Врахування цього факту дозволяє на ділянці N_5, що віддалена від ділянки N_2 у загальному випадку на T ділянок, аналізатору виявити аномалію в прийнятому сигналі.

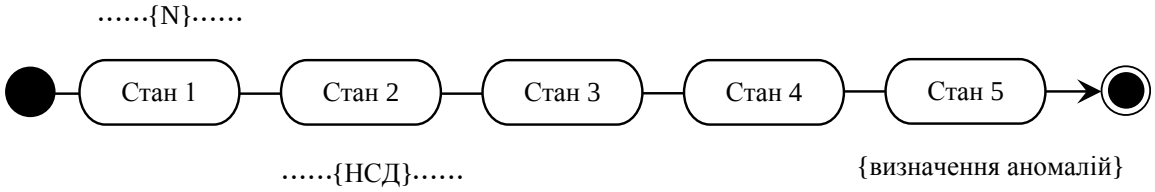

Рис. 9. Statechart-діаграма, що ілюструє процес виявлення аномалій під час передачі метаданих

Нехай x – кількість біт, переданих у ВОЛЗ після проведеної кібератаки («скомпрометованих») на інтервалі N_2. Тоді загальна кількість «скомпрометованих» біт даних буде дорівнювати:

$$X_i = x_i + N \cdot T + T_{pa}, \qquad (13)$$

де T_{pa} – час, поширення даних про сигнал аномалій.

Дані про число скомпрометованих біт необхідно використовувати при перерахуванні кількості метаданих, що перенаправляються за новим нескомпрометованим маршрутом.

Таким чином, розроблено метод контролю ліній зв'язку ТКС, що відрізняється від відомих введенням процедури врахування «скомпрометованих» біт даних спеціальних сигнатур, переданих у хмарні антивірусні системи.

Використання даного методу дозволить виявляти зміну характеристик ВОЛЗ у процесі функціонування ТКС, (отримати необхідні дані для початку процедури навчання нейронних експертів) і видавати необхідні сигнали аномалій (можливих кібератак) у лініях зв'язку в систему нейромережних експертів безпечної маршрутизації. Це дозволить знизити ймовірність маніпуляцій метаданими, переданими у вузли програмного сервера.

2.3 Розробка моделі системи нейромережних експертів безпечної маршрутизації

Проведені дослідження показали, що при рішенні складних завдань може виникнути ситуація, коли спроби отримати прийнятне рішення або необхідну якість апроксимуючої залежності, навіть при використанні різних алгоритмів, що паралельно обробляють і вирішують те саме завдання, не дають результатів [24], [25]. У цьому випадку об'єднання декількох алгоритмів у композицію дозволяє вирішити поставлене завдання.

При рішенні завдань за допомогою нейромережних методів, побудованих на застосуванні декількох нейронних мереж – ансамблів, вхідні дані обробляються за

допомогою множини (системи) нейромережних експертів – сукупності нейронних мереж різної архітектури з механізмом об'єднання рішень.

Загальна структура розробленої системи нейромережних експертів безпечної маршрутизації представлена на рис. 10.

Для нормального функціонування системи нейромережнх експертів безпечної маршрутизації необхідно підготувати і систематизувати дані, на основі яких відбувається навчання його окремих нейромережних компонентів. Для рішення цього завдання блок формування навчальної і тестової вибірки формує дані для навчання нейронної мережі, упорядковує і організовує з метою забезпечення можливості їхньої подальшої обробки за допомогою нейромережних технологій.

Цей етап роботи алгоритму є одним з найбільш важливих, тому що дозволяє реалізувати в сукупності нейронних мереж здатність до узагальнення. Вхідні дані, необхідні для виконання своїх функцій даним блоком, і спосіб їхнього отримання для формування навчальної і тестової множини асоціативної машини формуються відповідно до принципів, наведених в розділі статті 2.2.

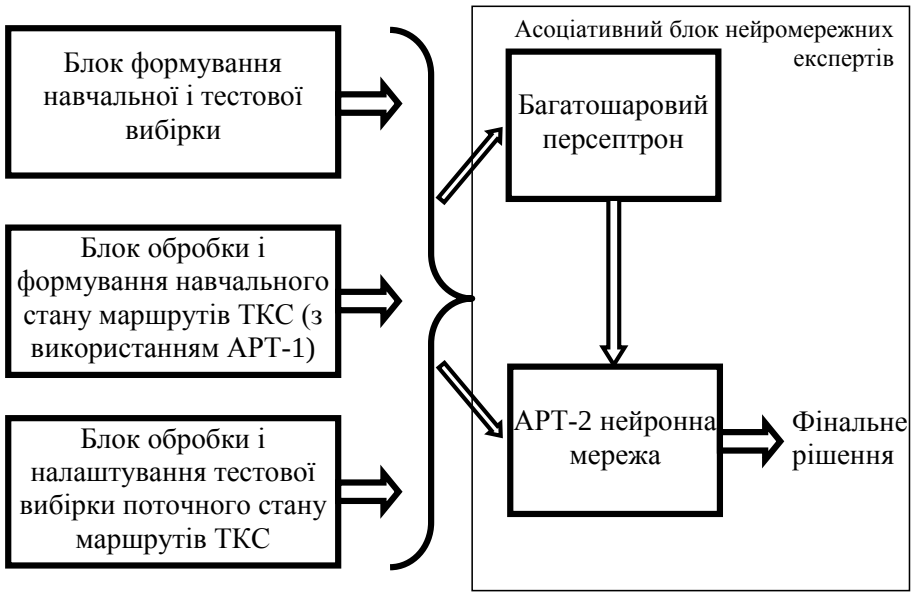

Рис. 10. Загальна структура системи нейромережних експертів безпечної маршрутизації

Блок обробки і формування початкового стану маршрутів ТКС формує значення параметрів всієї системи перед початком її навчання. Якщо змінні навчальної системи, які налаштовуються, ініціалізувати таким чином, щоб вони були наближені до оптимальних значень, то процедура навчання буде зведена до «підлаштування» моделі. Синтез оптимального алгоритму ініціалізації значно скоротить час навчання нейромережних експертів.

Проведений аналіз літератури [25, 26] показав, що для рішення цього завдання доцільно скористатися результатами роботи [27], де як алгоритм початкового встановлення параметрів був запропонований кооперативний імунний алгоритм із генерацією рішень на основі процедури генетичного пошуку з використанням нейронної мережі АРТ-1.

Оскільки нейронні мережі типу АРТ відносяться до класів мереж, що володіють властивостями пластичності і стабільності, то в загальну структуру блоку нейромережних експертів доцільно включити блок обробки і настроювання тестової вибірки поточного стану маршрутів ТКС, що виконує адаптацію компонентів нейронної мережі для рішення поставленого завдання. У статті процедура навчання здійснювалася для всіх нейронних мереж за алгоритмами, адаптованими до їх архітектур.

2.3.1 Система обробки і формування початкового стану маршрутів ТКС

Для нормального функціонування блоку нейромережних експертів необхідно сформувати їхні початкові стани, що виражені попередньою установкою вагових коефіцієнтів нейронних мереж. У зв'язку із цим необхідно використовувати принципи оптимізації на основі кооперативної коеволюції з декількома популяціями [27], що враховують спільне функціонування нейронних мереж. Як було зазначено раніше для рішення поставленого завдання доцільно використовувати імунний алгоритм оптимізації, побудований на основі принципів імунітету живих організмів, запропонований у роботі [27].

Передбачувана вага нейронних мереж кодується в антитілах, що утворюють популяцію. Як антиген розглядається завдання ініціалізації початкового стану експертів.

Як популяція антигенів виступає область всіх можливих значень векторів ваги і порогів нейронів. Кожне антитіло кодує вектори вагових коефіцієнтів і пороги нейронів. Приклад можливого кодування показаний на рис. 11.

Під кодування кожного параметру вагового коефіцієнту виділяється 20 біт даних. Антитіло має розрядність кратну 20 бітам і в ньому закодовані всі вагові коефіцієнти нейромережного експерту. У нейронну мережу послідовно підставляються параметри, закодовані в кожному з антитіл популяції. Обчислюється помилка навчання для кожного антитіла.

При обміні антитілами з популяцій видаляється частина антитіл, також це відбувається і після застосування оператора мутації, тому що для одержання правильного кубу з антитіл необхідно виконувати їхнє клонування для одержання потрібної кількості. Просте видалення гірших антитіл може призвести до видалення певної частини даних, що приводить до неефективного функціонування алгоритму навчання і збільшенню часу на пошук оптимального рішення. Для того щоб зберегти інформацію, накопичену в антитілах, був використаний адаптивний метод кластеризації за структурою, який заснований на застосуванні нейронної мережі АРТ-1 [26, 27].

Мережа навчається без вчителя і реалізує простий алгоритм кластеризації. Відповідно до цього алгоритму перше антитіло вважається зразком першого кластера. Наступне антитіло порівнюється зі зразком першого кластера. Антитіло належить першому кластеру, якщо відстань до зразка першого кластера менше порогу. Інакше, друге антитіло – зразок другого кластера. Цей процес повторюється для всіх наступних антитіл. Після того, як вся популяція антитіл буде розбита на кластери, обчислюється середня аффінність кожного кластеру. Антитіла спочатку віддаляються їхнього гіршого кластеру і далі із всіх кластерів один по одному в порядку аффінності. Це дозволяє зберегти різноманітну структуру антитіл [27].

У результаті, для кожного нейромережного експерту створюється окремий комплекс популяцій антитіл, усередині кожної популяції відбувається розвиток антитіл, мутація і видалення. Після зміни рішень імунними операторами відбувається запуск механізму міграцій. При перевірці експерту відбувається видалення тих антитіл з популяції, які не задовольняють критеріям функціонування нейромережної асоціативної машини. Навіть якщо в антитілі закодоване

краще рішення для конкретного експерту, а на рівні асоціативної машини воно показало незадовільний результат, то воно буде вилучене [27].

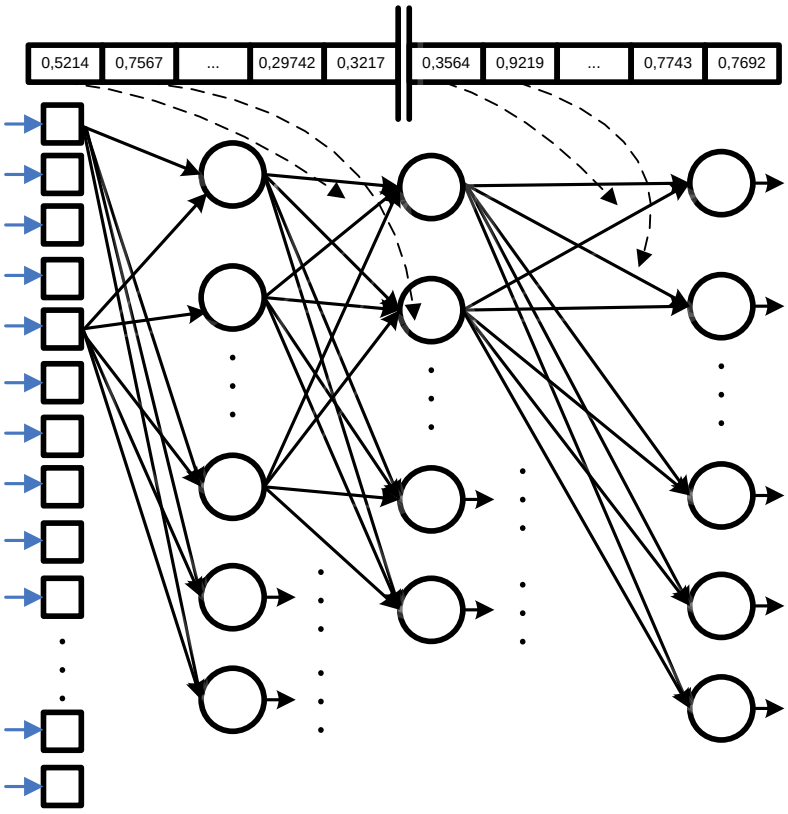

Рис. 11. Приклад можливого кодування при настроюванні нейронної мережі

2.3.2 Розробка асоціативного блоку нейромережних експертів

Аналіз літератури, а також проведені дослідження показали можливості використання моделі АР-2 Гроссберга-Карпентера для рішення завдань класифікації, кластеризації і розпізнавання аномального стану ліній зв'язку ТКС, тому що ця модель поєднує в собі властивості пластичності і стабільності, а також не вимагає достатньо більших апріорних знань.

Однак, ця модель має і істотні недолік. Вона припускає використання всього одного шару нейронів (не вважаючи вхідного, асоційованого із сенсорами). Це призводить до того, що нейронна мережа працює тільки з метрикою первинних ознак і обчислює відстань між образами, використовуючи зазвичай евклідову відстань.

Даний факт, в умовах наявних розходжень у поточних метриках характеристик ліній зв'язку ТКС, може призвести до значних неточностей при визначенні аномалій на маршрутах передачі метаданих у хмарних антивірусних системах.

Тому в статті для підвищення точності і забезпечення інваріантності визначення аномалій у лініях зв'язку пропонується використовувати багатошарові персептрони, що формують на проміжних шарах у процесі навчання побічні ознаки.

Можна відзначити, що в персептронах кожний шар забезпечує перетворення однієї метрики образів в іншу. У такій комбінованій моделі перші кілька шарів нейронів організовані як персептрон прямого поширення, виходи якого є входами моделі АР-2. Персептрон забезпечує перетворення метрики первинних ознак у метрику побічних ознак у просторі значно меншої розмірності. Нейронна мережа АР-2 розпізнає відхилення в характеристиках ліній зв'язку за побічними ознаками.

ISSN 2663 - 4023

Функціонування запропонованої в статті моделі описується алгоритмом, структурна схема якого наведена на рис. 12.

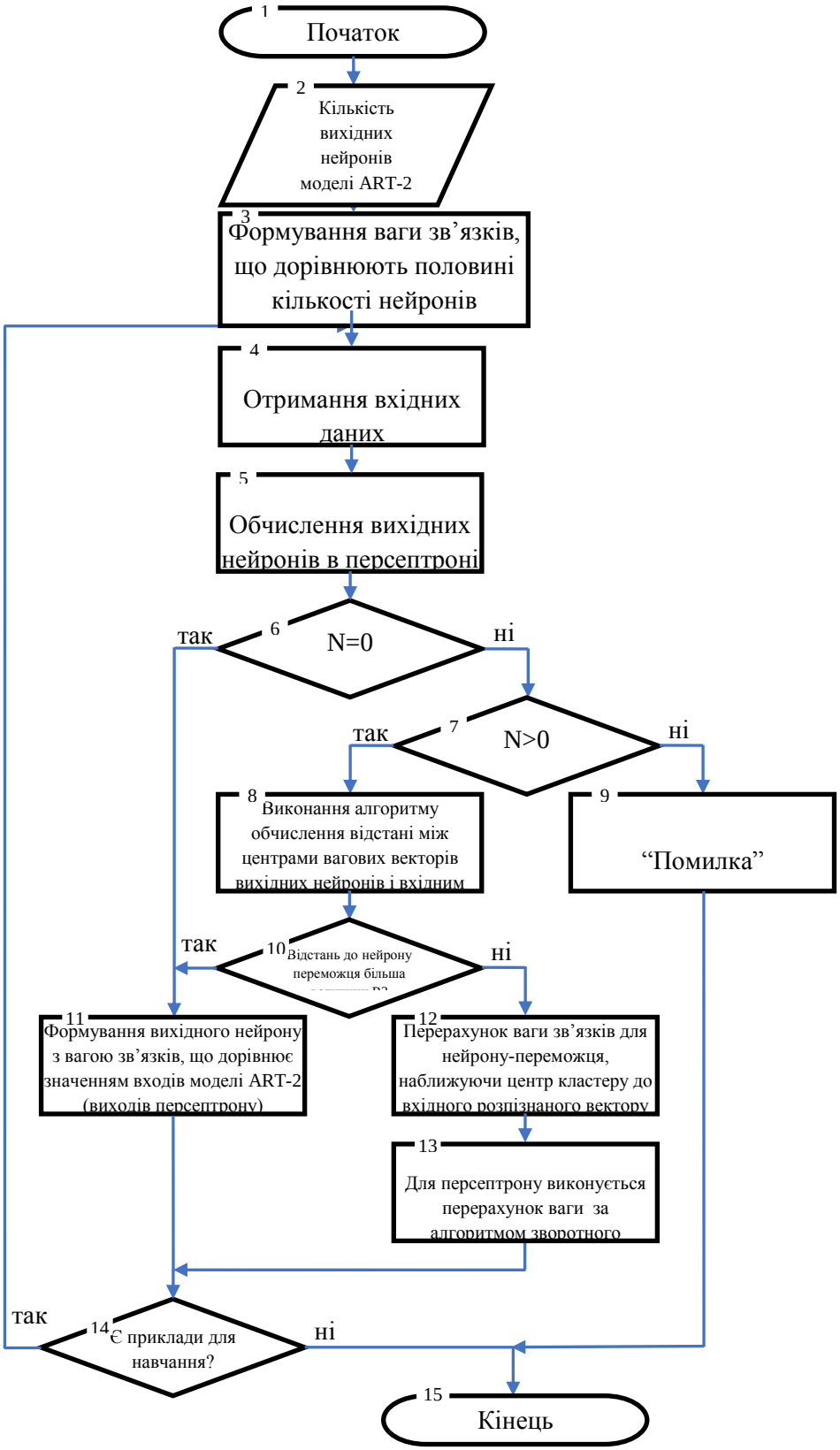

Рис. 12. Структурна схема алгоритму функціонування асоціативного блоку нейромережних експертів

Необхідно уточнити, що на кроках 10-13 якщо відстань для нейрона-переможця менше *R*, то в моделі АР-2 для нейрона-переможця перераховується вага зв'язків, наближаючи центр кластеру до вхідного розпізнаного вектору моделі АР-2 з урахуванням кількості розпізнаних раніше векторів цього кластеру (чим їх було більше, тим менша зміна ваги нейрона-переможця).

Для персептрону виконується перерахування ваги за алгоритмом зворотного поширення помилки [26]. При цьому вихідним еталонним вектором вважається новий вектор ваги вихідного нейрону переможця моделі АР-2, і кількість ітерацій може бути невеликою (зокрема, може бути всього одна ітерація).

Таким чином, розроблена модель системи нейромережних експертів, відрізняється від відомих комплексним використанням нейронних мереж різного типу і конфігурації.

Це дозволило синхронізувати роботу асоціативного блоку нейромережних експертів і підвищити точність ухвалення рішення про аномальність характеристик оптоволоконних ліній зв'язку.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано метод антивірусного захисту даних у ТКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи. Основними складовими методу є: алгоритми формування множини маршрутів передачі метаданих, метод контролю ліній зв'язку ТКС, моделі системи нейромережних експертів безпечної маршрутизації.

Рішення оптимізаційного завдання вибору і формування базової множини шляхів передачі даних проведено за критерієм мінімуму часу передачі метаданих на вузол програмного серверу. У той же час рішення приватного оптимізаційного завдання формування множини обраних маршрутів здійснювалося за критерієм максимуму ймовірності безпечної передачі даних.

Для постійного моніторингу і рішення завдання переформатування маршрутів зв'язку з вузлом програмного серверу розроблений метод контролю ліній зв'язку ТКС. Використання даного методу дозволить виявляти зміну характеристик ВОЛЗ у процесі функціонування ТКС, (одержати необхідні дані для початку процедури навчання нейронних експертів) і видавати необхідні сигнали аномалій (можливих кібератак) у лініях зв'язку в систему нейромережних експертів безпечної маршрутизації. Відмінною рисою запропонованого методу є введення процедури обліку «скомпрометованих» біт даних спеціальних сигнатур, що передані у хмарні антивірусні системи. Це дозволить знизити ймовірність маніпуляцій метаданими, переданими у вузли програмного серверу.

Для підвищення точності прийняття рішень про можливі атаки несанкціонованого доступу до ВОЛЗ і рішення в цілому завдання безпечної маршрутизації розроблена модель системи нейромережних експертів, що відрізняється від відомих комплексним використанням нейронних мереж різного типу і конфігурації. Даний механізм робить інтеграцію знань, накопичених експертами, у загальне рішення, що має пріоритет над кожним рішенням окремого експерта. При цьому рішення експертів, отримані на основі обробки даних, що пов'язані з безпечною маршрутизацією, дозволяють підвищити точність ухвалення правильного рішення про несанкціонований доступ на маршруті передачі метаданих.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] А.Г. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*. Київ, Україна: «МК-Пресс», 2006.
[2] А.В. Лукацкий, *Обнаружение атак*. Санкт- Петербург, Россия: BHV, 2001.
[3] А.А. Смирнов, В.В. Босько, и Е.В. Мелешко, " Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей", *Системи обробки інформації. ХУПС*, № 7(74), с. 120-123, 2008.
[4] А.А. Смирнов, и Е.В. Мелешко, " Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети ", на *II Всеукр. наук.-практ. конф. Системний аналіз. Інформатика. Управління,* Запоріжжя, 2011.
[5] А. А. Смирнов, С. А. Смирнов, и А. К. Дидык, " Разработка и реализация метода безопасной маршрутизации метаданных в облачные антивирусные системы " на *Securitea informationala 2015-2016: Conferenta internationala (editia a XII-a), Chisinau, Moldova, 3 martie 2016*, Chisinau: ADSEM, 2016, с. 90-96.
[6] О.А. Смірнов, С.А. Смірнов, Л.І. Поліщук, О.К. Конопліцька-Слободенюк, та Т.В. Смірнова, " GERT-моделі технології хмарного антивірусного захисту ", *Кібербезпека: освіта, наука, техніка. Київський університет ім.Бориса Грінченка*, т. 2, № 2, с. 6-30, Груд. 2018. doi:10.28925/2663-4023.2018.2
[7] Jiang Hu, and Sachin S. Sapatnekar, " A Timing-Constrained Simultaneous Global Routing Algorithm ", *IEEE Transactions on computer-aided design of integrated circuits and systems*, no.21(9), pp. 1025-1036, 2002.
[8] Joao Luis Sobrinho, " Algebra and Algorithms for QoS Path Computation and Hop-by-Hop Routing in the Internet ", *IEEE ACM Transactions on networking*, no.10(4), pp. 541-55, 2002.
[9] Jui-Fa Chen, and Wei-Chuan Lin, " A Message Interchange Protocol based on Routing Information Protocol in a Virtual World ", *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)*, pp. 201-208, 2005.
[10] Jun Wang, and Klara Nahrstedt, " Hop-by-Hop Routing Algorithms For Premium-class Traffic In DiffServ Networks ", *Proceedings of IEEE INFOCOM*, pp. 705-714, 2002.
[11] Mohamed G. Gouda, Member, IEEE, and Marco Schneider, " Maximizable Routing Metrics ", *IEEE ACM Transactions on networking*, no.11(4), pp. 663-675, 2003.
[12] В.М. Вишневский, *Теоретические основы проектирования компьютерных сетей*. Москва, Россия: Техносфера, 2003.
[13] Murali Kodialam, T. V. Lakshman, and Sudipta Sengupta, " Online Multicast Routing With Bandwidth Guarantees: A New Approach Using Multicast Network Flow ", *IEEE ACM Transactions on networking*, no.11(4), pp. 676-686, 2003.
[14] Vutukury S., and Garcia-Luna-Aceves J. J., " MDVA: A Distance-Vector Multipath Routing Protocol ", *Proc. IEEE INFOCOM. - Anchorage*, pp. 557-564, 2001.
[15] Vutukury S., and Garcia-Luna-Aceves J.J., " MPATH: a loop-free multipath routing algorithm ", *Elsevier Journal of Microprocessors and Microsystems*, no.24(6), pp. 319-327, 2001.
[16] Wendong Xiao, Boon Hee Soong, Choi Look Law, and Yong Liang Guan, " Evaluation of Heuristic Path Selection Algorithms' for Multi-Constrained QoS Routing ", *IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23*, pp. 112-116, 2004.
[17] Э. Майника, *Алгоритмы оптимизации на сетях и графах*: *пер. с англ.*, Е.К. Масловского, Ред. Москва, Россия: Мир, 1981.
[18] Pape U., " Implementation and Efficiency of Moore - Algorithms for the Shortest Path Problem ", *U. Pape.Math. Programming*, vol. 7, pp. 212-222, 1974.
[19] В. Е. Гмурман, *Теория вероятностей и математическая статистика*. Москва, Россия: Высшая школа, 2003.
[20] Ш. Одом, и Х. Ноттингем, *Коммутаторы CISCO*. Москва, Россия: "Кудиц-Образ", 2003.
[21] В.Г. Олифер, и Н.А. Олифер, *Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов*. 2-е изд. Санкт- Петербург, Россия: Питер, 2007.
[22] *ДСТУ В 3265 – 95. Зв'язок військовий. Терміни та визначення.* Київ, Україна: УкрНДІССІ, 1995.
[23] В.Л. Банкет и др., *Современные телекоммуникации. Технологии и экономика*. С.А. Довгого, Ред. Москва, Россия: Эко-Трендз, 2003.
[24] С.Г. Семенов, В.В. Давыдов, и С.Ю. Гавриленко, *Защита данных в компьютеризированных управляющих системах*. Саарбрюккен, Германия: LAP Lambert Academic Publishing GmbH & Co. KG, 2014.

ISSN 2663 - 4023

[25] В.В. Величко, Е.А. Субботин, В.П. Шувалов, и А.Ф. Ярославцев, *Телекоммуникационные системы и сети: учебное пособие*. В 3 томах. В.П. Шувалова, Ред. Москва, Россия: Горячая линия-Телеком, т.3, 2005.

[26] С. Хайкин, *Нейронные сети: полный курс*. Москва, Россия:Вильямс, 2006.

[27] Ю.Н. Лавренков, " Исследование и разработка комбинированных нейросетевых технологий для повышения эффективности безопасной маршрутизации информации в сетях связи ", дис. канд. техн.наук., 2014.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

Serhii Smirnov
Candidate of Science (Engineering), PhD, senior lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

Liudmyla Polishchuk
Senior lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-5093-1581
pli_80@ukr.net

Tetiana Smirnova
Candidate of Science (Engineering), PhD
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID:0000-0001-6896-0612
sm.tetyana.gmail.com

Oksana Konoplitska-Slobodeniuk
Lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-9981-5194
ksuha80@gmail.com

Oleksii Smirnov
Doctor of Engineering, Head of Cybersecurity & Software Academic Departmen
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

A METHOD OF FORMING OF ANTI-VIRUS PROTECTION OF DATA IS WITH THE USE OF SAFE ROUTING OF METADATAS

Abstract. In this article the method of anti-virus protection of data is worked out in TCS due to the safe routing of metadatas in anti-virus nephystems. He is intended for the decision of range of problems, that consists in that with the aim of increase of efficiency of the use of facilities of anti-virus protection of data and minimization of consequences of similar cyberbuck of crimes, a timely exposure and localization of computer viruses are an extremely important and at the same time difficult task. By the basic constituents of method, that is offered in this work, is, : algorithms of forming of great number of TPS of metadatas, method of control of flow of TCS, model of the system of neural network experts of the safe routing lines. The distinguishing feature of algorithms of forming of great number of TPS of metadatas are indexes of optimization and limitations that is entered, for the safe routing. The novelty of method of control of flow of TCS lines consists in the account of the "compromised" bats of these special signatures that is passed in anti-virus nephystems. It will allow to bring down probability of manipulations metadatas that is passed in the knots of programmatic server. The feature of the worked out system of neural network experts is a complexity of the use of neural networks as ART and multi-layered to perceptron for the decision of task of the safe routing that will allow to promote exactness of acceptance of correct decision about an unauthorized division to the fiber-optic lines.

Keywords: telecommunication systems; anti-virus defence; treatment of metadatas; anti-virus nephystems.

REFERENCES

[1] A.G. Korchenko, *Construction of the systems of priv on fuzzy sets. Theory and practical solutions*. Kyiv, Ukraine: MK-Press, 2006. (In Russian).
[2] A.V. Lukatsky, *Detection of attacks*. St. Petersburg, Russia: BHV, 2001. (In Russian).
[3] A.A. Smirnov, V.V. Bosko, i E.V. Meleshko, "Analysis and comparative study of promising directions for the development of digital telecommunication systems and networks", *Systems of treatment of information. KhUPS*, no. 7 (74), pp. 120-123, 2008. (In Russian).
[4] A.A. Smirnov, i E.V. Meleshko, " Improvement of management method by turns in the multiprotocol knots of TCN ", in *II Vseukr. nauk.-prakt. konf. Analysis of the systems. Informatics. Management*, Zaporizhzhya, 2011. (In Russian).
[5] A. A. Smirnov, S. A. Smirnov, i A. K. Didyik, " Development and realization of method of the safe routing of metadatas in anti-virus nephystems " in *Securitea informationala 2015-2016: Conferenta internationala (editia a XII-a), Chisinau, Moldova, 3 martie 2016*, Chisinau: ADSEM, 2016, pp. 90-96. (In Russian).
[6] O.A. Smirnov, S.A. Smirnov, L.I. Polishchuk, O.K. Konoplitska-Slobodeniuk, ta T.V. Smirnova, " GERT-models of technology of cloudy anty-virus defence", *Kiberbezpeka: osvita, nauka, tekhnika. Kyivskyi universytet im.Borysa Hrinchenka*, v. 2, № 2, pp. 6-30, Decem. 2018. (In Ukrainian).
[7] Jiang Hu, and Sachin S. Sapatnekar, " A Timing-Constrained Simultaneous Global Routing Algorithm ", *IEEE Transactions on computer-aided design of integrated circuits and systems*, no.21(9), pp. 1025-1036, 2002. (in English).
[8] Joao Luis Sobrinho, " Algebra and Algorithms for QoS Path Computation and Hop-by-Hop Routing in the Internet ", *IEEE ACM Transactions on networking*, no.10(4), pp. 541-55, 2002. (in English).
[9] Jui-Fa Chen, and Wei-Chuan Lin, " A Message Interchange Protocol based on Routing Information Protocol in a Virtual World ", *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)*, pp. 201-208, 2005. (in English).
[10] Jun Wang, and Klara Nahrstedt, " Hop-by-Hop Routing Algorithms For Premium-class Traffic In DiffServ Networks ", *Proceedings of IEEE INFOCOM*, pp. 705-714, 2002. (in English).
[11] Mohamed G. Gouda, Member, IEEE, and Marco Schneider, " Maximizable Routing Metrics ", *IEEE ACM Transactions on networking*, no.11(4), pp. 663-675, 2003. (in English).
[12] V.M. Vishnevskiy, *Theoretical bases of planning of computer networks*. Moscow, Russia : Tehnosfera, 2003. (In Russian).
[13] Murali Kodialam, T. V. Lakshman, and Sudipta Sengupta, " Online Multicast Routing With Bandwidth Guarantees: A New Approach Using Multicast Network Flow ", *IEEE ACM Transactions on networking*, no.11(4), pp. 676-686, 2003. (in English).
[14] Vutukury S., and Garcia-Luna-Aceves J. J., " MDVA: A Distance-Vector Multipath Routing Protocol ", *Proc. IEEE INFOCOM. - Anchorage*, pp. 557-564, 2001. (in English).
[15] Vutukury S., and Garcia-Luna-Aceves J.J., " MPATH: a loop-free multipath routing algorithm ", *Elsevier Journal of Microprocessors and Microsystems*, no.24(6), pp. 319-327, 2001. (in English).
[16] Wendong Xiao, Boon Hee Soong, Choi Look Law, and Yong Liang Guan, " Evaluation of Heuristic Path Selection Algorithms' for Multi-Constrained QoS Routing ", *IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23*, pp. 112-116, 2004. (in English).
[17] E. Maynika, *Algorithms of optimization on networks and columns : trudged. with an eng*, E.K. Maslovskogo, Ed. Moscow, Russia: Mir, 1981. (In Russian).
[18] Pape U., " Implementation and Efficiency of Moore - Algorithms for the Shortest Path Problem ", *U. Pape.Math. Programming*, vol. 7, pp. 212-222, 1974. (in English).
[19] V. E. Gmurman, *Theory of chances and mathematical statistics*. Moscow, Russia: Vyisshaya shkola, 2003. (In Russian).
[20] Sh. Odom, i H. Nottingem, *Kommutatoryi CISCO*. Moscow, Russia: "Kudits-Obraz", 2003. (In Russian).
[21] V.G. Olifer, i N.A. Olifer, *Computer networks. Principles, technologies, protocols : textbook for institutions of higher learning. a 2th publ*. Sankt - Petersburg, Russia: Piter, 2007. (In Russian).
[22] *SSU B 3265 - 95. Copulas is military. Terms and determinations*. Kyiv, Ukraine: UkrNDISSI, 1995. (In Ukrainian).
[23] V.L. Banket i dr., *Modern telecommunications. Technologies and economy*. S.A. Dovgogo, Ed. Moscow, Russia: Eko-Trendz, 2003. (In Russian).
[24] S.G. Semenov, V.V. Davydov, i S.Ju. Gavrilenko, *Defence the systems given in the computerized managers*. Saarbrjukken, Germany: LAP Lambert Academic Publishing GmbH & Co. KG , 2014. (In Russian).

[25] V.V. Velichko, E.A. Subbotin, V.P. Shuvalov, i A.F. Yaroslavtsev, *Telecommunication systems and networks : train aid. In 3 volumes*. V.P. Shuvalova, Ed. Moscow, Russia: Goryachaya liniya-Telekom, v.3, 2005. (In Russian).

[26] S. Haykin, *Neural networks: complete course*. Moscow, Russia:Vilyams, 2006. (In Russian).

[27] Ju.N. Lavrenkov, " Research-and-development the combined nejronetwork technologies for the increase of efficiency of the safe routing of information in communication networks ", work of candidate of engineering sciences, 2014. (In Russian).