ТЕЛЕКОМУНІКАЦІЇ

УДК 004.056.5

КОМПЛЕКСНИЙ МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ, ЗАСНОВАНИЙ НА СТАТИСТИЧНОМУ ТА ДИНАМІЧНОМУ ПІДХОДАХ АНАЛІЗУ ТРАФІКА

РАДІВІЛОВА Т.А., ІЛЬКОВ А.А., ТАВАЛБЕХ М.Х.

Наводиться аналіз робіт, що пропонують можливі рішення проблеми ідентифікації атак, а також дається опис запропонованого комплексного методу, який дозволяє в онлайн режимі виявляти атаки. Запропонований комплексний метод порівнюється з існуючими методами виявлення вторгнень шляхом імітаційного моделювання, результати якого показали, що він краще виявляє атаки і має менше помилок спрацьовувань.

Ключові слова: система виявлення вторгнень; ентропійний аналіз; комплексний метод; атаки; машинне навчання; виявлення аномалій; метод поведінки; аналіз підписів.

Key words: Intrusion detection system; entropy analysis; complex method; attacks; machine learning; anomaly detection; behaviour method; signature analysis.

1. Вступ

Швидкий розвиток комп'ютерних мереж та інформаційних технологій породжує ряд проблем, пов'язаних з безпекою мережних ресурсів, які вимагають нових підходів. Кожна комп'ютерна система повинна бути захищена від зовнішніх та внутрішніх вторгнень. В області мережної безпеки вторгнення визначаються як набір зловмисних дій проти цілісності, конфіденційності та доступності інформації в системі або мережі, які роблять її вразливою для майбутніх атак. З метою протидії таким загрозам та забезпечення якості обслуговування використовують множину методів, розгортають системи виявлення вторгнень (СВВ) в систему або мережу [1-4]. Використовуючи набір апаратних і програмних ресурсів, СВВ намагається виявити вторгнення, відстежуючи дані, зібрані з одного хоста або мережі, і генерувати тривогу в разі виявлення спроб вторгнення. СВВ можна розділити на різні категорії залежно від джерела інформації і техніки виявлення [1,4,5].

В даний час актуальним напрямком в області інформаційних технологій є побудова систем виявлення вторгнень [1,6]. Існує багато робіт, присвячених темі виявлення та класифікації атак. Використовують різноманітні математичні методи, які включають традиційні підходи, засновані на відповідності шаблонів підписам, та адаптаційні моделі з використанням методів аналізу даних [5-8].

В роботі [1] автори пропонують технологію паралельної мережної СВВ, засновану на аналізі сигнатур для зменшення кількості відкинутих пакетів. Одним з недоліків підходів, заснованих на аналізі сигнатур, є необхідність використання множини ресурсів. Для усунення цього недоліку використовують підхід, заснований на аномаліях.

У статті [6] автори проаналізували три популярних інструменти мережної СВВ з відкритим вихідним кодом і представили свої порівняльні показники ефективності: Suricata, Snort і Bro. Вони також використали плагіни для Snort з різними алгоритмами зіставлення шаблонів, які зменшують кількість невиявлених атак до 0,5% і підвищують точність до 96%.

Автори [9] використали модульну та ієрархічну структуру СВВ. Запропоновано двоступеневу СВВ, яка використовує модуль виявлення аномалій на основі Spark ML і сигнатурний модуль виявлення на основі конволюційної мережі LSTM (Conv-LSTM), що забезпечує передбачувану точність 97,29%.

У статті [10] було порівняно продуктивність двох відкритих СВВ: Suricata та Snort. Для роботи також паралельно з набором правил Snort до стандартної системи додано алгоритм машинного навчання (англ. Support Vector Machine – SVM). Для SVM з алгоритмом Firefly зафіксовано середнє значення точності виявлення 95%.

У [11] описано методи виявлення вторгнень на основі підписів та аномалій. Автори також пропонують новий тип виявлення аномалій на основі стандартів протоколу. Автори статті [12] пропонують новий СВВ, заснований на аналізі ентропії бітів ідентифікаторів у повідомленнях мережі області контролера. В [13] автори поєднують два методи: ентропійного аналізу і аналізу аномалій для захисту системи від атак багаторівневої розподіленої відмови в обслуговуванні (DDoS). Автори [14] пропонують заснований на ентропії метод детектування сучасних ботнет-подібних шкідливих програм в мережі. В роботі [15] автори використовують ентропійний аналіз різних типів протоколів для виявлення деяких типів мережевих атак.

В статті [16] описано гібридне виявлення вторгнень, засноване на аналізі підписів та аномалій. Автори [17] моделюють систему виявлення вторгнень, засновану на глибокому навчанні. Пропонують підхід до глибокого навчання з використанням рекурентних нейронних мереж (PHH-IDS) для виявлення вторгнення. Автори [18] описують таксономію СВВ і досліджують методи машинного нав-

чання і глибокого навчання в СВВ для забезпечення безпеки.

Використання кожного методу індивідуально не забезпечує необхідного рівня ідентифікації атаки. Однак якщо методи застосовуються комплексно, ймовірність ідентифікації атаки значно збільшується.

Таким чином, *метою* дослідження є розробка комплексного методу, який поєднує підходи аналізу сигнатур, виявлення аномалій (машинне навчання) та підходи аналізу ентропії для виявлення вторгнень в інформаційно-комунікаційних мережах.

2. Методи виявлення вторгнень

Кожен з методів детектування атак має як недоліки, так і переваги. Існують підходи, які пропонують комбіноване використання деяких методів для поліпшення ефективності детектування атак [11,15,18,19]. У даній роботі пропонується метод виявлення вторгнень, який базується на комплексному використанні методів сигнатурного аналізу, аналізу аномалій протоколів та методів машинного навчання.

Якість роботи СВВ характеризується значеннями матриці помилок, рівнем виявлення (DR), рівнем помилкових спрацьовувань (FPR), точністю, повнотою, F-мірою [7, 20, 21]. Ці параметри можуть бути обчислені за параметрами матриці помилок: справжнє позитивне (TP), справжнє негативне (TN), помилкове позитивне (FP), помилкове негативне (FN).

Міра точності (Precision) характеризує, скільки позитивних відповідей, отриманих від класифікатора, є правильними. Чим вищеа точність, тим менше помилкових спрацьовувань:

$$\text{Precision} = \text{TP}/(\text{TP}+\text{FP})$$

Однак вимірювання точності не вказує на те, чи повернув класифікатор всі правильні відповіді. Для цього існує так звана міра повноти.

Міра повноти (Recall) характеризує здатність класифікатора «вгадувати» якомога більше позитивних відповідей з числа очікуваних. Однак хибнопозитивні відповіді ніяк не впливають на дану міру:

$$\text{Recall} = \text{TP}/(\text{TP}+\text{FN}).$$

Міра повноти показує, яка частка об'єктів, що належать до позитивного класу, була прогнозована правильно.

Загальним критерієм якості є F-міра. Точність і повнота добре оцінюють якість класифікатора для задач зі зміщеною раніше ймовірністю, але якщо ми навчили модель з високою точністю, може статися, що повнота такого класифікатора низька, і навпаки. Для встановлення важливості конкретної метрики розглядається параметрична F-міра:

$$\text{F}_\beta = (1+\beta^2)\frac{\text{Precision}\cdot\text{Recall}}{\beta^2\text{Precision}+\text{Recall}},$$

де $\beta \in [0,\infty)$, при $\beta = 0$ обчислюється точність, при $\beta < 1$ точність переважна, при $\beta = 1$ непараметрична F-міра переважна, при $\beta = \infty$ обчислюється повнота.

Щоб зв'язати точність з повнотою F-міра вводиться як середнє гармонійне значення точності і повноти:

$$\text{F}_\beta = \frac{2\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}}. \qquad (1)$$

Нехай P_b відображає ймовірність виявлення вторгнення під час роботи комплексного методу. У цьому випадку функція залежить від показників, що характеризують якість СВВ:

$$\text{P}_\text{b} = \text{f}\left(\text{Recall}, \text{Precision}, \text{F}_\beta, \text{DR}, \text{FPR}\right). \qquad (2)$$

Вибір одного або всіх параметрів функції f залежить від бажаного результату: FPR – це частка помилкових попереджень, скільки передбачень з усіх позитивних прогнозів були невірними, повнота зазвичай використовується сумісно з точністю. У цьому дослідженні використовувалась F-міра (1), тому що це гармонійне середнє повноти і точності. Чим більше значення F_β, тим краща наша модель.

Нехай $\text{A}_\text{b}^\text{i}, \text{i} = 1,2,3,...$ змінні, що позначають деякі порогові ймовірності виявлення вторгнень. Вибираючи потрібну функцію f і порогові значення виявлення вторгнень, можна варіювати налаштування роботи СВВ (кількість алармів, рівень спрацьовувань тривоги, рівень блокування, реагування на атаку). Функція f і значення параметрів $\text{A}_\text{b}^\text{i}$ встановлюються фахівцем з безпеки і залежать від необхідного рівня виявлення вторгнень або безпеки системи.

Ентропійний аналіз використовується для виявлення атак, щоб сформувати статистичний критерій для перевірки належності досліджуваного екземпляра до аномального класу [12, 13, 15, 22]. Ентропія трафіка залежить від ймовірності появи пакетів ω-го типу під час їх передачі. Суть методу максимуму ентропії полягає в побудові моделі, яка максимізує значення ентропії. Це відповідає припущенню, що зі збільшенням кількості унікальних записів вони рівномірно розподіляються між обраними класами, що призводить до збільшення ентропії.

Наш підхід ділиться на два етапи. Перша фаза полягає у вивченні базового розподілу, а друга фаза – у виявленні аномалій в спостережуваному трафіку.

В роботі ентропія трафіка даних обчислюється через ковзане вікно з фіксованою шириною T. Розмір вікна T є настроюваним параметром, який контролює, наскільки згладжування короткочасних коливань буде виконуватися детектором. Збільшення T зменшить відхилення в ентропії і може зменшити швидкість помилкових позитивних результатів, що виникають внаслідок незначних аномалій. Тим не менш, для швидкого виявлення атак розмір T повинен бути досить малим. Величина граничного значення розбіжності ентропій d також задається і є настроюваним параметром.

В роботі запропоновано використовувати метод аналізу сигнатур [16, 23], який засновано на глибокому аналізі пакетів (DPI) незашифрованого трафіка і відомих протоколів четвертого (транспортного рівня мережної моделі). DPI аналізує кожен пакет, і приймає рішення в режимі реального часу на основі бази даних відомих мережних атак, правил, визначених компанією, провайдером або мережним адміністратором. При виявленні сигнатури Sg_j в пакетах даних включається правило реагування на певний тип вторгнення $R = \{R_1, R_2, .., R_n\}$, інформація про вторгнення записується в базу даних.

Метод аналізу поведінки трафіка для ідентифікації атак засновано на використанні алгоритмів машинного навчання [24-26]. Як методи класифікації для машинного навчання були обрані методи дерев рішень (випадкового лісу) і нейронні мережі. Як ознаки були використані статистичні, фрактальні і рекурентні характеристики, розраховані за реалізаціями трафіка [3, 26-29].

На основі сумісного застосування методів аналізу поведінки трафіка, аналізу протоколів та сигнатурного аналізу запропоновано комплексний метод ідентифікації атак.

3. Комплексний метод виявлення вторгнень

У даній роботі ми встановили такі пороги:

$$A_b^1 = 0,9,\ A_b^2 = 0,7,\ A_b^3 = 0,5.$$

Автори робіт [7, 12, 19, 25, 27-29] показали, що ймовірність виявлення вторгнень, більша 90%, є практично точною ідентифікацією наявності атаки, $A_b^2 = 0,7$ вказує на те, що необхідний додатковий аналіз трафіка. Якщо ж ймовірність виявлення менша 50%, то це вказує на відсутність атаки. Схему роботи запропонованого комплексного методу представлено на рисунку.

База даних нормальної поведінки містить запис про нормальне функціонування мережі, тобто без атак. База даних протоколів містить правильні структури кожного протоколу. У базі даних сигнатур є всі сигнатури відомих атак. Блок запису в бази даних підписів, протоколів, поведінки відправляє в зазначені бази даних інформацію про знайдені атаки відповідно.

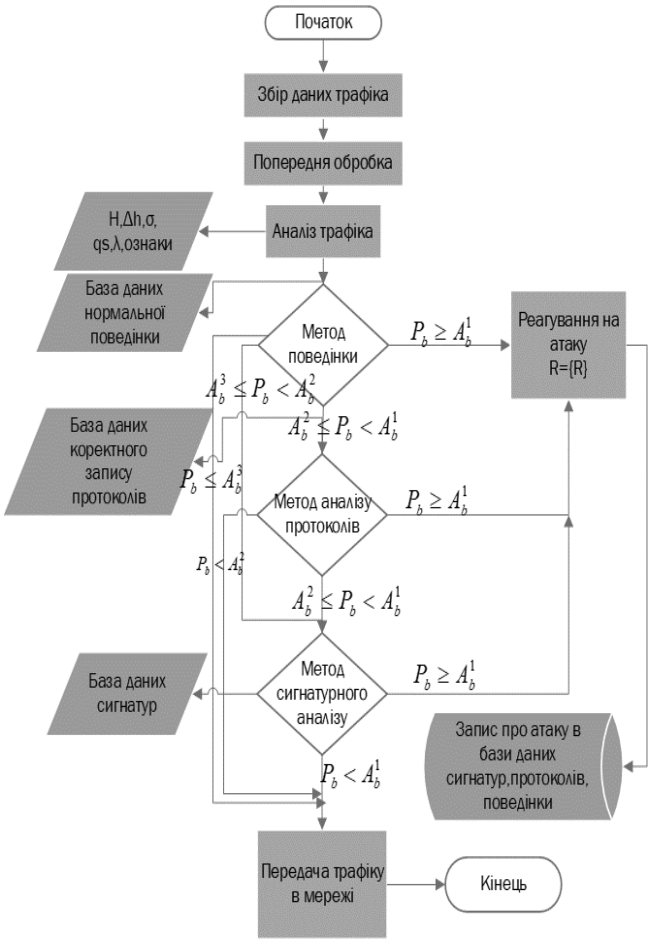

Схема роботи комплексного методу виявлення вторгень

Розглянемо роботу комплексного методу більш докладно.

Попередня обробка трафіка. На вхід детекторів надходить трафік, який вони захоплюють і відсилають на передобробку для приведення його в зручний вид для обробки і аналізу.

Далі трафік аналізується, вибираються його статистичні характеристики, ознаки, за якими він буде класифікуватися [28, 29]. В ході роботи як ознаки та характеристики трафіка використовувались його інтенсивність, якість обслуговування, самоподібні параметри, які впливають на ідентифікацію атак.

Метод поведінки. Далі трафік відсилається на аналіз методом поведінки.

1. При $P_b \ge A_b^1$ метод поведінки відправляє трафік в підсистему реагування на атаки (або видаляє його) і записує данні про атаку в базу даних атак.

2. При $A_b^2 \le P_b < A_b^1$ трафік відправляється на аналіз методом аналізу протоколів.

3. При $A_b^3 \le P_b < A_b^2$ трафік відправляється на аналіз методом сигнатурного аналізу, минаючи метод аналізу протоколів.

4. При $P_b < A_b^3$ трафік без всяких додаткових перевірок відправляється далі в мережу.

Метод аналізу протоколів. Трафік, який був переданий на вхід методу аналізу протоколів, проходить такі кроки:

1. При $P_b \ge A_b^1$ метод аналізу протоколів відправляє трафік в підсистему реагування на атаки (або видаляє його) і записує дані про цю атаку в базу даних атак.

2. При $A_b^2 \le P_b < A_b^1$ трафік відправляється на аналіз методом сигнатурного аналізу.

3. При $P_b < A_b^2$ трафік без всяких додаткових перевірок відправляється далі в мережу.

Метод сигнатурного аналізу. Трафік, що надійшов на вхід методу сигнатурного аналізу, обробляється і порівнюється з існуючими сигнатурами атак.

1. При $P_b \ge A_b^1$ метод сигнатурного аналізу відправляє трафік в підсистему реагування на атаки (або видаляє його) і записує дані про цю атаку в базу даних атак.

3. При $P_b < A_b^1$ трафік відправляється далі в мережу.

Далі трафік передається всередині мережі відповідно до встановлених правил обробки і передачі.

4. Результати експериментів роботи комплексного методу

Проведено аналіз роботи комплексного методу виявлення вторгнень, який об'єднує три методи детектування атак. Реальний трафік був узятий з [30, 31] репозиторіїв. Моделювання реалізації трафіка здійснювалося за алгоритмом, описаним в [26, 29]. За атаки приймалися реалізації шести типів: DDoS-атаки, Brute Force, UDP-flood, потоки TCP SYN, Ping of Death, HTTP-flood. Для проведення експериментів трафік був розділений на групи за типом інтерфейсу і протоколу і складався з 170 тисяч записів (більше 1го мільйона пакетів). У даній роботі був проведений аналіз протоколів на основі TCP і UDP.

Для оцінки якості роботи методу комплексного виявлення атаки була розгорнута віртуальна мережа, в якій трафік передавався з п'яти джерел на сервер ідентифікації атаки. Було використано програмне забезпечення Python для проведення експериментів шляхом підключення бібліотек, що реалізують статистичний аналіз і методи машинного навчання. Для аналізу сигнатур трафіка використовувалася СВВ Suricata. Весь трафік в мережі відстежувався і оброблявся на сервері як в режимі реального часу, так і шляхом автономної обробки раніше захопленого мережного трафіка. Це дозволило аналізувати трафік з різних джерел різної інтенсивності і розставляти пріоритети для його обробки. Модуль аналізу поведінки, що використовує методи машинного навчання, виконаний у вигляді плагінів, які транслюють отриманий трафік в часові ряди, обчислюють і аналізують властивості отриманих часових рядів, видають повідомлення і записують результати аналізу в лог-файли для збору поведінкової статистики. Це значно скорочує час на виявлення атак. Модуль аналізу ентропії був побудований як плагін, який отримує кожну IP-датаграму з відкритої бібліотеки WinCap і обробляє її. Це дозволило знову збирати потік даних і виконувати подальші маніпуляції з пакетами. Він також видає повідомлення і записує дані в лог-файли детектора ентропії з метою періодичного обчислення її значень для кожного атрибута пакета, зазначеного в файлі ініціалізації (наприклад, TCP/UDP порти, IP адреси джерела і одержувача, розмір вікна TCP і довжина датаграми). Це дозволило поліпшити настройку сигналів тривоги шляхом ручної або автоматичної настройки детектора.

Експерименти з навчання моделі для кожного типу атаки були проведені на 1000 прикладах трафіка по 120 секунд тривалості кожен. Тестування запропонованого комплексного методу проводилось на 100 тестових прикладах для комбінації різних типів атак.

В таблиці представлено показники якості роботи запропонованого комплексного методу та існуючих комплексних методів, запропонованих іншими дослідниками. Результати роботи даного комплексного методу збігаються з результатами, отриманими іншими дослідниками [1, 7, 9, 10, 22, 23, 32].

Для аналізу якості роботи запропонованого комплексного методу ідентифікації атак використовувались такі показники ефективності СВВ: відсоток виявлених атак; відсоток атак, які не були виявлені; відсоток втрачених даних від загальної кількості отриманих даних, відсоток помилкових спрацьовувань (FN+TN), F-міра.

При порівнянні якості роботи запропонованого комплексного методу виявлення вторгнень з існу-

ючими комплексними методами визначено, що запропонований метод на 1-3% краще ідентифікує атаки, при цьому відсоток невиявлених атак менший на 2-5%, помилкових спрацьовувань менше на 2% та час ідентифікації атак відносно однаковий при роботі існуючих методів.

	Khan [29]	Shah [30]	Hu [7]	Запропонований комплексний метод
Відсоток $*10^{-1}$ виявлених атак	9.7	9.7	9.5	9.8
Відсоток невиявлених атак	0.3	0.3	0.5	0.2
Відсоток втрачених даних	7	3.2	9.8	3.2
Відсоток помилкових спрацьовувань	0.71	3.2	1.7	1.6
F1 міра	0.973	0.953	0.944	0.98

5. Висновки

Досліджено проблему виявлення вторгнень в інфокомунікаційних мережах. Розроблено комплексний метод виявлення вторгнень, який базується на об'єднаному застосуванні методів аналізу поведінки трафіка, ентропійному аналізі протоколів та сигнатурному аналізі. Проведено імітаційне моделювання запропонованого методу і порівняльний аналіз результатів його роботи та інших існуючих методів за показниками відсотка виявлених атак, невиявлених атак, втрачених даних, помилкових спрацьовувань при ідентифікації атак та комплексному показнику F-міри. Результати імітаційного моделювання роботи запропонованого комплексного методу показали, що запропонований метод більш якісно ідентифікує атаки та має меншу кількість помилкових спрацьовувань.

В подальшому планується дослідження роботи комплексного методу при різній інтенсивності вхідного навантаження.

Література: 1. *Bulajoul W.* Network intrusion detection systems in high-speed traffic in computer networks / W. Bulajoul, A. James, M. Pannu // Proceeding of 10th International Conference on E-Business Engineering (ICEBE), IEEE, 2013. P. 168-175. doi: 10.1109/ICEBE.2013.26. **2.** *Semenova O.* Access fuzzy controller for CDMA networks / O. Semenova, A. Semenov, K. Koval, A. Rudyk, V. Chuhov // Proceeding of 2013 International Siberian Conference on Control and Communications (SIBCON), IEEE, 2013. P. 1-2. doi: 10.1109/SIBCON.2013.6693644. **3.** *Bulakh V.* Time Series Classification Based on Fractal Properties / V. Bulakh, L. Kirichenko, T. Radivilova // Proceeding of 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Ukraine, 2018. P. 198-201. doi: 10.1109/DSMP.2018.8478532. **4.** *Matuszewski J.* Neural network application for emitter identification / J. Matuszewski, K. Sikorska-Łukasiewicz // Proceeding of 2017 18th International Radar Symposium (IRS), Prague, 2017. P. 1-8. doi: 10.23919/IRS.2017.8008202. **5.** *Jacob N. M.* A Review of Intrusion Detection Systems / N. M. Jacob, M. Y. Wanjala // Global Journal of Computer Science and Technology. 2017. Vol. 17, №3. C. **6.** *Hu Q.* Evaluating network intrusion detection systems for high-speed networks / Q. Hu, M. R. Asghar, N. Brownlee // Proceeding of 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, 2017. P. 1-6. doi: 10.1109/ATNAC.2017.8215374. **7.** *Radivilova T.* Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise / T. Radivilova and H. A. Hassan // Proceeding of 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa. IEEE, 2017. P. 1-4. doi: 10.1109/UkrMiCo.2017.8095429. **8.** *Radivilova T.* Classification Methods of Machine Learning to Detect DDoS Attacks / T. Radivilova, L. Kirichenko, D. Ageiev, V. Bulakh // Proceeding of 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019. P. 207-210. doi: 10.1109/IDAACS.2019.8924406. **9.** *Khan M. A.* A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network / M. A. Khan, M. R. Karim, Y. A. Kim // Symmetry. 2019. Vol. 11. P. 581-585. doi: 10.3390/sym11040583. **10.** *Shah S. A. R.* Performance comparison of intrusion detection systems and application of machine learning to Snort system / S. A. R. Shah, B. Issac // Future Generation Computer Systems. 2018. Vol.80. P. 157-170. doi: https://doi.org/10.1016/j.future.2017.10.016. **11.** *Das K.* Protocol Anomaly Detection for Network-based Intrusion Detection. SANS Institute. Information Security Reading Room, 2002. 9 p. **12.** *Wang Q.* An Entropy Analysis Based Intrusion Detection System for Controller Area Network in Vehicles / Q. Wang, Z. Lu, G. Qu // Proceeding of 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, 2018. P. 90-95. doi: 10.1109/SOCC.2018.8618564. **13.** *Navaz A. S.* Entropy based anomaly detection system to prevent DDoS attacks in cloud / A. S. Navaz, V. Sangeetha, C. Prabhadevi // [Online]. Available at: arXiv preprint arXiv:1308.6745. 2013. **14.** *Bereziński P.* An entropy-based network anomaly detection method / P. Bereziński, J. Bartosz, M. Szpyrka // Entropy. 2015. Vol. 17(4). P. 2367-2408. **15.** *Radivilova T.* Entropy Analysis Method for Attacks Detection / T. Radivilova, L. Kirichenko, A. S. Alghawli // Proceeding of 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology

(PIC S&T), Kyiv, Ukraine, 2019. P. 443-446. doi: 10.1109/PICST47496.2019.9061451. **16.** *Kumar R.* Signature-Anomaly Based Intrusion Detection Algorithm / R. Kumar, D. Sharma // Proceeding of 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018. P. 836-841. doi: 10.1109/ICECA.2018.8474781. **17.** *Yin C.* A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks / C. Yin, Y. Zhu, J. Fei, X. He // IEEE Access. 2017. Vol. 5. P. 21954-21961. doi: 10.1109/ACCESS.2017.2762418. **18.** *Liu H.* Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey / H. Liu, B. Lang // Applied Sciences. 2019. Vol.9 P. 4396. doi:10.3390/app9204396. 19. *Sandosh S.* Complex Event Processing Over Intrusion Detection System: A Comprehensive Discussion / S. Sandosh, V. Govindasamy, G. Akila, A. Jeraldine, D. Mithunkala, V. MohannaKasturi // Proceeding of 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019. P. 1-6. **20.** *Ulvila J. W.* Evaluation of Intrusion Detection Systems / J. W. Ulvila, J. E. Gaffney // Journal of research of the National Institute of Standards and Technology. 2003. Vol. 108(6). P. 453-473. doi:10.6028/jres.108.040. **21.** *Kumar G.* Evaluation Metrics for Intrusion Detection Systems – A Study // International Journal of Computer Science and Mobile Applications. 2014. Vol.2, iss. 11. P. 11-17. **22.** *Gu Y.* Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation / Y. Gu, A. McCallum, D. Towsley // Proceeding of 5th ACM SIGCOMM conference on Internet Measurement, 2005, pp. 32–32. **23.** *Almutairi A. H.* Innovative signature based intrusion detection system: Parallel processing and minimized database / A. H. Almutairi, N. T. Abdelmajeed // Proceeding of 2017 International Conference on the Frontiers and Advances in Data Science (FADS), Xi'an, 2017. P. 114-119. doi: 10.1109/FADS.2017.8253208. **24.** *Kirichenko L.* Binary Classification of Fractal Time Series by Machine Learning Methods / L. Kirichenko, T. Radivilova, V. Bulakh // In Eds.: V. Lytvynenko, S. Babichev, W. Wojcik, O. Vynokurova, S. Vyshemyrskaya, S. Radetskaya. Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2019. Advances in Intelligent Systems and Computing. 2020. Vol. 1020. P. 701-711. doi: https://doi.org/10.1007/978-3-030-26474-1_49. **25.** *Liu X.* Detecting Anomaly in Traffic Flow from Road Similarity Analysis / X. Liu, Y. Wang, J. Pu, X. Zhang // In Eds.: B. Cui, N. Zhang, J. Xu, X. Lian, D. Liu // Web-Age Information Management. WAIM 2016. Lecture Notes in Computer Science. 2016. Vol. 9659. P. 92-104. doi: https://doi.org/10.1007/978-3-319-39958-4_8. **26.** *Kirichenko L.* Machine Learning in Classification Time Series with Fractal Properties / L. Kirichenko, T. Radivilova, V. Bulakh // Data. 2019. Vol.4, issue 1, 5. P. 1-13. doi: 10.3390/data4010005. **27.** *Cuadra-Sánchez A.* Traffic Anomaly Detection / A. Cuadra-Sánchez, J. Aracil // Elsevier, 2015. 70 p. **28.** *Alazzam H.* A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer / H. Alazzam, A. Sharieh, K. E. Sabri // Expert Systems with Applications. 2020. Vol. 148. P. 113249. doi: https://doi.org/10.1016/j.eswa.2020.113249. **29.** *Ivanisenko I.* Investigation of multifractal properties of additive data stream / I. Ivanisenko, L. Kirichenko, T. Radivilova // 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, 2016. P. 305-308. doi: 10.1109/DSMP.2016.7583564. **30.** *Al-Kasassbeh M.* Towards generating realistic SNMP-MIB dataset for network anomaly detection / M. Al-Kasassbeh, G. Al-Naymat, E. Al-Hawari // International Journal of Computer Science and Information Security. 2016. Vol. 14, №9. P. 1162–1185. **31.** *GitHub*. 2020. Ddos-Attack. [online] Available at: https://github.com/Ha3MrX/DDos-Attack. [Accessed 02 April 2020]. **32.** *Dromard J.* Online and Scalable Unsupervised Network Anomaly Detection Method / J. Dromard, G. Roudière, P. Owezarski // IEEE Transactions on Network and Service Management. 2014. Vol. 14, №1. P. 34-47. doi: 10.1109/TNSM.2016.2627340.

Транслітерований список літератури:

1. *Bulajoul W.* Network intrusion detection systems in high-speed traffic in computer networks / W. Bulajoul, A. James, M. Pannu // Proceeding of 10th International Conference on E-Business Engineering (ICEBE), IEEE, 2013. P. 168-175. doi: 10.1109/ICEBE.2013.26.

2. *Semenova O.* Access fuzzy controller for CDMA networks / O. Semenova, A. Semenov, K. Koval, A. Rudyk, V. Chuhov // Proceeding of 2013 International Siberian Conference on Control and Communications (SIBCON), IEEE, 2013. P. 1-2. doi: 10.1109/SIBCON.2013.6693644.

3. *Bulakh V.* Time Series Classification Based on Fractal Properties / V. Bulakh, L. Kirichenko, T. Radivilova // Proceeding of 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Ukraine, 2018. P. 198-201. doi: 10.1109/DSMP.2018.8478532.

4. *Matuszewski J.* Neural network application for emitter identification / J. Matuszewski, K. Sikorska-Łukasiewicz // Proceeding of 2017 18th International Radar Symposium (IRS), Prague, 2017. P. 1-8. doi: 10.23919/IRS.2017.8008202.

5. *Jacob N. M.* A Review of Intrusion Detection Systems / N. M. Jacob, M. Y. Wanjala // Global Journal of Computer Science and Technology. 2017. Vol. 17, №3-C.

6. *Hu Q.* Evaluating network intrusion detection systems for high-speed networks / Q. Hu, M. R. Asghar, N. Brownlee // Proceeding of 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, 2017. P. 1-6. doi: 10.1109/ATNAC.2017.8215374.

7. *Radivilova T.* Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise / T. Radivilova and H. A. Hassan // Proceeding of 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa. IEEE, 2017. P. 1-4. doi: 10.1109/UkrMiCo.2017.8095429.

8. *Radivilova T.* Classification Methods of Machine Learning to Detect DDoS Attacks / T. Radivilova, L. Kirichenko, D. Ageiev, V. Bulakh // Proceeding of 2019

10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019. P. 207-210. doi: 10.1109/IDAACS.2019.8924406.
9. *Khan M. A.* A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network / M. A. Khan, M. R. Karim, Y. A. Kim // Symmetry. 2019. Vol. 11. P. 581-585. doi: 10.3390/sym11040583.
10. *Shah S. A. R.* Performance comparison of intrusion detection systems and application of machine learning to Snort system / S. A. R. Shah, B. Issac // Future Generation Computer Systems. 2018. Vol.80. P. 157-170. doi: https://doi.org/10.1016/j.future.2017.10.016.
11. *Das K.* Protocol Anomaly Detection for Network-based Intrusion Detection. SANS Institute. Information Security Reading Room, 2002. 9 p.
12. *Wang Q.* An Entropy Analysis Based Intrusion Detection System for Controller Area Network in Vehicles / Q. Wang, Z. Lu, G. Qu // Proc. of 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA. 2018. P. 90-95. doi: 10.1109/SOCC.2018.8618564.
13. *Navaz A. S.* Entropy based anomaly detection system to prevent DDoS attacks in cloud / A. S. Navaz, V. Sangeetha, C. Prabhadevi // [Online] Available at: arXiv preprint arXiv:1308.6745. 2013.
14. *Bereziński P.* An entropy-based network anomaly detection method / P. Bereziński, J. Bartosz, M. Szpyrka // Entropy. 2015. Vol. 17(4). P. 2367-2408.
15. *Radivilova T.* Entropy Analysis Method for Attacks Detection / T. Radivilova, L. Kirichenko, A. S. Alghawli // Proceeding of 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 2019. P. 443-446. doi: 10.1109/PICST47496.2019.9061451.
16. *Kumar R*. Signature-Anomaly Based Intrusion Detection Algorithm / R. Kumar, D. Sharma // Proc. of 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018. P. 836-841. doi: 10.1109/ICECA.2018.8474781.
17. *Yin C.* A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks / C. Yin, Y. Zhu, J. Fei, X. He // IEEE Access. 2017. Vol. 5. P. 21954-21961. doi: 10.1109/ACCESS.2017.2762418.
18. *Liu H.* Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey / H. Liu, B. Lang // Applied Sciences. 2019. Vol.9 P. 4396. doi:10.3390/app9204396.
19. *Sandosh S.* Complex Event Processing Over Intrusion Detection System: A Comprehensive Discussion / S. Sandosh, V. Govindasamy, G. Akila, A. Jeraldine, D. Mithunkala, V. MohannaKasturi // Proceeding of 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019. P. 1-6.
20. *Ulvila J. W*. Evaluation of Intrusion Detection Systems / J. W. Ulvila, J. E. Gaffney // Journal of research of the National Institute of Standards and Technology. 2003. Vol. 108(6). P. 453-473. doi:10.6028/jres.108.040.
21. *Kumar G.* Evaluation Metrics for Intrusion Detection Systems – A Study // International Journal of Computer Science and Mobile Applications. 2014. Vol.2, iss. 11. P. 11-17.
22. *Gu Y.* Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation / Y. Gu, A. McCallum, D. Towsley // Proceeding of 5th ACM SIGCOMM conference on Internet Measurement, 2005, pp. 32–32.
23. *Almutairi A. H.* Innovative signature based intrusion detection system: Parallel processing and minimized database / A. H. Almutairi, N. T. Abdelmajeed // Proceeding of 2017 International Conference on the Frontiers and Advances in Data Science (FADS), Xi'an, 2017. P. 114-119. doi: 10.1109/FADS.2017.8253208.
24. *Kirichenko L.* Binary Classification of Fractal Time Series by Machine Learning Methods / L. Kirichenko, T. Radivilova, V. Bulakh // In Eds.: V. Lytvynenko, S. Babichev, W. Wojcik, O. Vynokurova, S. Vyshemyrskaya, S. Radetskaya. Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2019. Advances in Intelligent Systems and Computing. 2020. Vol. 1020. P. 701-711. doi: https://doi.org/10.1007/978-3-030-26474-1_49.
25. *Liu X.* Detecting Anomaly in Traffic Flow from Road Similarity Analysis / X. Liu, Y. Wang, J. Pu, X. Zhang // In Eds.: B. Cui, N. Zhang, J. Xu, X. Lian, D. Liu // Web-Age Information Management. WAIM 2016. Lecture Notes in Computer Science. 2016. Vol. 9659. P. 92-104. doi: https://doi.org/10.1007/978-3-319-39958-4_8.
26. *Kirichenko L.* Machine Learning in Classification Time Series with Fractal Properties / L. Kirichenko, T. Radivilova, V. Bulakh // Data. 2019. Vol.4, issue 1, 5. P. 1-13. doi: 10.3390/data4010005.
27. *Cuadra-Sánchez A.* Traffic Anomaly Detection / A. Cuadra-Sánchez, J. Aracil // Elsevier, 2015. 70 p.
28. *Alazzam H.* A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer / H. Alazzam, A. Sharieh, K. E. Sabri // Expert Systems with Applications. 2020. Vol. 148. P. 113249. doi: https://doi.org/10.1016/j.eswa.2020.113249.
29. *Ivanisenko I.* Investigation of multifractal properties of additive data stream / I. Ivanisenko, L. Kirichenko, T. Radivilova // 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, 2016. P. 305-308. doi: 10.1109/DSMP.2016.7583564.
30. *Al-Kasassbeh M.* Towards generating realistic SNMP-MIB dataset for network anomaly detection / M. Al-Kasassbeh, G. Al-Naymat, E. Al-Hawari // International Journal of Computer Science and Information Security. 2016. Vol. 14, №9. P. 1162–1185.
31. *GitHub*. 2020. Ddos-Attack. [online] Available at: https://github.com/Ha3MrX/DDos-Attack. [Accessed 02 April 2020].
32. *Dromard J.* Online and Scalable Unsupervised Network Anomaly Detection Method / J. Dromard, G. Roudière, P. Owezarski // IEEE Transactions on Network and Service Management. 2014. Vol. 14, №1. P. 34-47. doi: 10.1109/TNSM.2016.2627340.

Надійшла до редколегії 12.05.2020
Рецензент: д-р техн. наук, проф. Толюпа С.В.

Радівілова Тамара Анатоліївна, канд. техн. наук, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського, ХНУРЕ. Наукові інтереси: інформаційна безпека, виявлення аномалій, управління трафіком, фрактальний аналіз, телекомунікаційні системи. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 380577021320, e-mail: tamara.radivilova@gmail.com.

Ільков Андрій Анатолійович, старший помічник начальника навчального відділу, ХНУПС ім. І.Кожедуба. Наукові інтереси: інформаційна безпека, радіолокація, радіоелектронні системи, ідентифікація вторгнень. Адреса: Україна, 61023, Харків, вул. Сумська 77/79, тел. +380577049645, e-mail: andreyilkov428@gmail.com.

Тавалбех Максим Хаджем, аспірант кафедри інфокомунікаційної інженерії ім. В.В. Поповського, ХНУРЕ. Наукові інтереси: телекомунікаційні системи, інформаційна безпека, маршрутизація, якість обслуговування, управління трафіком. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. +380577021320, e-mail: tavalbeh@icloud.com.

Radivilova Tamara, Ph.D., ass.professor, ass.professor at V.V. Popovskyy department of infocommunication engineering, Kharkiv National University of Radio Electronics. Research interests: information security, anomaly detection, traffic engineering, fractal analysis, telecommunication system. Address: Ukraine, 61166, Kharkiv, Nauka Ave., 14, Phone/fax: +380577021320, e-mail: tamara.radivilova@gmail.com.

Ilkov Andrii, senior assistant of the head of educational department, Ivan Kozhedub Kharkiv National Air Force University. Research interests: information security, radiolocation, radioelectronic systems, intrusion detection. Address: Ukraine, 61023, Kharkiv, Sumska St., 77/79, Phone/fax: +380577049645, e-mail: andreyilkov428@gmail.com.

Tawalbeh Maxim, postgraduate student at V.V. Popovskyy department of infocommunication engineering, Kharkiv National University of Radio Electronics. Research interests: telecommunication system, information security, routing, quality of service, traffic engineering. Address: Ukraine, 61166, Kharkiv, Nauka Ave., 14, Phone/fax: +380577021320, e-mail: tavalbeh@icloud.com.