УДК 004.056:004.94
DOI https://doi.org/10.32782/IT/2021-1-2

Валерій КОРНІЄНКО
доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, korniienko.v.i@nmu.one
***ORCID:** 0000-0002-0800-3359*
***Scopus Author ID:** 56446921900*

Олександра ГЕРАСІНА
кандидатка технічних наук, доцентка, доцентка кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, herasina.o.v@nmu.one
***ORCID:** 0000-0002-8196-0657*
***Scopus Author ID:** 55998621600*

Дмитро ТИМОФЄЄВ
старший викладач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, tymofieiev.d.s@nmu.one
***ORCID:** 0000-0002-9718-6678*
***Scopus Author ID:** 55437340600*

Олександр САФАРОВ
кандидат технічних наук, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, safarov o.o@nmu.one
***ORCID:** 0000-0003-1489-2006*
***Scopus Author ID:** 57191867000*

Юлія КОВАЛЬОВА
асистентка кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, kovalova.yu.v@nmu.one
***ORCID:** 0000-0002-9234-4454*
***Scopus Author ID:** 55320891100*

Бібліографічний опис статті: Корнієнко, В., Герасіна, О., Тимофєєв, Д., Сафаров, О., Ковальова, Ю. (2021). Оцінювання характеристик самоподібного трафіку інформаційно-комунікаційних мереж для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 1, 8–15, doi: https://doi.org/10.32782/IT/2021-1-2

ОЦІНЮВАННЯ ХАРАКТЕРИСТИК САМОПОДІБНОГО ТРАФІКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

У роботі визначена актуальність розробки та вдосконалення систем виявлення вторгнень, головним завданням яких є розпізнавання мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Ця проблема вирішується шляхом використання засобів моніторингу, здатних аналізувати трафік мережі в режимі реального часу. Для цього розроблена методика оцінювання та визначення характеристик самоподібного трафіку сучасних інформаційно-комунікаційних мереж, що дозволяє формувати вектор інформативних ознак щодо визначення аномалій для системи виявлення атак. На прикладі експериментального сигналу трафіка мережі Ethernet відповідно до запропонованої методики проаналізовані та визначені характеристики мережевого трафіка. ***Метою роботи*** *є обгрунтування методики комплексного оцінювання характеристик самоподібного трафіка інформаційно-комунікаційних систем і мереж щодо визначення аномалій для систем виявлення атак.* ***Методологія*** *вирішення поставленого*

завдання полягає у комплексному використанні методів час-частотного, статистичного, фрактального та мультифрактального аналізів, адекватних закономірностям сучасного трафіку інформаційно-комунікаційних мереж, що має самоподібний (фрактальний чи мультифрактальний) характер. ***Наукова новизна****. Обгрунтована методика комплексної оцінки характеристик самоподібного трафіка інформаційно-комунікаційних мереж, що включає час-частотний, статистичний, фрактальний і мультифрактальний аналізи, яка дозволяє підвищити ймовірність визначення вторгнень для систем виявлення атак за рахунок підвищення достовірності інформативних ознак самоподібного трафіка.* ***Висновки****. Запропонована методика комплексного використання методів аналізу, адекватних закономірностям сучасного трафіку інформаційно-комунікаційних мереж, підвищує ефективність визначення аномалій за рахунок підвищення інформативності оцінюваних характеристик трафіку.*

Ключові слова: *оцінка, характеристика, самоподібний трафік, інформаційно-комунікаційна мережа, виявлення атак.*

Valerii KORNIIENKO
Doctor of Technical Sciences, Professor, Head of Information Security and Telecommunication Department, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, korniienko.v.i@nmu.one
ORCID: *0000-0002-0800-3359*
Scopus Author ID: *56446921900*

Oleksandra HERASINA
Candidate of Technical Sciences, Associate Professor, Associate Professor of Information Security and Telecommunication Department, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, herasina.o.v@nmu.one
ORCID: *0000-0002-8196-0657*
Scopus Author ID: *55998621600*

Dmytro TYMOFIEIEV
Senior Lecturer of Information Security and Telecommunication Department, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, tymofieiev.d.s@nmu.one
ORCID: *0000-0002-9718-6678*
Scopus Author ID: *55437340600*

Oleksandr SAFAROV
Candidate of Technical Sciences, Associate Professor of Information Security and Telecommunication Department, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, safarov o.o@nmu.one
ORCID: *0000-0003-1489-2006*
Scopus Author ID: *57191867000*

Yuliia KOVALOVA
Assistant of Information Security and Telecommunication Department, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, kovalova.yu.v@nmu.one
ORCID: *0000-0002-9234-4454*
Scopus Author ID: *55320891100*

To cite this article: Korniienko, V., Herasina, O., Tymofieiev, D., Safarov, O., Kovalova, Yu. (2021) Otsiniuvannia kharakterystyk samopodibnoho trafiku informatsiino-komunikatsiinykh merezh dlia system vyiavlennia atak [Estimation of self-similar traffic characteristics of information and communication networks for attack detection systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 1, 8–15, doi: https://doi.org/10.32782/IT/2021-1-2

ESTIMATION OF SELF-SIMILAR TRAFFIC CHARACTERISTICS OF INFORMATION AND COMMUNICATION NETWORKS FOR ATTACK DETECTION SYSTEMS

The urgency of development and improvement of intrusion detection systems, the main task of which is to recognize network attacks, attempts of unauthorized access and use of network resources, is determined in the work. This problem is solved by using monitoring tools that can analyze network traffic in real time. For this

purpose, a method of estimating and determining the characteristics of self-similar traffic of modern information and communication networks has been developed, which allows to form a vector of informative features for determining anomalies for the attack detection system. On the example of the experimental signal of Ethernet traffic in accordance with the proposed method, the characteristics of network traffic are analyzed and determined. ***The aim*** *there is a substantiation of a technique of complex estimation of characteristics of self-similar traffic of information and communication systems and networks concerning definition of anomalies for systems of detection of attacks.* ***The methodology*** *the solution of this problem is the integrated use of methods of time-frequency, statistical, fractal and multifractal analysis, adequate to the laws of modern traffic of information and communication networks, which has a self-similar (fractal or multifractal) nature.* ***Scientific novelty****. The method of complex estimation of self-similar traffic characteristics of information and communication networks, including time-frequency, statistical, fractal and multifractal analyzes, which allows to increase the probability of intrusion detection for attack detection systems by increasing the reliability of informative features of self-similar traffic.* ***Conclusions.*** *The offered technique of complex use of the methods of the analysis adequate to laws of modern traffic of information and communication networks, increases efficiency of definition of anomalies at the expense of increase of informativeness of the estimated characteristics of traffic.*

Key words: *estimation, characteristics, self-similar traffic, information and communication network, detection of attacks.*

Актуальність проблеми. Стрімкий розвиток інформаційно-комунікаційних систем і мереж (ІКМ) та інформаційних технологій викликає ряд проблем, пов'язаних з безпекою мережевих ресурсів. Тому актуальною є розробка та вдосконалення систем виявлення та запобігання вторгнень, головним завданням яких є розпізнавання мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі [1; 2].

Ця проблема вирішується шляхом використання засобів моніторингу, здатних аналізувати трафік мережі в режимі реального часу. До таких засобів моніторингу відносяться системи виявлення та запобігання атак (СВА).

Аналіз останніх досліджень і публікацій. Захист критично важливих об'єктів інфраструктури від навмисних кібернетичних вторгнень зі сторони окремих осіб, організацій або країн є надзвичайно актуальним. Наприклад, до основних загроз для промислових систем управління відносяться, зокрема: мережеві атаки через корпоративні мережі; атаки на стандартні мережеві компоненти; атаки типу «відмова в обслуговуванні» [3].

Засобом захисту ІКМ від інформаційно руйнівних втручань у вигляді кібернетичних вторгнень є системи СВА, основне завдання яких полягає в оперативному їх виявленні та в ініціюванні ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів.

Наразі сформувались два напрямки протидії вторгнень: виявлення зловживань та виявлення аномалій [4; 5].

При виявленні мережевих аномалій [1] даними для аналізу є мережевий трафік, представлений як інтенстівность (швидкість) передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP. Дані можуть бути агреговані за певний часовий інтервал і нормалізовані, по ним оцінюються характеристики (набір ознак) трафіку. Створений набір ознак порівнюється з набором характеристик нормальної діяльності об'єкта (користувача або системи) – шаблоном нормальної поведінки. Якщо спостерігається суттєва розбіжність порівнюваних наборів, то фіксується мережева аномалія. В іншому випадку відбувається уточнення шаблону нормального трафіку за допомогою зміни параметрів його настройки з урахуванням поточного спостережуваного профілю мережевої активності.

На такий алгоритм виявлення аномалій орієнтуються поведінкові методи аналізу мережевого трафіку, до яких можна віднести: вейвлет-аналіз; статистичний аналіз; аналіз ентропії; спектральний аналіз; фрактальний аналіз; кластерний аналіз [1; 6; 7].

Трафік в ІКМ є нелінійним стохастичним процесом з властивостями самоподоби та з хаотичною і фрактальною динамікою. Крім того, встановлено, що агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер [8].

Таким чином, актуальною задачею є комплексне спостереження інформативних ознак мережевого самоподібного трафика для визначення аномалій в системах виявлення атак.

Мета статті: Обгрунтування методики комплексного оцінювання характеристик самоподібного трафіка інформаційно-комунікаційних систем і мереж щодо визначення аномалій для систем виявлення атак.

Виклад основного матеріалу.

Комплексна оцінка характеристик трафіку. Фрактальним (самоподібним) є стаціонарний випадковий процес x із постійним середнім і автокореляційною функцією (АКФ), яку можно записати як:

$$r(k) \sim L_1(t)k^{-\beta} \text{ при } k \to \infty, \quad (1)$$

де L_1 – поволі змінювана на нескінченності функція, тобто для $x > 0$ вона має $\lim_{t\to\infty} L_1(xt)/L_1(t) = 1$; $\beta = 2 - 2H$; $0 < \beta < 1$; H – параметр Херста.

Час-частотний аналіз. Для самоподібних процесів з довготривалою (поволі убуваючою – ПУЗ) залежністю АКФ гіперболічно убуває зі зростанням часової затримки k. Навпаки, процеси з короткостроковою (швидко убуваючою – ШУЗ) залежністю характеризуються експоненційно спадаючою інтегрованою АКФ. Для визначення типу залежності в експериментальному часовому ряді необхідно його АКФ апроксимувати за величиною похибки встановити тип процесу (ПУЗ або ШУЗ).

Спектральна щільність самоподібного процесу підкорюється ступеневому закону:

$$S(f) \sim L_2(t)f^{-\gamma} \text{ при } f \to 0, \quad (2)$$

де $L_2(t)$ – поволі змінювана в нулі функція; $0 < \gamma < 1$; $\gamma = 2H + 1$.

Спектральний аналіз дозволяє виділяти найбільш інформативні складові досліджуваного процесу за допомогою зміни розмірності вихідного простору ознак. Головні компоненти обираються таким чином, щоб вони відповідали найбільшій мінливості процесу. Інші компоненти можуть бути розглянуті як складові шуму.

Вейвлет-аналіз полягає у визначенні коефіцієнтів розкладання вихідного сигналу по базисним функціям. Як сигнал може розглядатися інтенсивність мережевого трафіку або дані про кореляцію IP-адрес призначення [1].

Виконання вейвлет-перетворення дозволяє виділити найбільш вагому інформацію за рівнем коефіцієнтів перетворення. Наприклад, воно дозволяє виділити [1]: аномалії, викликані помилками в налаштуваннях мережевого обладнання, а також збоєм в роботі обладнання; мережеві атаки класом «відмова в обслуговуванні»; перевантаження в мережі та інші.

Скелетон (потужність коефіцієнтів вейвлет перетворення) показує наявність самоподоби у вигляді розвиненої деревоподібної структури з розгалуженнями (гілками), залежність від масштабу яких описується по ступеневому закону.

Підраховуючи число точок максимумів коефіцієнтів вейвлет-перетворення $N(\eta)$ уздовж параметра зсуву в області масштабу η можна оцінити значення параметра Херста:

$$H = \log[N(\eta)]/\log(\eta). \quad (3)$$

Статистичний аналіз. Якщо дисперсія процесу поволі убуває, тобто дисперсія вибіркового середнього має повільніший спад, ніж величина, зворотна довжині вибірки:

$$\sigma^2(x^{(m)}) \sim m^{-\beta} \text{ при } m \to \infty, \quad (4)$$

то даний процес є самоподібним ($\beta = [0,1]$).

Інструментом статистичного аналізу є дослідження функції розподілу. Для самоподібних процесів зі ступеневим (гіперболічним) убуванням АКФ характерним є розподіл з «важким хвостом».

Випадкова величина Z має розподіл з «важким хвостом», якщо

$$P[Z > x] \sim cx^{\alpha} \text{ при } x \to \infty, \quad (5)$$

де $0 < \alpha < 2$ – параметр форми (показник «тяжкості хвоста»), c – позитивна константа.

Найчастіше для апроксимації гістограм експериментальних даних самоподібних процесів застосовуються функції субекспоненціальних законів розподілу: Парето, Вейбулла, логнормальний тощо. Для перевірки адекватності теоретичних розподілів експериментальним даним використовуються критерії згоди Колмогорова і Пірсона.

Показник «тяжкості хвоста» (параметр форми) α визначають по методу Хілла або шляхом побудови графіка додаткового розподілу в подвійному логарифмічному масштабі (LLCD).

Для перевірки нульової гіпотези про незалежність і тотожність розподілу значень часового ряду запропоновано BDS-тест, який також дозволяє виявити нелінійність породжуючої системи, відрізнити випадкові системи від детермінованого хаосу або від нелінійних стохастичних систем [8].

BDS-статистика w є нормально розподіленою: якщо w приймає значення $|w| \le 1{,}96$, то нульову гіпотезу з вірогідністю 95% можна прийняти (спостерігається стохастичний процес, відліки якого незалежні, однаково розподілені випадкові величини), інакше $|w| > 1{,}96$ – нульову гіпотезу необхідно відхилити (спостерігається хаотичний процес). Якщо в результаті виконання BDS-теста для залишків (похибки) лінійної моделі виявиться, що нульову гіпотезу потрібно відхилити, то даний процес є нелінійним.

Статистичний аналіз [1; 7; 8] є ядром методів виявлення аномалій в мережі. Перевагами статистичних систем є їх адаптація до зміни поведінки користувача, а також здатність до виявлення модифікацій атаки. Серед недоліків можна відзначити високу ймовірність виникнення помилкових повідомлень про атаки і залежність від порядку проходження подій.

Фрактальний аналіз. Сучасний мережевий трафік є самоподібним і має фрактальну (дробову) розмірність в часі.

За часовим рядом при відомому значенні кореляційного інтеграла $C(\varepsilon)$ визначається кореляційна розмірність D_C:

$$D_C = \lim_{\varepsilon \to 0} \frac{\log C(\varepsilon)}{\log(\varepsilon)}, \quad (6)$$

де ε – мінімальна відстань у просторі.

Показник Херста H характеризує ступінь самоподоби процесу. Для його визначення використовують: метод періодограм, вейвлет-аналіз, метод агрегованих дисперсій і R/S-аналіз. Згідно з останнім показник Херста визначається по формулі

$$H = \frac{\log(R/S)}{\log(cN)}, \quad (7)$$

де S – середньоквадратичне відхилення спостережуваного часового ряду, R – розмах накопиченого відхилення, N – число періодів спостережень, c – позитивна константа.

Даний показник свідчить про наявність тренда або про випадковість процесу, а також характеризує еволюцію досліджуваного процесу. Якщо $0{,}5 < H < 1$, то даний процес характеризується довготривалою пам'яттю і є персистентним, якщо ж $0 < H < 0{,}5$, то це говорить про антиперсистентність процесу. Значення $H = 0{,}5$ характерне для броунівського руху з незалежними добутками і відповідає випадковим відхиленням процесу від середнього.

Для визначення режиму породжуючого процесу, оцінюють його ентропію Колмогорова K, яка дорівнює сумі старших показників Ляпунова і характеризує швидкість втрати інформації про стан динамічної системи в часі. К-ентропія дорівнює нулю при регулярному русі, нескінченна для випадкових систем, позитивна і обмежена для систем з динамічним хаосом.

Значення кореляційної ентропії оцінюють по кореляційному інтегралу $C(\varepsilon, d)$, залежному як від відстані ε, так і від розміру фазового простору d:

$$K_C(\varepsilon, d) = \frac{C(\varepsilon, d)}{C(\varepsilon, d+1)}. \quad (8)$$

Кореляційна ентропія також дозволяє визначити оцінку інтервалу точної передбачуваності процесу:

$$T_C = \frac{1}{K_C} \ln\left(\frac{1}{\varepsilon}\right). \quad (9)$$

Кореляційна ентропія K_C є нижньою межею К-ентропії. За час, більший T_C можливе тільки статистичне прогнозування.

Мультифрактальний аналіз. Агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер, тобто має гнучкий закон масштабування.

Залежність узагальненої статистичної функції Q від відстані ε та значення порядку q описується як

$$Q(q, \varepsilon) \approx \varepsilon^{\tau_q}, \quad (10)$$

де τ_q – скейлінгова експонента (масштабна функція), що визначається як

$$\tau_q = \lim_{\varepsilon \to 0} \frac{\ln Q(q, \varepsilon)}{\ln \varepsilon}, \quad (11)$$

$$\tau_q = (q-1) D_q, \quad (12)$$

де D_q – спектр сингулярностей, який характеризує розподіл точок в деякій області і показує наскільки неоднорідною є досліджувана множина точок.

Якщо D_q залежить від q, то даною множиною точок є мультифрактал (неоднорідна фрактальна множина) з нелінійною функцією τ_q.

Для аналізу властивостей самоподоби і довготривалої залежності нестаціонарних часових рядів застосовують мультифрактальний аналіз детрендових флуктуацій (АДФ), який є різновидом дисперсійного аналізу.

Часовий ряд $x(k)$ розбивається на m підпослідовностей довжини n ($nm = N$), для кожного з яких обчислюється локальний тренд $x_n(k)$ та середньоквадратична похибка такої апроксимації $F(n)$. Відповідні розрахунки повторюються для відрізків різної довжини. Про наявність самоподоби свідчить ступеневий характер залежності:

$$F(n) \sim n^{\alpha}; \ \alpha \sim \log F(\log n). \quad (13)$$

Залежно від значення показник скейлінга α можна класифікувати часовий ряд. Так, для випадкового процесу (некорельована поведінка) $\alpha = 0{,}5$; $0 < \alpha < 0{,}5$ відповідає антиперсистентному ряду; $0{,}5 < \alpha < 1$ визначає персистентні довготривалі кореляції; $\alpha = 1$ характерне для 1/f-шума. При $\alpha > 1$ кореляції існують, проте ступеневу залежність вони не відображають; $\alpha = 1{,}5$ характерне для броунівського шуму.

При мультифрактальному АДФ обчислюється кумулятивний ряд $x(k)$, що потім розділяється на $N_s = N/s$ непересічних відрізків довжини s, для яких обчислюється дисперсія $F^2(s)$.

Функції флуктуацій q-го порядку визначається усередненням цих дисперсій:

$$F_q(s) = \left\{ \frac{1}{2N_s} \sum_{\nu=1}^{2N_s} \left[F_\nu^2(s) \right]^{q/2} \right\}^{1/q}. \quad (14)$$

Якщо залежність $F_q(s)$ від s має ступеневий характер

$$F_q(s) \sim s^{h(q)}, \quad (15)$$

то даний часовий ряд зводиться до самоподібної множини, що проявляє довготривалі кореляції.

З виразів (14), (15) випливає, що при $q = 2$ показник Гельдера (узагальнений показник Херста) $h(q) = H$. Для монофрактальних часових рядів узагальнений показник Херста не залежить від q, а флуктуаційна функція $F^2(s)$ постійна.

Для мультифрактальних рядів $h(q)$ – нелінійна функція. При позитивних значеннях q основний внесок у функцію $F_q(s)$ дають сегменти з великими відхиленнями $F^2(s)$, а при негативних – з малими. Таким чином, при негативних значеннях q узагальнений показник Херста $h(q)$ описує поведінку сегментів, що проявляють малі флуктуації, а при позитивних – великі.

Методика оцінки характеристик мережевого трафіку на основі вищевикладеного включає наступні етапи.

1. Час-частотний аналіз:

– визначення по АКФ процесу виду залежності (короткострокова або довготривала);

– побудова і аналіз графіка спектральної щільності потужності (вираз (2));

– аналіз виду вейвлет перетворення (оцінка показника Херста H (вираз (3)).

2. Статистичний аналіз:

– аналіз дисперсії вибіркового середнього (вираз (4));

– побудова гістограми експериментального розподілу і визначення його адекватності теоретичним розподілам за допомогою критеріїв згоди Колмогорова і Пірсона;

– визначення показника «тяжкості хвоста» α розподілу методом Хілла та/або методом LLCD

– застосування BDS-теста для перевірки нульової гіпотези про незалежність і тотожність розподілу значень часового ряду та виявлення нелінійної залежності.

3. Фрактальний аналіз:

– обчислення кореляційної розмірності атрактора D_C за виразом (6);

– визначення показника Херста H за виразом (7);

– обчислення кореляційної ентропії K_C за виразом (8);

– обчислення кореляційного інтервалу прогнозованості (глибини прогнозу) процесу T_C за виразом (9).

4. Мультифрактальний аналіз:

– визначення показника скейлінга α (вираз (13));

– обчислення скейлінгової експоненти τ_q (вираз (11));

– обчислення показника Гельдера $h(q)$ (вираз (15));

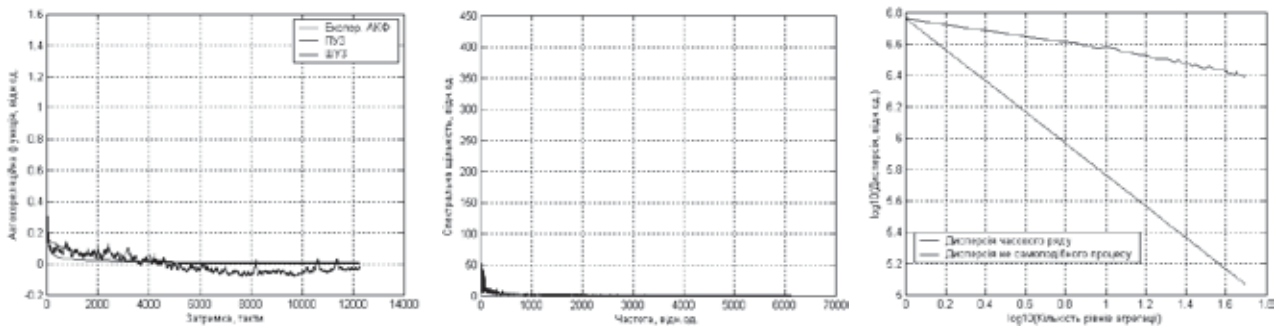
– визначення спектра сингулярностей D_q (вираз (12)).

Таким чином формується вектор інформативних ознак (характеристик і параметрів) мережевого самоподібного трафіку для подальшого виявлення аномалій для СВА.

Приклад аналізу та оцінки характеристик мережевого трафіку. Відповідно до методики, розглянутої вище, був виконаний аналіз сигналу трафіку мережі Ethernet [8], який був агрегований з кроком 5 с.

Процес, що породжує експериментальний сигнал трафіку має властивості, притаманні самоподібним процесам: гіперболічне убування АКФ із зростанням часової затримки (рис. 1,*а*), ступеневий закон його спектральної щільності (рис. 1,*б*) та поволі убуваючу дисперсію (рис. 1,*в*).

Сигнал має (табл. 1) розподіл з «важким хвостом» (показник форми становить $\alpha = 1{,}4$), гістограма експериментального розподілу згідно з критеріями згоди Колмогорова і Пірсона відповідає розподілу Парето, скейлетон вейвлет-перетворення сигналу має деревоподібну структуру, а показник Херста має діапазон значень [0,888; 0,980]. Процес також є нелінійним відповідно до результатів BDS-тесту.



а *б* *в*

Рис. 1. АКФ (*а*), спектр (*б*) та дисперсія (*в*) сигналу трафика

Таблиця 1

Таблиця вектору ознак мережевого трафіку

Показник	Сигнал трафіку
АКФ	ПУЗ
Спектр	Ступеневий закон
Вейвлет-перетворення	Деревоподібна структура скейлетона
Дисперсія	Поволі убуваюча
Закон розподілу за критерієм: – Колмогорова – Пірсона	 Парето Парето
Показник «важкості хвоста»	1,40
BDS-тест	Хаотичний нелінійний процес
Показник Херста – періодограмний метод – метод агрегованої дисперсії – R/S аналіз	 0,980 0,888 0,913
Кореляційна розмірність	2,956
Кореляційна ентропія	0,640
Інтервал прогнозованості	2,525
Показник скейлінга	0,980
Скейлінгова експонента*	- 0,253
Показник Гельдера*	0,212
Спектр сингулярностей*	0,614

** Значення функцій для порядку q=2.*

Гіпотези про тотожність розподілу значень сигналу приймались з вірогідністю 95 %.

Аналіз детрендових флуктуацій проводився на всьому сигналі трафіку (довжиною 16384 такти тривалістю 5 с), а також на малій частині цього сигналу (довжиною 256 тактів) – сигнал 1.

Для сигналу трафіка значення показника скейлінга склало $\alpha = 0.980$, що близьке до 1 (рис. 2, *а*) і це властиво для флікер-шума, у якого енергія спектра зворотно пропорційна частоті. Слід відмітити, що отримане значення показника скейлінга α співпадає зі значеннями показника Херста, отриманим періодограмним методом. (див. табл. 1).

Аналіз сигналу 1 дозволив виділити різні режими стану мережі (його трафіку). Поведінка сигналу 1 (рис. 2,*б*) на інтервалі від 10 до 86 тактів некорельована, оскільки показник скейлінга $\alpha 1 = 0,5$.

Проміжку часу від 87 до 129 тактів відповідає $\alpha 2 = 1,793 > 1$, що свідчить про кореляції, проте ступеневу залежність вони не мають. На інтервалі більше 129 тактів показник приймає значення $0,5 < \alpha = 0,921 < 1$, що властиве для персистентних процесів, які мають тренд.

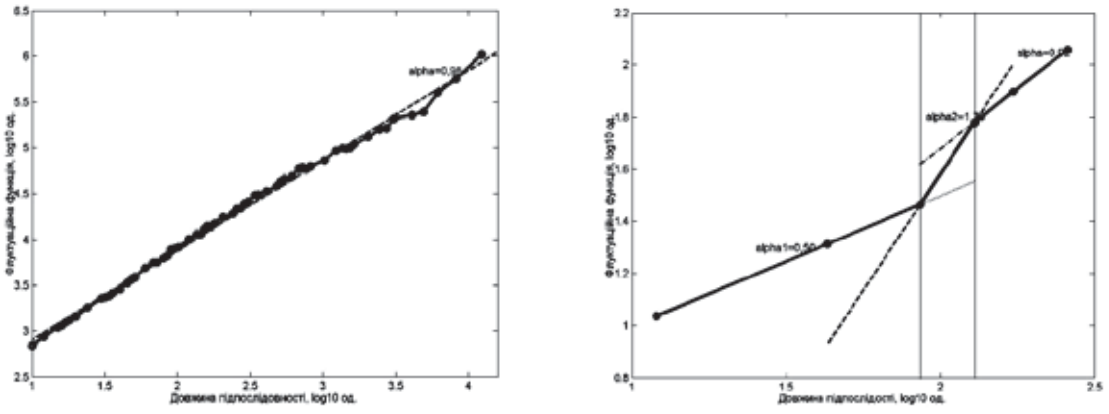
Таким чином, використання АДФ на малих часових інтервалах дозволяє визначити різні стани мережі та класифікувати її аномалії.

Сигнал трафіку в цілому виявив мультифрактальні властивості: його графіки скейлінгової експоненти та показника Гельдера є кривими лініями, що залежать від значення порядку, а спектр сингулярностей не є компактною множиною.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Обгрунтована методика комплексної оцінки характеристик самоподібного трафіка ІКМ, що включає час-частотний, статистичний, фрактальний і мультифрактальний аналізи, що дозволяє підвищити ймовірність визначення вторгнень для СВА за рахунок підвищення достовірності інформативних ознак самоподібного трафіка.

На прикладі експериментального сигналу трафіку мережі Ethernet проведений аналіз та визначені його характеристики.

Подальші дослідження мають бути спрямовані на розробку адекватних прогнозуючих моделей мережевого самоподібного трафіку для підвищення ефективності оперативного визначення вторгнень для СВА.



а *б*

Рис. 2. Показники скейлінга сигналу трафіка (*а*) та сигналу 1 (*б*)

ЛІТЕРАТУРА:

1. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН.* 2016. Вып. 2(45). С. 207–244. URL: www.proceedings.spiiras.nw.ru.

2. Носенко К.М., Півторак О.І., Ліхоузова Т.А. Огляд систем виявлення атак в мережевому трафіку. *Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління».* 2014. № 1(24). С. 67–75.

3. Лукова-Чуйко Н., Наконечний В., Толюпа С., Зюбіна Р. Проблеми захисту критично важливих об'єктів інфраструктури. *Безпека інформаційних систем і технологій.* 2020. № 1(2). С. 31–39.

4. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації.* 2019. № 1(37). С. 6–15.

5. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи. *Сучасний захист інформації*. 2015. № 1. С. 33–40.

6. Смирнов А., Дрейс Ю., Даниленко Д. Имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях. *Ukrainian Scientific Journal of Information Security.* 2014. Vol. 20. Issue 1. P. 29–35.

7. Радівілова Т.А., Кіріченко Л.О., Тавалбех М.Х., Ільков А.А. Виявлення аномалій в телекомунікаційному трафіку статистичними методами. *Кібербезпека: освіта, наука, техніка.* 2021. № 3 (11). С. 183–194.

8. Корнієнко В.І., Гусєв О.Ю., Герасіна О.В. Інтелектуальне моделювання нелінійних динамічних процесів у системах керування, кібербезпеки, телекомунікацій: підручник. Дніпро : НТУ «ДП», 2020. 536 с.

REFERENCES:

1. Branitskii A.A., Kotenko I.V. Analiz i klassifikatsiia metodov obnaruzheniia atak. *Trudy SPIIRAN.* 2016. Vyp. 2(45). S. 207–244. Access mode: www.proceedings.spiiras.nw.ru.

2. Nosenko K.M., Pivtorak O.I., Lichouzova T.A. Ogliad system vyiavlennia atak v merezhevomu trafiku. *Mizhvidomchii naukovo-technichnyi zbirnyk «Adaptyvni systemy avtomatychnogo upravlinnia»,* 2014, № 1(24). S. 67–75.

3. Lukova-Chuiko N., Nakonechnyi V., Toliupa S., Ziubina R. Problemy zachystu krytychno vazhlyvych ob`iektiv infrastruktury. *Bezpeka informatciinych system i technologii,* 2020, № 1(2). S. 31–39.

4. Dovbeshko S.V., Toliupa S.V., Shestak Ya.V. Zastosuvannia metodiv intelektualnogo analizu danych dlia pobudovy system vyiavlennia atak. *Suchasnyi zachyst informatsii.* 2019, № 1(37). S. 6–15.

5. Lazarenko S.V. Osoblyvosti funktsionuvannia system vyiavlennia atak na avtomatyzovani systemy. *Suchasnyi zachyst informatsii.* 2015, № 1. S. 33–40.

6. Smirnov A., Dreis Yu., Danylenko D. Smstatsionnaia model NIPDS dlia obnaruzheniia i predotvrascheniia vtorzhenii v telekommunikatsionnych sistemach i setiach. *Ukrainian Scientific Journal of Information Security*. 2014, vol. 20, issue 1, p. 29–35.

7. Radivilova T.A., Kirichenko L.O., Tavalbech M.Ch., Il`kov A.A. Vyiavlennia anomalii v telekommunikatsiinomu trafiku statystychnymy metodamy. *Kiberbezpeka: osvita, nauka, technika*. 2021, № 3 (11). S. 183–194.

8. Korniienko V.I., Husiev O.Yu., Herasina O.V. Intelektualne modeliuvannia neliniinych dynamichnych protsesiv u systemach keruvannia, kiberbezpeky, telekomunikatsii: pidruchnyk. Dnipro: NTU «DP», 2020. 536 s.