УДК 004.056.5

Корченко А.О.
Національний авіаційний університет

Іванченко Є.В.
Національний авіаційний університет

Погорелов В.В.
Національний авіаційний університет

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЕКСПЕРТНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА БАЗІ НЕЧІТКОЇ ЛОГІКИ

Стаття присвячена вирішенню завдання доведення ефективності експертної системи виявлення вторгнень на базі нечіткої логіки. Обґрунтовано можливість експериментального оцінювання ефективності системи виявлення на основі похибки розпізнавання та її функціональних можливостей. Наведено опис і результати експериментальних досліджень, спрямованих на виявлення різних типів спуфінг-атак. Показано, що стосовно відомих систем виявлення вторгнень запропонована система дає змогу в 1,1–1,2 рази зменшити похибку розпізнавання та розширити номенклатуру аномальних станів. Визначено, що напрями подальших досліджень полягають в адаптації рішень, використаних під час розроблення експертної системи виявлення вторгнень для створення методу визначення номенклатури вхідних параметрів нейромережевої системи виявлення комп'ютерних вірусів.

Ключові слова: *система виявлення вторгнень, кібератака, спуфінг, експертна система, нечітка логіка.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій, ускладнення й поширеність шкідливого програмного забезпечення зумовлюють зниження ефективності класичних систем захисту ресурсів інформаційних систем, що базуються на явних алгоритмічних механізмах розпізнавання кіберзагроз. Варто зазначити, що несанкціоновані дії щодо ресурсів інформаційних систем впливають і на середовище оточення, породжуючи в ньому так звані аномалії. Таке середовище зазвичай гетерогенне, нечітко визначене, і для вирішення завдань виявлення кібератак, що породили аномалії в цьому середовищі, необхідні відповідні системи виявлення вторгнень, які дають можливість виявити вторгнення за безліччю різних характерних ознак, включаючи їх динамічний складник, контрольований у реальному режимі часу. Більшість поширених систем виявлення вторгнень ґрунтуються на математичних методах, реалізація яких вимагає тривалого підготовчого етапу. Такий підготовчий етап найчастіше пов'язаний із накопиченням статистичних даних. Варто також зазначити, що вся статистика про систему буде тоді, коли вона припинить своє існування в тому вигляді, в якому вона досліджувалася, але потреба в ній уже буде відсутня. Більш ефективні в цьому стосунку є експертні методи, які використовують математичний апарат нечіткої логіки [1].

У зв'язку з цим актуальним завданням є розроблення експертної системи виявлення вторгнень, яка базується на апараті нечіткої логіки (далі – ЕСОВ).

Аналіз останніх досліджень і публікацій. У результаті аналізу літературних даних [1–4] визначено, що основою для побудови та розширення функціональності ЕСОВ може бути вдосконалена методологія виявлення аномалій, породжених кібератаками в інформаційних системах. Методологія досить докладно представлена в роботі [2]. У її основі закладено логіко-лінгвістичний підхід [3] і кортежна модель [3; 4]. Удосконалення полягають у використанні методів, розроблених авторами:

– формування лінгвістичних еталонів [5–8];

– фазифікації параметрів на лінгвістичних стандартах [9];

– α-рівневої номіналізації нечітких чисел [10];

– визначення ідентифікувальних термів [11];

– формування базових детекційних правил [12].

Базовий механізм пропонованої методології ґрунтується на семи етапах:

1. Формування атакуючих середовищ;

2. Побудова m_i-мірного параметричного підсередовища;

3. Формування $m_i i$-мірних еталонних підсередовищ;

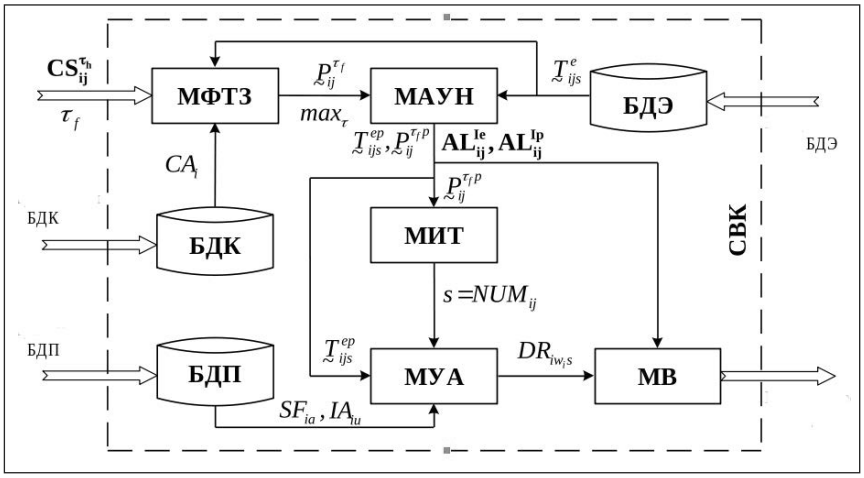

Рис. 1. Структурна схема ЕСОВ

4. Формування $m_i i$-мірних поточних підсередовищ (фазифікації);

5. α-рівнева номіналізація еталонних поточних підсередовищ;

6. Визначення ідентифікувальних термів;

7. Формування детекційних середовищ.

Також відзначимо, що в працях [1–4] визначена загальна структура такої ЕСОВ. Водночас потрібне проведення досліджень, пов'язаних з оцінюванням її ефективності, щодо подібних наявних систем. Відповідно до робіт [1; 7], у першому наближенні ефективність систем виявлення вторгнень можна оцінити на основі похибки розпізнавання та функціональних можливостей таких систем.

Постановка завдання. Мета статті – проведення досліджень, пов'язаних із доведенням ефективності експертної системи виявлення вторгнень на базі нечіткої логіки.

Виклад основного матеріалу дослідження. Відповідно до згаданої методології, основними структурними блоками ЕСОВ є:

– бази даних кібератак (далі – БДК),

– бази даних правил виявлення кібератак (далі – БДП),

– бази даних еталонів кібератак (далі – БДЕ),

– модуль формування поточних значень (далі – МФПЗ),

– модуль здійснення k-рівневої номіналізації (далі – МЗН),

– модуль пошуку ідентифікувальних умов (далі – МІУ),

– модуль визначення рівня аномальності (далі – МУА),

– модуль візуалізації (далі – МВ).

Структура ЕСОВ здображена на рис. 1.

БДК містить безліч ідентифікаторів (ВД) кібератак $CA_i \left(i = \overline{1,n}\right)$ (див. (1) в [3]), за допомогою яких здійснюється однозначне визначення атаки в процесі присвоєння її імені конкретного ВД (див. етап 1 в [2]).

БДП складається із бінарних вирішальних функцій $SF_{ia} \left(i = \overline{1,n}, a = \overline{1,w_i}\right)$ див. (15) в [12]) та ідентифікаторів аномальності $IA_{iu} \left(i = \overline{1,n}, u = \overline{1,v_i}\right)$ (див. (5) в [12]), які входять в множину базових правил $DR_i \left(i = \overline{1,n}\right)$ (див. (21) в [12]), які, в свою чергу, необхідні для виявлення і-ї кібератаки за посередництва параметричних підсередовищ різної розмірності (див. етап 7 в [2]).

БДЕ містить множину лінгвістичних еталонів $T_{ijs}^{ep} \left(i = \overline{1,n}, j = \overline{1,m_i}, s = \overline{1,r_j}\right)$ (див. (29) в [5]), які призначені для відображення стану множини відповідних параметрів $P_i \left(i = \overline{1,n}\right)$ в певному середовищі оточення, які направлені на виявлення кібератаки з ІД CA_i (див. етап 3 в [2]).

Відмітимо, що БДК, БДП та БДЕ повинні бути узгоджені по параметрах кібератак.

Модуль МФПЗ призначений для формування всіх можливих поточних значень нечітких параметрів $P_{ij}^{t_f} \left(i = \overline{1,n}, j = \overline{1,m_i}\right)$ (див. етап 2 в [2]), що отримуються за посередництва $T_i^e \left(i = \overline{1,n}\right)$ в певний момент часу t_f в заданому проміжку, тривалість якого становить $t_h = t_f - t_{f-1} \left(f = \overline{1,max_t}\right)$ [3].

З допомогою модуля МЗН відбуваються еквівалентні перетворення нечітких чисел (НЧ) через приведення всіх еталонних T_{ijs}^e і поточних $P_{ijs}^{t_f} \left(i = \overline{1,n}, j = \overline{1,m_i}, s = \overline{1,r_j}\right)$ до номінального (єдиного для всіх) числа компонент на основі підмножин α-рівневих інтервалів AL_{ij}^{Ie} і міжточкових α-рівневих інтервалів AL_{ij}^{Ip} (див. етап 5 в [2]) [10].

Модуль МІТ орієнтований на пошук по заданій лінгвістичній змінній, що ідентифікує еталонного

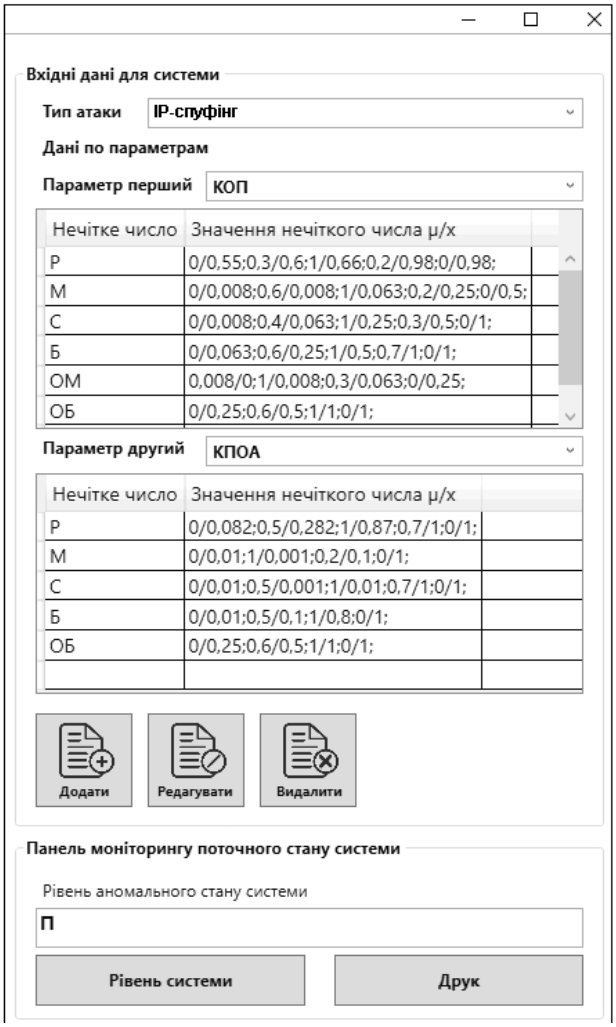

Рис. 2. Вікно введення початкових даних під час розпізнавання IP-спуфінгу

терма (тобто його номер, а $s = NUM_{ij}$), по якому за допомогою детекційних правил можна визначити рівень аномального стану, характерного для певного типу кібератак.

Модуль МІТ необхідній для формування DR_{iws} на основі ідентифікації еталонного терма (використання NUM_{ij}), еталонного перетвореного НЧ T_{ijs}^{ep}, а також ідентифікаторів аномальність IA_{iu} і бінарних вирішальних функцій SF_{ia}, за допомогою обробки підмножин умовних детекціонних виразів

$$DR_i = \left\{ \sum_{a=1}^{Wi} \left(\sum_{u=1}^{Vi} if\, SF_{ia} then IA_{iu} \right) \right\} \left(i = \overline{1,n}, \overline{1,w_i}, \overline{1,v_i} \right),$$

які відображають формування базових правила для виявлення і-ї кібератаки з використанням параметричних підсередовищ різної розмірності.

Модуль МВ використовується для графічної інтерпретації поліпараметричного мультирозмірнго середовища, розподілу ідентифікаторів атакуючих дій і фазифікованих значень поточних параметрів fpij ~ Pi щодо лінгвістичних еталонів T_{ijs}^{ep} у вигляді виявленої області, що характеризує атаки, а також відображення умовного виразу (DR_{iws}) базового детекційного правила, згідно якого відбулося виявлення кібератак.

Умовно роботу ЕСОВ можна представити двома процесами:

– процес ініціалізації БД який пов'язаний з наповненням (модифікацією) БДК, БДП і БДЕ;

– процес виявлення кібератак.

На базі запропонованої методології та структурного рішення відповідної обчислювальної системи, розроблено алгоритмічне забезпечення для реалізації відповідного програмне забезпечення (ПО) для виявлення кібератак. Інтерфейс розроблення ПЗ при его використанні для розпізнавання IP-спуфінгу частково показано на рис. 2.

Для оцінки ефективності розробленої ЕСОВ проведено чисельні експерименти з розпізнавання кібератак типу спуфінг. Відзначимо, що на тепер, спуфінг-атаки є одними з найнебезпечніших засобів реалізації хакерських вторгнень. Спуфінгове ПЗ вводить користувача в оману, маскуючись під реально існуючі web-сервіси та інші програмні застосунки. Розрізняють наступні типи спуфінг-атак: email-спуфінг, IP-спуфінг, ARP-спуфінг та GPS-спуфінг.

Розглянуто процес виявлення одного із найпоширеніших видів спуфінгу, який орієнтований на підробку email листів. Зазвичай, фальсифікована адреса є частиною більш масштабної фішингової атаки, метою якої є отримання даних доступу користувача до певних сервісів чи ПЗ, однак подібні атаки можуть використовуватись і для розповсюдження неліцензійного ПЗ. Головна мета email-спуфінгу направлена на змушення користувача довіряти отриманому електронному листу. Тому подібні листи мають оформлення і наповнення максимально подібне до листів, що надсилають аутентичні сервіси.

Оскільки пряме виявлення email-спуфінгу є досить складним завданням, то для ідентифікації таких кібератак необхідно дослідити можливі зміни параметрів визначеного середовища, значення яких при проведенні атаки буде суттєво відрізнятись від нормального стану. Для його виявлення використано параметри: «Кількість виявлених IP-адрес у спам базах (КСБ)», «Кількість спам слів у темі (КСТ)» та «Кількість спам слів у повідомленні (КСП)». Якщо значення описаних параметрів характерних для нормальної роботи клієнта будуть певні відхилення від допустимих меж, то це може бути сигналом, що даний лист є

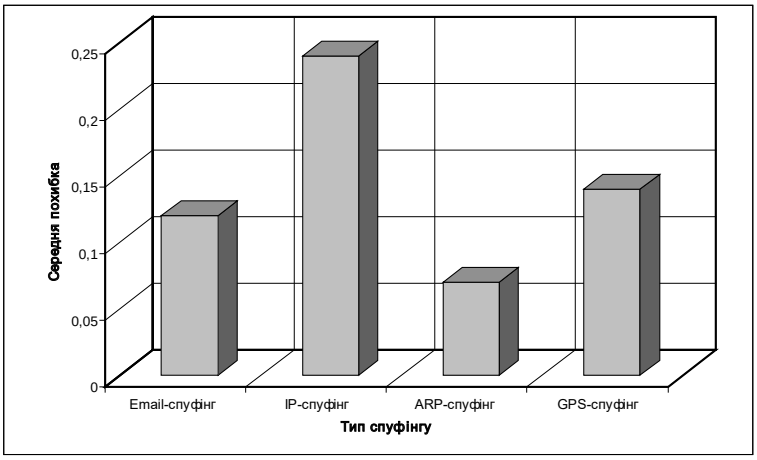

Рис. 3. Гістограма середньої похибки розпізнавання різних типів спуфінг-атак

частиною email-спуфінг-атаки. Наприклад, значна величина КСБ може служити ознакою того, що лист який аналізується є частиною email-спуфінг атаки. Максимальний показник цього параметра ($max_{КСБ}$) обмежений кількістю актуальних спам-баз за якими здійснюється сканування.

Для отримання конкретних параметрів був проведений експеримент з використанням наступного програмного забезпечення (ПЗ): MX Tool Box Super Tool 7, Subject Line, Mailing Check. У процесі досліджень спуфінгу листа зафіксовано 32 IP-адреси у спам-базах, $max_{КСБ} = 32$. При аналізі нормальних листів величина КСБ не перевищувала 7. Також встановлене середнє та високе значення таких IP-адрес, що відповідають кількості 11 та 21.

Виходячи з зручності проведення експерименту для параметра КСБ використано чотири терми з інтервалами – *[0;8], [9;16], [17;24], [25;32]*.

Параметр КСТ є одним за найважливіших при перевірці електронних листів на предмет причетності до email-спуфінг атак, оскільки відображає кількість спам-слів у темі повідомлення. Утиліта Subject Line дає можливість проаналізувати тему на предмет наявності спам слів, максимальна кількість яких у даному випадку задається параметром $max_{КСТ}$. В ході експерименту з використанням відповідного ПЗ значення $max_{КСТ} = 12$ спам-ознакам. При аналізі було виявлено такі ознаки, як помилка першого слова та символа у темі, повторення великих літер, послідовність пробілів, повторювання одних і тих самих слів у темі тощо. Відповідно до цього і визначається максимальна величина параметра КСТ. Слід зазначити, що при аналізі нормального електронного листа, відповідний показник не перевищував 3-х спам-ознак. На основі цього, для параметру КСТ сформовані інтервали *[0;4], [5;8], [9,12],* які відображають діапазони мінімальних, середніх та максимальних значень для даного параметру. Максимальна величина КСП ($max_{КСП}$) визначається максимальною кількістю спам-ознак, що можуть бути виявлені у відповідному повідомленні. Значення $max_{КСП}$, отримане з використанням утиліти Mailing Check дорівнює *5,7*. На основі цього визначені наступні інтервали, що найбільш коректно описують даний параметр – *[0;2], [3,4], [5,6]*. Передбачено, що для усіх параметрів, значення в діапазоні від середнього до максимального може бути свідченням реалізації email-спуфінг атаки. Відповідно до експерименту, мінімальні та максимальні граничні значення, що з великою впевненістю щодо суджень експерта можуть бути сигналом фальсифікації email-листа наступні: КСБ – *[25;32]*; КСТ – *[3;12]*.

Базуючись на аналогічних підходах визначено номенклатуру та діапазони діагностичних параметрів, аналіз яких доцільно використовувати для розпізнавання IP-спуфінгу, ARP-спуфінгу та GPS-спуфінгу. Це дозволило провести числові експерименти по розпізнаванню всіх вказаних типів спуфінг-атак. При проведені експериментів використано приклади спуфінгу зібрані авторським колективом та приклади наведені в *[1, 4, 8]*. Рішення про виявлення факту кібератаки приймалось при перевищенні результату порівняння піддослідного зразка з еталонами спуфінгу порогового значення 0,5. Основні результати експериментів представлені в табл. 1 та показані на рис. 3-4.

Для порівняння ЕСВВ з подібними відомими системами використано вільно доступна система розпізнавання мережевих кібератак

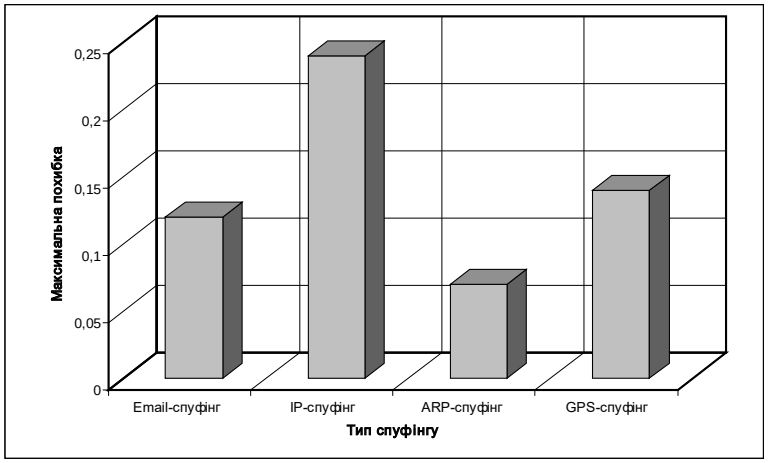

Рис. 4. Гістограма максимальної похибки розпізнавання різних типів спуфінг-атак

Таблиця 1

Похибки розпізнавання спуфінг-атак

Тип				
спуфінг-атаки	Email-спуфінг	IP-спуфінг	ARP-спуфінг	GPS-спуфінг
Середня похибка	0,12	0,24	0,07	0,14
Максимальна похибка	0,18	0,31	0,12	0,17

Snort (https://www.snort.org/) та ознайомчі версії систем виявлення атак від компаній-розробників Cisco (https://www.cisco.com) та InfoWatch (https://www.infowatch.ru/). Результати порівняння дають змогу стверджувати, що в середньому похибка розпізнавання спуфінгу при використанні ЕСВВ приблизно в 1,1–1,2 рази нижча за похибку розпізнавання означених систем виявлення. При цьому системи Snort, Cisco й InfoWatch показали неспроможність виявлення низки спуфінг-атак, що належать до типу 0-day. Можливим поясненням цього факту є недосконалість механізму експертного оцінювання аномального стану інформаційного ресурсу та відсутність необхідних статистичних даних, що використовуються для навчання вказаних систем виявлення. Отже, використання запропонованої експертної системи дає змогу підвищити ефективність виявлення вторгнень за рахунок зменшення похибки розпізнавання та розширення номенклатури аномальних станів. Крім того, отримані результати свідчать про перспективність застосування рішень [2] для виявлення нових видів кібератак, що характеризуються складністю визначення номенклатури діагностичних параметрів. Наприклад, одним із основних недоліків сучасних нейромережевих систем виявлення комп'ютерних вірусів є емпіричний вибір множини вхідних параметрів [1]. При цьому застосування використаних під час побудови ЕСВВ базової моделі параметрів, кортежної моделі формування базових компонент і методу формування лінгвістичних еталонів дасть можливість формалізувати процес формування вказаної множини параметрів.

Для порівняння ЕСВВ з подібними відомими системами використано вільно доступна система розпізнавання мережевих кібератак Snort (https://www.snort.org/) та ознайомчі версії систем виявлення атак від компаній-розробників Cisco (https://www.cisco.com) та InfoWatch (https://www.infowatch.ru/). Результати порівняння дають змогу стверджувати, що в середньому похибка розпізнавання спуфінгу при використанні ЕСВВ приблизно в 1,1–1,2 рази нижча за похибку розпізнавання означених систем виявлення. При цьому системи Snort, Cisco й InfoWatch показали неспроможність виявлення низки спуфінг-атак, що належать до типу 0-day. Можливим поясненням цього факту є недосконалість механізму експертного оцінювання аномального стану інформаційного ресурсу та відсутність необхідних статистичних даних, що використовуються для навчання вказаних систем виявлення. Отже, використання запропонованої експертної системи дає змогу підвищити ефективність виявлення вторгнень за рахунок зменшення похибки розпізнавання та розширення номенклатури аномальних станів. Крім того, отримані результати свідчать про перспективність застосування рішень [2] для виявлення нових видів кібератак, що характеризуються складністю визначення номенклатури діагностичних параметрів.

Наприклад, одним із основних недоліків сучасних нейромережевих систем виявлення комп'ютерних вірусів є емпіричний вибір множини вхідних параметрів [1]. При цьому застосування використаних під час побудови ЕСВВ базової моделі параметрів, кортежної моделі формування базових компонент і методу формування лінгвістичних еталонів дасть можливість формалізувати процес формування вказаної множини параметрів.

Висновки. У результаті проведених досліджень з'ясовано, що використання запропонованої експертної системи виявлення вторгнень на базі нечіткої логіки дає змогу підвищити ефективність виявлення за рахунок зменшення похибки розпізнавання та розширення номенклатури аномальних станів. Визначено, що напрями подальших досліджень полягають в адаптації рішень, використаних під час розроблення експертної системи виявлення вторгнень для створення методу визначення номенклатури вхідних параметрів нейромережевої системи виявлення комп'ютерних вірусів.

Список літератури:

1. Нейросетевые модели, методы и средства оценки параметров безопасности Интернет-ориентированных информационных систем: монография / А. Корченко, И. Терейковский, Н. Карпинский, С. Тынымбаев. Киев: ТОВ «Наш Формат», 2016. 275 с.

2. Корченко А., Щербина В., Вишневская Н. Методология построения систем выявления аномалий, порожденных кибератаками. *Захист інформації*. 2016. № 1. Т. 18. С. 30–38.

3. Корченко А.А. Кортежная модель формирования набора базовых компонент для выявления кибератак. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2014. Вип. 2 (28). С. 29–36.

4. Korchenko A., Warwas K., Kłos-Witkowska A. The Tupel Model of Basic Components' Set For-mation for Cyberattacks. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*: Proceedings of the 2015 IEEE 8th International Conference (Warsaw, 24–26 September, 2015). Warsaw, 2015. Vol. 1. P. 478–483.

5. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений. *Захист інформації*. 2014. № 1. Т. 16. С. 5–12.

6. Модели эталонов лингвистических переменных для обнаружения сниффинг-атак / И. Терейковский, А. Корченко, П. Викулов, А. Шаховал. *Захист інформації*. 2017. № 3. Т. 19. С. 228–242.

7. Improved method for the formation of linguistic standards for of intrusion detection systems / B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva. *Journal of Theoretical and Applied Information Technology*. 2016. Vol. 87. №. 2. P. 221–32.

8. The Etalon Models of Linguistic Variables for Sniffing-Attack Detection / M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*: Proceedings of the 2017 IEEE 9th International Conference (Bucharest, 21–23 September, 2017). Bucharest, 2017. Vol. 1. P. 258–264.

9. Корченко А.А. Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак. *Безпека інформації*. 2014. № 1 (20). С. 21–28.

10. Корченко А.А. Метод уровневой номинализации нечетких чисел для систем обнаружения вторжений. *Захист інформації*. 2014. № 4. Т. 16. С. 292–304.

11. Корченко А.А. Метод определения идентифицирующих термов для систем обнаружения вторжений. *Безпека інформації*. 2014. № 3. Т. 20. С. 217–223.

ОЦЕНКА ЭФФЕКТИВНОСТИ ЭКСПЕРТНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА БАЗЕ НЕЧЕТКОЙ ЛОГИКИ

Статья посвящена решению задачи доказательства эффективности экспертной системы обнаружения вторжений на базе нечеткой логики. Обоснована возможность экспериментальной оценки эффективности системы обнаружения на основе погрешности распознавания и ее функциональных возможностей. Приведены описание и результаты экспериментальных исследований, направленных на выявление различных типов спуфинг-атак. Показано, что по отношению к известным системам обнаружения вторжений предложенная система позволяет в 1,1–1,2 раза уменьшить погрешность распознавания и расширить номенклатуру аномальных состояний. Определено, что направления дальнейших исследований заключаются в адаптации решений, использованных при разработке экспертной системы обнаружения вторжений для создания метода определения номенклатуры входных параметров нейросетевой системы обнаружения компьютерных вирусов.

Ключевые слова: *система обнаружения вторжений, кибератака, спуфинг, экспертная система, нечеткая логика.*

EVALUATION OF EFFICIENCY OF EXPERT SYSTEM FOR EXPRESSION OF SUSPENSION ON THE BASIS OF FUZZY LOGIC

The article is devoted to solving the problem of proving the effectiveness of an expert intrusion detection system based on fuzzy logic. The possibility of experimental evaluation of the effectiveness of the detection system based on the recognition error and its functionality has been substantiated. The description and results of experimental studies aimed at identifying various types of spoofing attacks are given. It is shown that, with respect to the known intrusion detection systems, the proposed system makes it possible to reduce the recognition error by a factor of 1.1–1.2 and expand the range of anomalous states. It was determined that the directions of further research are to adapt the solutions used in the development of an expert intrusion detection system to create a method for determining the nomenclature of input parameters of a neural network computer virus detection system.

Key words: *intrusion detection system, cyber attack, spoofing, expert system, fuzzy logic.*