© Tereykovsky I., Korchenko A., Vikulov P., Ireifej Imad Issa Jamil. Etalons models of linguistic variables for email-spoofing-attack detection systems // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 2, p.99-109.

DOI: 10.18372/2225-5036.24.13062

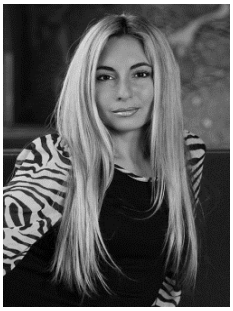
МОДЕЛІ ЕТАЛОНІВ ЛІНГВІСТИЧНИХ ЗМІННИХ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ EMAIL-СПУФІНГ-АТАК

Ігор Терейковський[1], Анна Корченко[2], Павло Вікулов[2], Ірейфідж Імад Ісса Джаміль[2]

[1]Національний технічний університет України «КПІ ім. Ігоря Сікорського»
[2]Національний авіаційний університет, Україна

ТЕРЕЙКОВСЬКИЙ Ігор Анатолійович, д.т.н.

Рік і місце народження: 1967 рік, м Тернопіль, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1992 рік.
Посада: професор кафедри системного програмування і спеціалізованих комп'ютерних систем НТУУ «КПІ ім. Ігоря Сікорського» з 2015 року.
Наукові інтереси: інформаційна безпека.
Публікації: більше 100 наукових праць, серед яких монографії, навчальні посібники, навчально-методичні комплекси дисциплін, наукові статті.
E-mail: terejkowski@ukr.net



КОРЧЕНКО Анна Олександрівна, к.т.н.

Рік і місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: більше 90 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: annakor@ukr.net

ВІКУЛОВ Павло Олександрович

Рік і місце народження: 1993 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2015 рік.
Посада: аспірант кафедри безпеки інформаційних технологій.
Наукові інтереси: аналітика інформаційної безпеки, системи виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: 5 наукових публікацій, серед яких наукові статті та тези.
E-mail: p.vikulov@ukr.net

ІРЕЙФІДЖ Імад Ісса Джаміль

Рік і місце народження: 1971 рік, м. Аммаан, Йорданія.
Освіта: Національний технічний університет України «КПІ ім. Ігоря Сікорського».
Посада: асистент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, система виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: 8 наукових статтей.
E-mail: kmuinform@gmail.com

Анотація. *Розвиток інформаційних систем у сучасному світі невід'ємно пов'язаний з вдосконаленням деструктивного програмного забезпечення, яке спрямоване на різноманітні ресурси інформаційних систем.*

Серед різноманітних способів впливу на користувача особливо небезпечними є такі, що за допомогою маскування під реально існуюче програмне забезпечення чи web-сервіс намагаються отримати доступ до персональних даних користувача, або використати його ресурси чи програмне забезпечення у шахрайських цілях. Активізація подібних атак вимагає створення спеціалізованих засобів виявлення та протидії, що будуть однаково ефективні як проти наявних, так і майбутніх кіберзагроз з невстановленими або нечітко визначеними властивостями. Тобто подібні засоби можуть функціонувати у нечіткому, слабоформалізованому середовищі. Сучасні методи, моделі та системи, що засновані на нечітких множинах можуть бути використані для побудови та вдосконалення наявних засобів виявлення вторгнень та аномалій у інформаційних системах, що виникають в результаті реалізації кіберзагроз. Є ряд розробок, що використовуються при їх виявленні, однією з яких є метод формування лінгвістичних еталонів для систем виявлення вторгнень. В описаному методі не розкритий механізм процесу формування еталонів параметрів для email-спуфінг-атак. З урахуванням цього, розроблено модель еталонів лінгвістичних змінних для виявлення email-спуфінг-атак, що дозволить формалізувати процес отримання еталонів параметрів (кількість виявлених IP-адрес у спам-базах, кількість спам-слів у темі, кількість спам-слів у повідомленні) для заданих лінгвістичних змінних обраного середовища оточення при вирішенні задач, щодо виявлення атак. Подібні моделі можуть бути використані для підвищення ефективності засобів захисту інформації, що спрямовані на протидію email-спуфінг атакам в інформаційних системах.

Ключові слова: *атаки, кібератаки, аномалії, методи формування лінгвістичних еталонів, системи виявлення вторгнень, системи виявлення атак, виявлення аномалій в інформаційних системах.*

Вступ

На сьогодні еволюція інформаційних систем неможлива без паралельного розвитку деструктивного програмного забезпечення (ПЗ), яке спрямоване на різноманітні ресурси інформаційних систем (РІС). Значна кількість зазначеного забезпечення створена для отримання доступу до персональних даних користувача, використання його ПЗ або інших його ресурсів у шахрайських цілях. Кібератаки такого типу можуть полягати у маскуванні ПЗ неавторизованої сторони (НАС) під авторизовані системи та сервіси з метою введення користувача в оману і отримання доступ до пов'язаних з ним РІС.

За останні роки кількість кібератак, які спрямовані та реалізовані проти України значно збільшилась, наприклад, у грудні 2015 року за допомогою деструктивного ПЗ (ДПЗ) BlackEnergy3, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більш 200 тисяч жителів області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго [1].

У грудні 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, що вивела з ладу низку комп'ютерів, а також знищила критично важливі бази даних. Це також призвело до затримки бюджетних виплат на сотні мільйонів гривень. В цей же час українські хакери на замовлення невстановленої особи здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. На думку профільного міністра, ця кібератака була націлена на крадіжку даних про пассажироперевезення [1].

У червні 2017 року відбулася масштабна хакерська атака за допомогою ДПЗ – вірус Petya.A, яка порушила роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці, КМ України, низку ЗМІ тощо[1].

Також протягом п'яти місяців 2018 року Службою безпеки України виявлено та задокументовано використання російськими спецслужбами більше 180 інтернет ресурсів з метою дестабілізації соціально-політичної ситуації в нашій країні [2].

Активізація подібних атак вимагає створення спеціалізованих засобів виявлення та протидії, що будуть однаково ефективні як проти наявних, так і майбутніх кіберзагроз з невстановленими або нечітко визначеними властивостями. Тобто, подібні засоби можуть функціонувати у нечіткому, слабоформалізованому середовищі [3]. Сучасні методи, моделі та системи, що засновані на нечітких множинах [3]–[24] можуть бути використані для побудови та вдосконалення наявних засобів виявлення вторгнень та аномалій у інформаційних системах, що виникають в результаті реалізації кіберзагроз. Базуючись на цьому, розробка відповідних технічних рішень, що зможуть функціонувати у нечітких умовах в слабоформалізованому середовищі, дасть можливість виявляти та протидіяти новим, модифікованим та майбутнім кібервторгненням.

Є низка відомих та корисних розробок, що використовуються при виявленні кіберзагроз, однією з яких є метод формування лінгвістичних еталонів для систем виявлення вторгнень (СВВ) [8, 20-24]. В описаному методі не розкритий механізм процесу формування еталонів параметрів для email-спуфінг-атак. З урахуванням вищезазначеного, актуальною задачею є створення нових моделей, що дозволять розширити множину лінгвістичних еталонів параметрів [8] для СВВ.

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. Для здійснення такого типу атак, НАС може використовувати різни види спуфінг-атак: EMAIL-спуфінг, IP-спуфінг, ARP-спуфінг та GPS-спуфінг.

Email-спуфінг – вид атаки, направлений на підробку email даних (адреса відправника, тема, текст чи вкладення). Користувачу надсилається лист на електронну пошту, який майже нічим не відрізня-

ється від авторизованих (рис. 1). Подібний лист зазвичай містить посилання чи вкладення які часто активує користувач, в результаті чого НАС може отримати доступ, наприклад, до персональних даних користувача, таких як логіни та паролі, номери банківських рахунків, особистої інформації тощо.

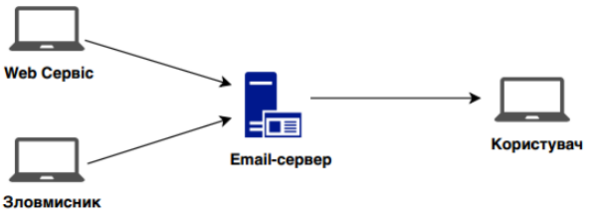


Рис. 1. Схема реалізації email-спуфінгу

IP-спуфінг зазвичай є частиною DOS-атаки. Його головною метою є маскування реальної IP-адреси НАС, а користувач при цьому отримує пакети що перевантажують систему з IP-адреси, яка не є автентичною (рис. 2), що і ускладнює протидію даному виду кібератаки.

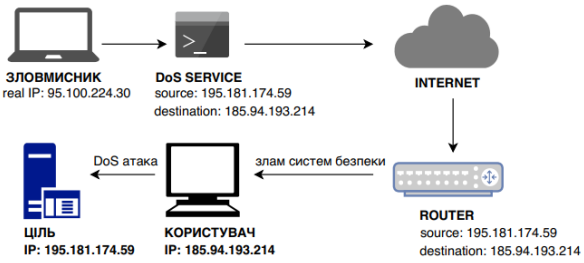


Рис. 2. Приклад реалізації атаки типу IP-спуфінг

Кібератака ARP-спуфінг базується на APR-протоколі (Address Resolution Protocol), використовується для моніторингу та перехоплення трафіку всередині локальної мережі (рис. 3). У більшості випадків НАС пов'язує свою MAC-адресу з IP-адресою мережі, на яку здійснюється атака. У разі успішної підміни НАС має можливість доступу до усіх пакетів, що проходять через комутатор мережі. Варто зазначити, що реалізація даної кібератаки обмежена мережами, що використовують ARP-протокол.

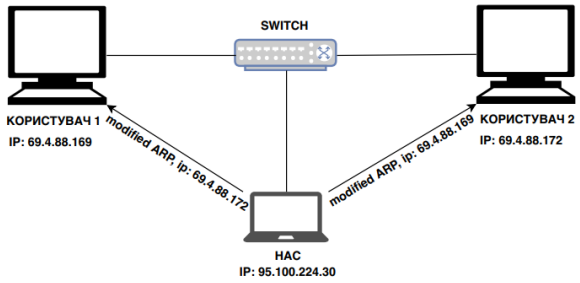


Рис. 3. Схема атаки типу ARP-спуфінг

Атака GPS-спуфінг спрямована на підміну даних у GPS-приймачі, при цьому НАС транслює в безпосередній близькості від користувача GPS-сигнал з дещо більшою потужністю, ніж реальний. У результаті цього користувач отримує дані не про фактичне місце розташування приймача, а те, яке йому надіслала НАС (рис. 4). Варто зазначити, що даний вид кібератаки є відносно складним, оскільки GPS-дані розраховуються відносно затримки сигналу від супутника. В такому випадку НАС необхідно мати інформацію про точне місце розташування користувача, для правильного налаштування затримки. У разі успішної реалізації GPS-спуфінгу користувач отримає ефект подібний розташуванню магніту біля компаса, а НАС поступово змінить дані фактичного розташування на фальсифіковані.

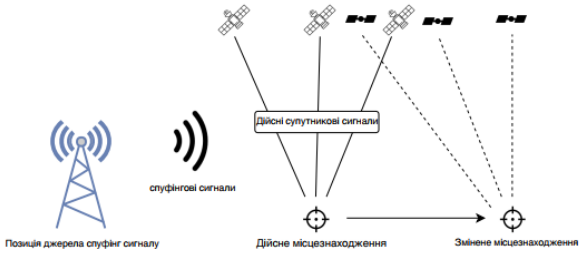


Рис. 4. Схема реалізації GPS-спуфінгу

Розглянемо один з 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. Зазвичай подібні спуфінгові листи містять посилання, які направляють користувача на фальсифікований сайт чи web-сервіс, який теж буде максимально схожий на автентичний. Такими сервісами можуть бути платні web-служби, онлайн банки тощо. Після переходу на такий сайт користувач, як правило, вводить свої особисті дані (логін, пароль, банківські реквізити тощо). Ця інформація одразу буде доступна НАС і може бути використана нею для протиправних дій на автентичному web-сервісі чи сайті. Зазвичай користувач у такому випадку отримує повідомлення про відмову в обробці даних.

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 виявлення такої атаки запропоновано використовувати наступні параметри: «Кількість виявлених IP-адрес у спам базах (КСБ)», «Кількість спам слів у темі (КСТ)» та «Кількість спам слів у повідомленні (КСП)». Для успішного проведення кібератаки НАС необхідно лише знати email користувача та сайт, що буде імітувати роботу автентичного web-сервісу, на який його буде перенаправлено за допомогою інформації з електронного листа.

Якщо в значення описаних параметрів характерних для нормальної роботи клієнта будуть певні відхилення від допустимих меж, то це може бути сигналом, що даний лист є частиною email-спуфінг-

атаки. Для отримання конкретних параметрів був проведений експеримент з використанням наступного ПЗ: MX Tool Box Super Tool 7, Subject Line, Mailing Check. Дане ПЗ має достатню кількість засобів для ідентифікації email-спуфінг атак за описаними параметрами. Як показує практика, електронні листи, що пересилаються під час зазначеної атаки можна виявити шляхом контроля параметрів КСБ, КСТ та КСП. 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.

В процесі експерименту, під час аналізу спуфінгового листа було зафіксовано 32 IP-адреси у спам-базах, тобто можемо припустити що $max_{КСБ}$=32 (рис. 5). При аналізі нормальних листів, здійсненого за допомогою утиліти MX Tool Box Super Tool 7 [25] величина зазначеного параметру не перевищувала 7 (рис. 6-7). Також встановлене середнє та високе значення таких IP-адрес, що відповідають кількості 11 та 21. (рис. 8-9).

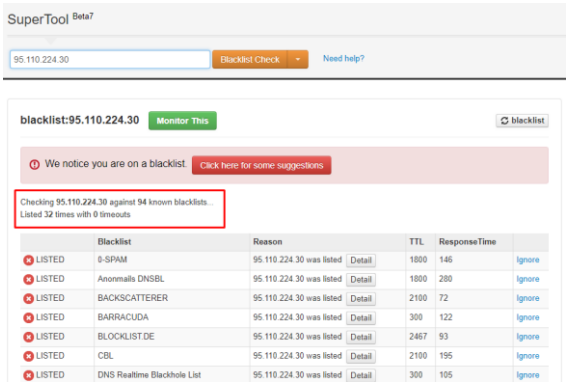


Рис. 5. Визначення максимальної величини КСБ за допомогою утиліти MX Tool Box Super Tool 7

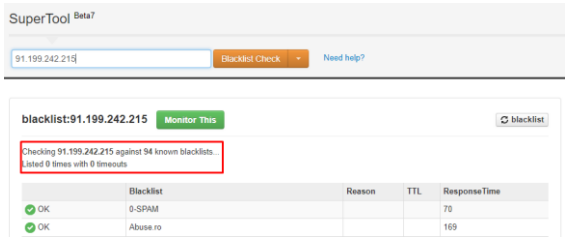


Рис. 6. Визначення мінімальної величини КСБ за допомогою утиліти MX Tool Box Super Tool 7

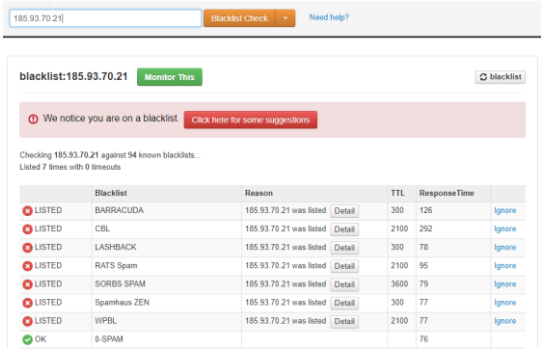


Рис. 7. Визначення малої величини КСБ за допомогою утиліти MX Tool Box Super Tool 7

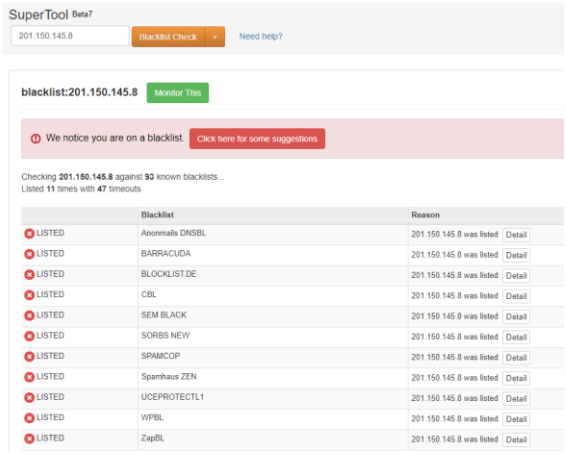


Рис. 8. Визначення середньої величини КСБ за допомогою утиліти MX Tool Box Super Tool 7

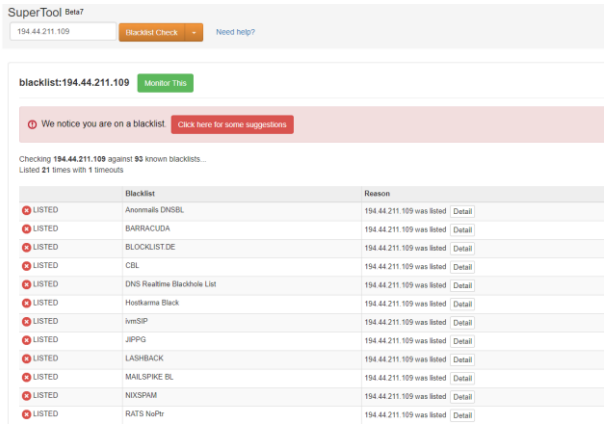


Рис. 9. Визначення високої величини КСБ за допомогою утиліти MX Tool Box Super Tool 7

Для зручності оцінювання параметрів на основі суджень експерта прийнято рахувати, що найбільш раціональною та достатньою для сприйняття кількість термів знаходиться в межах від 3-х до 5-ти [24]. Більшість варіантів застосувань повністю вичерпується використанням мінімальної кількості термів. Виходячи з експерименту для параметра КСБ, найбільш раціональним буде використання 4-х термів з відповідними 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. Зазвичай, користувач у власному email-клієнті приймає рішення про відкриття листа на основі його теми, оскільки вона, як і відправник, відображаються у швидкому перегляді в переліку листів. Велика кількість спам-слів у темі листа може бути свідченням того, що він є фальсифікованим і може бути частиною відповідної атаки. Утиліта Subject Line [26] 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 (рис. 10). 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 (рис. 11), які включають цифровий символ на початку теми, довжину теми та наявність послідовних цифрових символів.

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.

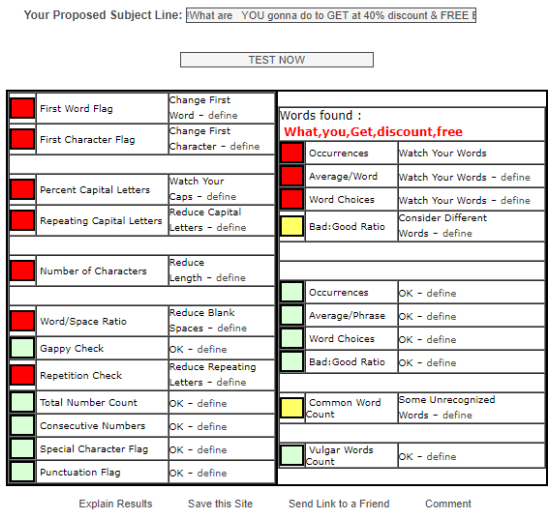


Рис. 10. Визначення величини КСТ за допомогою утиліти subject line tester

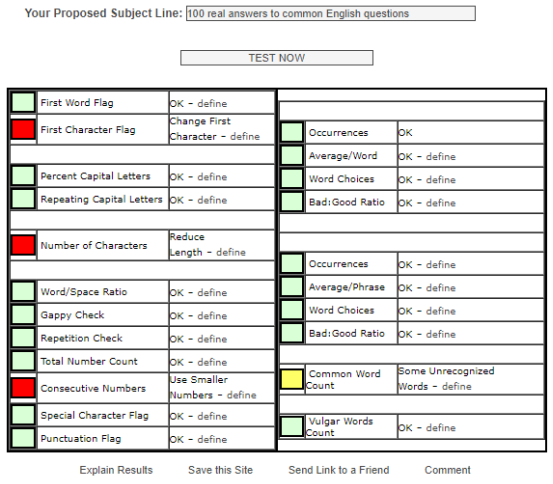


Рис. 11. Визначення величини КСТ в нормальному режимі роботи за допомогою утиліти subject line tester

Для роботи з КСП необхідно проводити більш детальний аналіз, оскільки текст повідомлення може містити не тільки символи, а і зображення, html розмітку, посилання тощо. Даний параметр описує кількість виявлених спам-ознак у повідомленні і може бути використаний за сигнал реалізації email-спуфінгу на користувача. Максимальна величина КСП ($max_{КСП}$) визначається максимальною кількістю спам-ознак, що можуть бути виявлені у відповідному повідомленні. Для їх ідентифікації необхідно скористатись утилітою Mailing Check. Для цього потенційний спам лист завантажується до утиліти у форматі .eml і далі утиліта аналізує його вміст та формує виявлені спам-ознаки. Кожна така ознака має певну кількість спам-балів, що впливають на загальну оцінку листа. Проаналізувавши усі спам-ознаки отримаємо сумарну кількість спам-балів, що і буде значення параметру КСП.

При аналізі безпечного електронного листа значення КСП, як правило, не перевищує 2 (рис. 12). При цьому у листі було виявлено такі 4 потенційні спам-ознаки, як велика кількість html розмітки та вставлених зображень, велика довжина рядка в листі та наявність табличних даних в листі. Таким чином, допомогою утиліти було отримано спам-рейтинг листа 1,4.

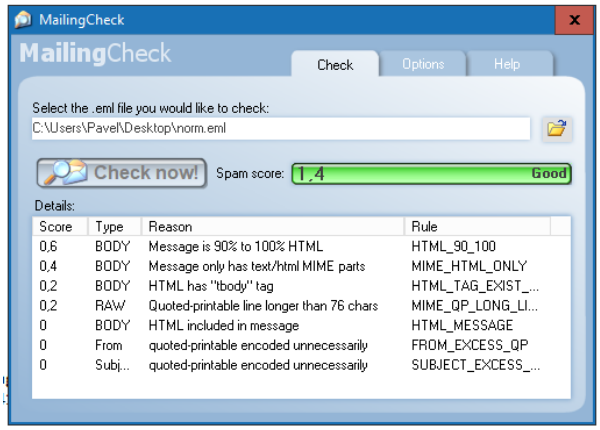


Рис. 12 Визначення величини КСП при аналізі безпечного email-листа

Експертний аналіз листа дозволив ідентифікувати 8 спам-ознак, що характерно для середнього значення параметра КСП. Ознаки пов'язані з кольором html-розмітки, що співпав з фоном, помилками кодування символів, великою кількістю вставлених зображень і html-розмітки, помилками html-розмітки тощо. Отримане значення при цьому становило 3,3 спам ознак (рис. 13).

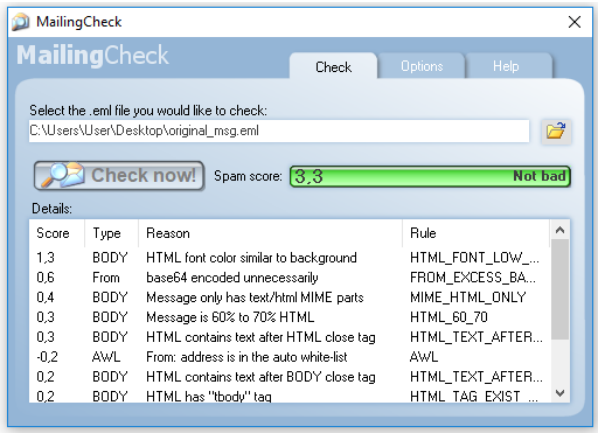


Рис. 13. Визначення середньої величини КСП

Значення $max_{КСП}$, отримане під час експерименту з використанням утиліти Mailing Check дорівнює $5{,}7$ (рис. 14). На основі цього визначені наступні інтервали, що найбільш коректно описують даний параметр – $[0;2]$, $[3;4]$, $[5;6]$.

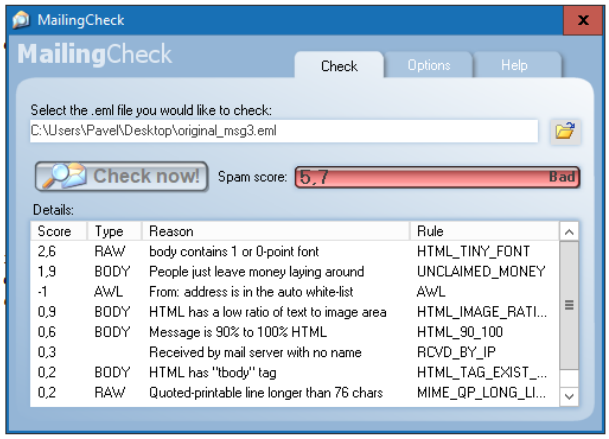


Рис. 14. Визначення максимальної величини КСП за допомогою утиліти Mailing Check

Логічно припустити, 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 – $[9;12]$; КСП – $[5;6]$.

З урахуванням зазначеного, розробимо модель еталонів лінгвістичних змінних для виявлення email-спуфінг-атак (МЕЕСА), що дозволить формалізувати процес отримання еталонів параметрів для заданих лінгвістичних змінних обраного середовища при вирішенні задач, щодо виявлення атак на інформаційні системи. Запропонована МЕЕСА частково базується на методі лінгвістичних термів з використанням статистичних даних (МЛТС) [3], а також на методі формування лінгвістичних еталонів для СВВ МФЛЕ [8, 23].

Для цього сформуємо підмножину ідентифікаторів (ІД) експертних суджень, при $n=1$ для кібератаки з ІД $CA_1 = CA_{ESP} = ESP$, $m_1 = 3$, $r_1 = 4$, $r_2 = 3$, $r_3 = 3$ відповідно етапу 1 виразу (7) в [8, 23]:

$$\{\bigcup_{i=1}^{1}\mathbf{LE}_1\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{\mathbf{m_1}}\mathbf{LE}_{ij}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_1}\{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\{\{LE_{ESPKCБ1}, LE_{ESPKCБ2}, LE_{ESPKCБ3}, LE_{ESPKCБ4}\},$$
$$\{LE_{ESPKCT1}, LE_{ESPKCT2}, LE_{ESPKCT3}\},$$
$$\{LE_{ESPKCП1}, LE_{ESPKCП2}, LE_{ESPKCП3}\}\} =$$
$$\{\{"M","C","B","ДВ"\},\{"H","C","B"\},\{"H","C","B"\}\}, (1)$$

де ESP – «Email-Spoffing-атака», а $LE_{ESPKCБ1} = "M"$, $LE_{ESPKCБ2} = "C"$, $LE_{ESPKCБ3} = "B"$, $LE_{ESPKCБ4} = "ДВ"$, $LE_{ESPKCT1} = "H"$, $LE_{ESPKCT2} = "C"$, $LE_{ESPKCT3} = "B"$ та $LE_{ESPKCП1} = "H"$, $LE_{ESPKCП2} = "C"$, $LE_{ESPKCП3} = "B"$ відповідно є ІД таких лінгвістичних оцінок експерта, що відображають стан параметрів $P_{ESPKCБ} = КСБ$, $P_{ESPKCT} = КСТ$ та $P_{ESPKCП} = КСП$ в 3-вимірному параметричному підсередовищі [15].

Далі, відповідно етапу 2 в [8, 23], необхідно сформувати базову матрицю частот. Для цього побудуємо підмножину ІД інтервалів $\mathbf{N_{ij}}$ $(j = \overline{1,m_i})$ (див. вираз (12) в [8, 23]), що характеризують кібератаку з ІД $CA_{ESP} = ESP$, на області визначення якої експерт виконує лінгвістичне оцінювання відносно значень параметрів $P_{ESPKCБ}$, P_{ESPKCT} та $P_{ESPKCП}$.

При $n=1$, $m_1 = 3$, $r_1 = 4$,, $r_2 = 3$, $r_3 = 3$ отримаємо:

$$\{\bigcup_{i=1}^{1}\mathbf{N}_i\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{3}\mathbf{N}_{ij}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{3}\{\bigcup_{k=1}^{k_j} N_{ijk}\}\}\} =$$
$$\{N_{ESPKCБ1}, N_{ESPKCБ2}, N_{ESPKCБ3}, N_{ESPKCБ4}\},$$
$$\{N_{ESPKCT1}, N_{ESPKCT2}, N_{ESPKCT3}\},$$
$$\{N_{ESPKCП1}, N_{ESPKCП2}, N_{ESPKCП3}\}\}. \quad (2)$$

Враховуючи елементи підмножин $\mathbf{LE_{ij}}$ та $\mathbf{NE_{ij}}$ на основі узагальненої таблиці (див. табл. (1) в [8, 23]) побудуємо поточні оцінки (див. табл. 1-3) по елементам підмножин, тобто:

$LE_{ESPKCБk}(r_1 = 4, k = \overline{1,4})$, $N_{ESPKCБk}$, тобто

$N_{ESPKCБ1} = [N^{min}_{ESPKCБ1}; N^{max}_{ESPKCБ1}] \Leftrightarrow [0;8]$,

$N_{ESPKCБ2} = [N^{min}_{ESPKCБ2}; N^{max}_{ESPKCБ2}] \Leftrightarrow [9;16]$,

$N_{ESPKCБ3} = [N^{min}_{ESPKCБ3}; N^{max}_{ESPKCБ3}] \Leftrightarrow [17;24]$,

$N_{ESPKCБ4} = [N^{min}_{ESPKCБ4}; N^{max}_{ESPKCБ4}] \Leftrightarrow [25;32]$.

$LE_{ESPKCTk}(r_2 = 3, k = \overline{1,3})$, $N_{ESPKCTk}$, тобто

$N_{ESPKCT1} = [N^{min}_{ESPKCT1}; N^{max}_{ESPKCT1}] \Leftrightarrow [0;4]$,

$N_{ESPKCT2} = [N^{min}_{ESPKCT2}; N^{max}_{ESPKCT2}] \Leftrightarrow [5;8]$,

$N_{ESPKCT3} = [N^{min}_{ESPKCT3}; N^{max}_{ESPKCT3}] \Leftrightarrow [9;12]$,

а також $LE_{ESPKCПk}(r_2 = 3, k = \overline{1,3})$, $N_{ESPKCПk}$, тобто

$N_{ESPKCП1} = [N^{min}_{ESPKCП1}; N^{max}_{ESPKCП1}] \Leftrightarrow [0;2]$,

$N_{ESPKCП2} = [N^{min}_{ESPKCП2}; N^{max}_{ESPKCП2}] \Leftrightarrow [3;4]$,

$N_{ESPKCП3} = [N^{min}_{ESPKCП3}; N^{max}_{ESPKCП3}] \Leftrightarrow [5;6]$.

Поточна таблиця оцінок по $\mathbf{LE_{ESPKCБ}}$ Таблиця 1

$\mathbf{LE_{ESPKCБ}}$	$\mathbf{N_{ESPKCБ}}$			
	$N_{ESPKCБ1}$	$N_{ESPKCБ2}$	$N_{ESPKCБ3}$	$N_{ESPKCБ4}$
«М»	2	1	0	0
«С»	1	4	2	0
«Б»	0	1	4	2
«ОБ»	0	0	1	6

Поточна таблиця оцінок по $\mathbf{LE_{ESPKCT}}$ Таблиця 2

$\mathbf{LE_{ESPKCT}}$	$\mathbf{N_{ESPKCT}}$		
	$N_{ESPKCT1}$	$N_{ESPKCT2}$	$N_{ESPKCT3}$
«Н»	3	1	0
«С»	1	2	1
«В»	0	1	2

Поточна таблиця оцінок по $\mathbf{LE}_{\mathbf{ESPKC\,П}}$ Таблиця 3

$\mathbf{LE}_{\mathbf{ESPKC\,П}}$		$\mathbf{N}_{\mathbf{ESPKCП}}$		
		$N_{ESPKCП1}$	$N_{ESPKCП2}$	$N_{ESPKCП3}$
«Н»		2	1	0
«С»		1	4	3
«В»		0	3	5

Далі, з урахуванням даних таблиць 1-3 та виразу (13), в [8, 23] сформуємо матриці частот при $n=1$, $m_1=\overline{1,3}$, $s,q=\overline{1,r_1}$, $s,q=\overline{1,r_2}$, $s,q=\overline{1,r_3}$:

$$F_{11}=F_{ESPKCБ}=\left\|f_{11sq}\right\|=\begin{vmatrix} f_{1111} & f_{1112} & f_{1113} & f_{1114} \\ f_{1121} & f_{1122} & f_{1123} & f_{1124} \\ f_{1131} & f_{1132} & f_{1133} & f_{1134} \\ f_{1141} & f_{1142} & f_{1143} & f_{1144} \end{vmatrix},$$

$$F_{12}=F_{ESPKCT}=\left\|f_{12sq}\right\|=\begin{vmatrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{vmatrix} \text{ та}$$

$$F_{13}=F_{ESPKCП}=\left\|f_{13sq}\right\|=\begin{vmatrix} f_{1311} & f_{1312} & f_{1313} \\ f_{1321} & f_{1322} & f_{1323} \\ f_{1331} & f_{1332} & f_{1333} \end{vmatrix}.$$

Далі для формування похідної матриці частот, при $n=1$, $m_1=3$ побудуємо по відповідним стовпчикам матриць $F_{ESPKCБ}$, F_{ESPKCT} та $F_{ESPKCП}$ з урахуванням виразу (15) в [8, 23] вектори сум:

$$VS_{ESPKCБ}=\left\|vs_{ESPKCБq}\right\|=$$

$$\left\|vs_{ESPKCБ1},vs_{ESPKCБ2},vs_{ESPKCБ3},vs_{ESPKCБ4}\right\|=$$

$$\left\|\bigcup_{q=1}^{4}\sum_{s=1}^{4}f_{ESPKCБsq}\right\|=\left\|3,6,7,8\right\|,\ (q=\overline{1,4}),$$

$$VS_{ESPKCT}=\left\|vs_{ESPKCTq}\right\|=\left\|vs_{ESPKCT1},vs_{ESPKCT2},vs_{ESPKCT3}\right\|=$$

$$\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{ESPKCTsq}\right\|=\left\|4,4,3\right\|,\ (q=\overline{1,3}),$$

$$VS_{ESPKCП}=\left\|vs_{ESPKCПq}\right\|=\left\|vs_{ESPKCП1},vs_{ESPKCП2},vs_{ESPKCП3}\right\|=$$

$$\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{ESPKCПsq}\right\|=\left\|3,8,8\right\|,\ (q=\overline{1,3}).$$

Далі, з урахуванням (16) в [8, 23] з $VS_{ESPKCБ}$, VS_{ESPKCT}, $VS_{ESPKCП}$ визначимо максимальний елемент:

$$vsm_{ESPKCБ}=\bigvee_{q=1}^{4}vs_{ESPKCБq}=vs_{ESPKCБ1}\vee vs_{ESPKCБ2}\vee vs_{ESPKCБ3}$$

$$\vee vs_{SPFKCБ4}=3\vee 6\vee 7\vee 8=vsm_{SPFKCБ}=8,$$

$$vsm_{ESPKCT}=\bigvee_{q=1}^{3}vs_{ESPKCTq}=vs_{ESPKCT1}\vee vs_{ESPKCT2}\vee vs_{ESPKCT3}=$$

$$4\vee 4\vee 3=vsm_{ESPKCT}=4,$$

$$vsm_{ESPKCП}=\bigvee_{q=1}^{3}vs_{ESPKCПq}=vs_{ESPKCП1}\vee vs_{ESPKCП2}\vee vs_{ESPKCП3}=$$

$$3\vee 8\vee 8=vsm_{ESPKCП}=8,$$

а відповідно з (17) в [8, 23] отримаємо похідну матрицю частот:

$$F'_{ESPKCБ}=(vsm_{ESPKCБ}/vsm_{ESPKCБq})F_{ESPKCБ}=$$

$$\begin{Vmatrix} 5,3 & 1,3 & 0 & 0 \\ 2,7 & 5,3 & 2,3 & 0 \\ 0 & 1,3 & 4,6 & 2 \\ 0 & 0 & 1,1 & 6 \end{Vmatrix},$$

$$F'_{ESPKCT}=(vsm_{ESPKCT}/vsm_{ESPKCTq})F_{ESPKCT}=\begin{Vmatrix} 3 & 1 & 0 \\ 1 & 2 & 1,3 \\ 0 & 1 & 2,7 \end{Vmatrix},$$

$$F'_{ESPKCП}=(vsm_{ESPKCП}/vsm_{ESPKCПq})F_{ESPKCП}=\begin{Vmatrix} 5,3 & 1 & 0 \\ 2,7 & 4 & 3 \\ 0 & 3 & 5 \end{Vmatrix}.$$

Далі, відповідно, (22) в [8, 23] сформуємо підмножину нечітких термів $\mathbf{T}_{\mathbf{ESPKCБ}}$, $\mathbf{T}_{\mathbf{ESPKCT}}$, $\mathbf{T}_{\mathbf{ESPKCП}}$ при $n=1$ (тобто для кібератак з ІД $CA_{ESP}=ESP$), $m_1=3$, $r_1=4$, $r_2=3$, $r_3=3$:

$$\{\bigcup_{i=1}^{1}\mathbf{T}_i\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{T}_{ij}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\}=$$

$$\{\{\underset{\sim}{T}_{ESPKCБ1},\underset{\sim}{T}_{ESPKCБ2},\underset{\sim}{T}_{ESPKCБ3},\underset{\sim}{T}_{ESPKCБ4}\},$$

$$\{\underset{\sim}{T}_{ESPKCT1},\underset{\sim}{T}_{ESPKCT2},\underset{\sim}{T}_{ESPKCT3}\},$$

$$\{\underset{\sim}{T}_{ESPKCП1},\underset{\sim}{T}_{ESPKCП2},\underset{\sim}{T}_{ESPKCП3}\}\}=$$

$$\{\{\underset{\sim}{M}_{ESPKCБ},\underset{\sim}{C}_{ESPKCБ},\underset{\sim}{B}_{ESPKCБ},\underset{\sim}{ДВ}_{ESPKCБ}\},$$

$$\{\underset{\sim}{H}_{ESPKCT},\underset{\sim}{C}_{ESPKCT},\underset{\sim}{B}_{ESPKCT}\},\{\underset{\sim}{H}_{ESPKCП},\underset{\sim}{C}_{ESPKCП},\underset{\sim}{B}_{ESPKCП}\}\}.$$

Відповідно (23) в [8, 23] по відповідним рядкам $F'_{ESPKCБ}$, F'_{ESPKCT}, $F'_{ESPKCП}$ побудуємо вектори максимумів, тобто:

$$FM_{ESPKCБ}=\left\|fm_{ESPKCБs}\right\|=$$

$$\left\|fm_{ESPKCБ1},fm_{ESPKCБ2},fm_{ESPKCБ3},fm_{ESPKCБ4}\right\|=\left\|5,3;5,3;4,6;6\right\|,$$

$$FM_{ESPKCT}=\left\|fm_{ESPKCTs}\right\|=$$

$$\left\|fm_{ESPKCT1},fm_{ESPKCT2},fm_{ESPKCT3}\right\|=\left\|3;2;2,7\right\|,$$

$$FM_{ESPKCП}=\left\|fm_{ESPKCПs}\right\|=$$

$$\left\|fm_{ESPKCП1},fm_{ESPKCП2},fm_{ESPKCП3}\right\|=\left\|5,3;4;5\right\|.$$

На основі $FM_{ESPKCБ}$, FM_{ESPKCT} та $FM_{ESPKCП}$ по виразу (24) в [8, 23] сформуємо матриці функцій належності:

$$M_{ESPKCБ}=\left\|\mu_{ESPKCБsq}\right\|=\begin{Vmatrix} 1 & 0,25 & 0 & 0 \\ 0,5 & 1 & 0,5 & 0 \\ 0 & 0,25 & 1 & 0,3 \\ 0 & 0 & 0,24 & 1 \end{Vmatrix},$$

$$M_{ESPKCT}=\left\|\mu_{ESPKCTsq}\right\|=\begin{Vmatrix} 1 & 0,5 & 0 \\ 0,3 & 1 & 0,5 \\ 0 & 0,5 & 1 \end{Vmatrix},$$

$$M_{ESPKCП}=\left\|\mu_{ESPKCПsq}\right\|=\begin{Vmatrix} 1 & 0,3 & 0 \\ 0,5 & 1 & 0,6 \\ 0 & 0,8 & 1 \end{Vmatrix},$$

де $\mu_{ESPKCБsq}=f'_{ESPKCБsq}/fm_{ESPKCБs}$, $(s,q=\overline{1,4})$, $\mu_{ESPKCTsq}=f'_{ESPKCTsq}/fm_{ESPKCTs}$, $(s,q=\overline{1,3})$, $\mu_{ESPKCПsq}=f'_{ESPKCПsq}/fm_{ESPKCПs}$, $(s,q=\overline{1,3})$.

На основі отриманих даних, $\mu_{ESPRKCБsq}$, $\mu_{ESPRKCTsq}$, $\mu_{ESPRKCПsq}$ і обчислених за виразом (26) в [8, 23] $x_{ESPRKCБsq}$, $x_{ESPRKCTsq}$, $x_{ESPRKCПsq}$ визначимо набори нечітких термів відповідно (25) в [8, 23] $\underset{\sim}{T}_{ESPRKCБs} = \{ \mu_{ESPRKCБs1} / x_{ESPRKCБs1}, \mu_{ESPRKCБs2} / x_{ESPRKCБs2}, \mu_{ESPRKCБs3} / x_{ESPRKCБs3}, \mu_{ESPRKCБs4} / x_{ESPRKCБs4} \}$, $(s,q = \overline{1,4})$, де відповідно (26) в [8, 23] $X_{ESPRKCБsq} = N^{max}_{ESPRKCБq} / N^{max}_{ESPRKCБr}$, $(q = \overline{1,4})$ або $\{\bigcup_{q=1}^{4} X_{ESPRKCБsq}\} = \{0,25;0,5;0,75;1\}$. $\underset{\sim}{T}_{ESPRKCTs} = \{ \mu_{ESPRKCTs1} / x_{ESPRKCTs1}, \mu_{ESPRKCTs2} / x_{ESPRKCTs2}, \mu_{ESPRKCTs3} / x_{ESPRKCTs3} \}$, $(s,q = \overline{1,3})$, де $X_{ESPRKCTsq} = N^{max}_{ESPRKCTq} / N^{max}_{ESPRKCTr}$, $(q = \overline{1,3})$ або $\{\bigcup_{q=1}^{3} X_{ESPRKCTsq}\} = \{0,33;0,67;1\}$. $\underset{\sim}{T}_{ESPRKCПs} = \{ \mu_{ESPRKCПs1} / x_{ESPRKCПs1}, \mu_{ESPRKCПs2} / x_{ESPRKCПs2}, \mu_{ESPRKCПs3} / x_{ESPRKCПs3}$, $(s,q = \overline{1,3})$, де $X_{ESPRKCПsq} = N^{max}_{ESPRKCПq} / N^{max}_{ESPRKCПr}$, $(q = \overline{1,3})$ або $\{\bigcup_{q=1}^{3} X_{ESPRKCПsq}\} = \{0,33;0,67;1\}$.

Таким чином, отримані члени підмножини $\mathbf{T}_{\mathbf{ESPRKCБ}}$, $\mathbf{T}_{\mathbf{ESPRKCT}}$, $\mathbf{T}_{\mathbf{ESPRKCП}}$ (числова форма), відповідно є відображенням членів підмножини $\mathbf{LE}_{\mathbf{ESPRKCБ}}$, $\mathbf{LE}_{\mathbf{ESPRKCT}}$, $\mathbf{LE}_{\mathbf{ESPRKCП}}$ (лінгвістична форма) та подані у наступному вигляді:

$\underset{\sim}{T}_{ESPRKCБ1} = \underset{\sim}{M} = \{1 / 0,25; 0,25 / 0,5; 0 / 0,75; 0 / 1\}$;

$\underset{\sim}{T}_{ESPRKCБ2} = \underset{\sim}{C} = \{0,5 / 0,25;\ 1 / 0,5; 0,5 / 0,75; 0 / 1\}$;

$\underset{\sim}{T}_{ESPRKCБ3} = \underset{\sim}{B} = \{0 / 0,25; 0,25 / 0,5;\ 1 / 0,75; 0,3 / 1\}$;

$\underset{\sim}{T}_{ESPRKCБ4} = \underset{\sim}{ДВ} = \{0 / 0,25; 0 / 0,5; 0,24 / 0,75; 1 / 1\}$,

$\underset{\sim}{T}_{ESPRKCT1} = \underset{\sim}{H} = \{1 / 0,33; 0,5 / 0,67; 1 / 1\}$;

$\underset{\sim}{T}_{ESPRKCT2} = \underset{\sim}{C} = \{0,3 / 0,33; 1 / 0,67; 0,5 / 1\}$;

$\underset{\sim}{T}_{ESPRKCT3} = \underset{\sim}{B} = \{0 / 0,33; 0,5 / 0,67; 1 / 1\}$,

$\underset{\sim}{T}_{ESPRKCП1} = \underset{\sim}{H} = \{1 / 0,33; 0,3 / 0,67; 0 / 1\}$;

$\underset{\sim}{T}_{ESPRKCП2} = \underset{\sim}{C} = \{0,5 / 0,33; 1 / 0,67; 0,6 / 1\}$;

$\underset{\sim}{T}_{ESPRKCП3} = \underset{\sim}{B} = \{0 / 0,33; 0,8 / 0,67; 1 / 1\}$.

Далі відповідно (29) в [8, 23] сформуємо еталонні НЧ $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCБ}} \subseteq \mathbf{T}^{\mathbf{e}}$, $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCT}} \subseteq \mathbf{T}^{\mathbf{e}}$, $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCП}} \subseteq \mathbf{T}^{\mathbf{e}}$:

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCБ}} = \{\bigcup_{s=1}^{4} \underset{\sim}{T}^{e}_{ESPRKCБs}\} = \{\underset{\sim}{T}^{e}_{ESPRKCБ1}, \underset{\sim}{T}^{e}_{ESPRKCБ2}, \underset{\sim}{T}^{e}_{ESPRKCБ3}, \underset{\sim}{T}^{e}_{ESPRKCБ4}\} = \{\underset{\sim}{M}^{e}_{ESPRKCБ1}, \underset{\sim}{C}^{e}_{ESPRKCБ2}, \underset{\sim}{B}^{e}_{ESPRKCБ3}, \underset{\sim}{ДВ}^{e}_{ESPRKCБ4}\},\ (s = \overline{1,4}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCT}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{ESPRKCTs}\} = \{\underset{\sim}{T}^{e}_{ESPRKCT1}, \underset{\sim}{T}^{e}_{ESPRKCT2}, \underset{\sim}{T}^{e}_{ESPRKCT3}\} = \{\underset{\sim}{H}^{e}_{ESPRKCT1}, \underset{\sim}{C}^{e}_{ESPRKCT2}, \underset{\sim}{B}^{e}_{ESPRKCT3}\},\ (s = \overline{1,3}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCП}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{ESPRKCПs}\} = \{\underset{\sim}{T}^{e}_{ESPRKCП1}, \underset{\sim}{T}^{e}_{ESPRKCП2}, \underset{\sim}{T}^{e}_{ESPRKCП3}\} = \{\underset{\sim}{H}^{e}_{ESPRKCП1}, \underset{\sim}{C}^{e}_{ESPRKCП2}, \underset{\sim}{B}^{e}_{ESPRKCП3}\},\ (s = \overline{1,3}),$$

де: члени підмножини $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCБ}}$ – $\underset{\sim}{M}^{e}_{ESPRKCБ1}, \underset{\sim}{C}^{e}_{ESPRKCБ2}, \underset{\sim}{B}^{e}_{ESPRKCБ3}, \underset{\sim}{ДВ}^{e}_{ESPRKCБ4}$; $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCT}}$ – $\underset{\sim}{H}^{e}_{ESPRKCT1}, \underset{\sim}{C}^{e}_{ESPRKCT2}, \underset{\sim}{B}^{e}_{ESPRKCT3}$; $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPRKCП}}$ – $\underset{\sim}{H}^{e}_{ESPRKCП1}, \underset{\sim}{C}^{e}_{ESPRKCП2}, \underset{\sim}{B}^{e}_{ESPRKCП3}$ є еталонними НЧ.

Далі перетворимо нечіткі терми $\underset{\sim}{M}_{ESPRKCБ}$, $\underset{\sim}{C}_{ESPRKCБ}$, $\underset{\sim}{B}_{ESPRKCБ}$ та $\underset{\sim}{ДВ}_{ESPRKCБ}$ таким чином, щоб для усіх $\underset{\sim}{T}_{ESPRKCБs}$ було справедливим відношення порядку, тобто. $\forall x_{ESPRKCБsq} : x_{ESPRKCБsq} < x_{ESPRKCБsq+1}$, $(q = \overline{1,4})$ (відповідно кроку 1, етапу 5 в [8, 23]). Якщо в якості компонентів таких термів використовувати конкретні значення, отримані в прикладі вище, то для них таке відношення буде істинним. Так, наприклад, для $\underset{\sim}{M}_{ESPRKCБ}$ це $x_{ESPRKCБ11} < x_{ESPRKCБ12} < x_{ESPRKCБ13} < x_{ESPRKCБ14} = 0,25 < 0,5 < 0,75 < 1$.

Також аналогічно буде істинним відношення для $\underset{\sim}{H}_{ESPRKCT}$ – це $x_{ESPRKCT11} < x_{ESPRKCT12} < x_{ESPRKCT13} = 0,33 < 0,67 < 1$, та для $\underset{\sim}{H}_{ESPRKCП}$ – це $x_{ESPRKCП11} < x_{ESPRKCП12} < x_{ESPRKCП13} = 0,33 < 0,67 < 1$.

Далі відповідно кроку 2 етапу 5 в [8, 23] для $\underset{\sim}{T}_{ESPRKCБs}$ виконаємо процедуру поглинання.

Для $\underset{\sim}{M}_{ESPRKCБ1}$ (де мода $x_{ESPRKCБ1M} = x_{ESPRKCБ11} = 0,25$, а її порядковий номер $M = 1$) при умові U_2 (тобто $\mu_{ESPRKCБ13} = \mu_{ESPRKCБ14} = 0$) виконується поглинання одним компонентом $0 / x^{max}_{ESPRKCБ1}$ ряду інших відповідно виразу $x^{max}_{ESPRKCБ1} = x_{ESPRKCБ13} \wedge x_{ESPRKCБ14} = 0,75 \wedge 1 = 0,75$ $(q = \overline{1,4})$. Таким чином, $\mu_{ESPRKCБ13} / x_{ESPRKCБ13} = 0 / 0,75$, $\mu_{ESPRKCБ14} / / x_{ESPRKCБ14} = 0 / 1$ поглинаються компонентом $\mu_{ESPRKCБ13} / x_{ESPRKCБ13} = 0 / 0,75$.

Далі, для $\underset{\sim}{ДВ}_{ESPRKCБ1}$ (де мода $x_{ESPRKCБ4M} = x_{ESPRKCБ44} = 1$, а її порядковий номер $M = 4$) при умові U_1 ($\mu_{ESPRKCБ41} = \mu_{ESPRKCБ42} = 0$) відбувається поглинання одним компонентом, $0 / x^{min}_{ESPRKCБ4}$ іншого відповідно виразу $x^{min}_{ESPRKCБ4} = x_{ESPRKCБ41} \vee x_{ESPRKCБ42} = 0,25 \vee 0,5 = 0,5$. Таким чином, $\mu_{ESPRKCБ41} / x_{ESPRKBCБ41} = 0 / 0,25$, $\mu_{ESPRKCБ42} / x_{ESPRKCБ42} = 0 / 0,5$ поглинається компонентом $\mu_{ESPRKCБ42} / x_{ESPRKCБ42} = 0 / 0,5$.

Далі, для кожного $\underset{\sim}{T}_{ESPRKCTs}$ ($\underset{\sim}{H}$, $\underset{\sim}{C}$, $\underset{\sim}{B}$) і $\underset{\sim}{T}_{ESPRKCПs}$ ($\underset{\sim}{H}$, $\underset{\sim}{C}$, $\underset{\sim}{B}$) умови U_1 та U_2 не виконуються і тому операція поглинання не відбувається. Враховуючи описані перетворення, а також вирази (28) в [8, 23] визначимо проміжні терми у вигляді:

$\underset{\sim}{T}'_{ESPRKCБ1} = \underset{\sim}{M}'_{ESPRKCБ1} = \{1 / 0,25; 0,25 / 0,5; 0 / 0,75\}$;

$\underset{\sim}{T}'_{ESPRKCБ2} = \underset{\sim}{C}'_{ESPRKCБ2} = \{0,5 / 0,25;\ 1 / 0,5; 0,5 / 0,75; 0 / 1\}$;

$\underset{\sim}{T}'_{ESPRKCБ3} = \underset{\sim}{B}'_{ESPRKCБ3} = \{0 / 0,25; 0,25 / 0,5;\ 1 / 0,75; 0,3 / 1\}$;

$\underset{\sim}{T}'_{ESPRKCБ4} = \underset{\sim}{ДВ}'_{ESPRKCБ4} = \{0 / 0,5; 0,24 / 0,75; 1 / 1\}$,

$\underset{\sim}{T}'_{ESPRKCT1} = \underset{\sim}{H}'_{ESPRKCT1} = \{1 / 0,2; 0,5 / 0,5; 1 / 1\}$;

$\underset{\sim}{T}'_{ESPRKCT2} = \underset{\sim}{C}'_{ESPRKCT2} = \{0,3 / 0,2; 1 / 0,5; 0,5 / 1\}$;

$\underset{\sim}{T}'_{ESPKCT3} = \underset{\sim}{B}'_{ESPKCT3} = \{0/0,2; 0,5/0,5; 1/1\}$,

$\underset{\sim}{T}'_{ESPKCП1} = \underset{\sim}{H}'_{ESPKCП1} = \{1/0,3; 0,3/0,6; 0/1\}$;

$\underset{\sim}{T}'_{ESPKCП2} = \underset{\sim}{C}'_{ESPKCП2} = \{0,5/0,3; 1/0,6; 0,6/1\}$;

$\underset{\sim}{T}'_{ESPKCП3} = \underset{\sim}{B}'_{ESPKCП3} = \{0/0,3; 0,8/0,6; 1/1\}$.

Відповідно кроку 3 етапу 5 в [8] при реалізації другого кроку в (28) для набору проміжних термів $\underset{\sim}{M}'_{ESPKCБ}$ та $\underset{\sim}{C}'_{ESPKCБ}$ $\exists \underset{\sim}{T}'_{ESPKCБ1} : \{0/x^{min}_{ESPKCБ1}\} \in \varnothing$ і $\exists \underset{\sim}{T}'_{ESPKCБ2} : \{0/x^{min}_{ESPKCБ2}\} \in \varnothing$ ($\mu_{ESPKCБ11} = 1 \neq 0$ та $\mu_{ESPKCБ21} = 0,5 \neq 0$), а для $\underset{\sim}{B}'_{ESPKCБ}$ і $\underset{\sim}{ДВ}'_{ESPKCБ}$ $\exists \underset{\sim}{T}'_{ESPKCБ3} : \{0/x^{max}_{ESPKCБ3}\} \in \varnothing$ та $\exists \underset{\sim}{T}'_{ESPKCБ4} : \{0/x^{max}_{ESPKCБ4}\} \in \varnothing$ (тобто $\mu_{ESPKCБ34} = 0,3 \neq 0$ і $\mu_{ESPKCБ44} = 1 \neq 0$), то формування підмножин $\underset{\sim}{T}^{e}_{ESPKCБ1}$, $\underset{\sim}{T}^{e}_{ESPKCБ2}$ та $\underset{\sim}{T}^{e}_{ESPKCБ3}$, $\underset{\sim}{T}^{e}_{ESPKCБ4}$ здійснимо за рахунок розширення $\underset{\sim}{T}'_{ESPKCБ1}$, $\underset{\sim}{T}'_{ESPKCБ2}$ та $\underset{\sim}{T}'_{ESPKCБ3}$, $\underset{\sim}{T}'_{ESPKCБ4}$ (див. (28) в [8]) шляхом введення додаткових $\mu_{ESPKCБ1\beta-1} / x_{ESPKCБ1\beta-1} = 0/0,25$, $\mu_{ESPKCБ1r_j-\gamma+2} / x_{ESPKCБ1r_j-\gamma+2} = 0/1$ $\mu_{ESPKCБ2\beta-1} / x_{ESPKCБ2\beta-1} = 0/0,25$ та $\mu_{ESPKCБ3r_j-\gamma+2} / x_{ESPKCБ3r_j-\gamma+2} = 0/1$, $\mu_{ESPKCБ4r_j-\gamma+2} / x_{ESPKCБ4r_j-\gamma+2} = 0/1$ відповідно, після чого в НЧ відбувається переіндексація компонент починаючи з першої.

З урахуванням цього, набір проміжних термів для $\underset{\sim}{M}'_{ESPKCБ}$ буде мати наступний вигляд $\underset{\sim}{T}'_{ESPKCБ1} = \underset{\sim}{M}'_{ESPKCБ1} = \{\mu_{ESPKCБ11} / x_{ESPKCБ11}, \mu_{ESPKCБ12} / x_{ESPKCБ12}, \mu_{ESPKCБ13} / x_{ESPKCБ13}, \mu_{ESPKCБ14} / x_{ESPKCБ14}\} = \{0/0,25, 1/0,25; 0,25/0,5; 0/0,75\}$, де $\mu_{ESPKCБ1\beta-1} = 0$. Аналогічним способом отримуємо проміжні терми для $\underset{\sim}{C}'_{ESPKCБ}$, $\underset{\sim}{B}'_{ESPKCБ}$ та $\underset{\sim}{ДВ}'_{ESPKCБ}$, де $\mu_{ESPKCБ2\beta-1} = \mu_{ESPKCБ3r_j-\gamma+2} = \mu_{ESPKCБ4r_j-\gamma+2} = 0$. Таким способом, компоненти підмножини еталонів $\underset{\sim}{T}^{e}_{ESPKCБ1}$ згідно (29) в [8] будуть визначатись як $\mu^{e}_{ESPKCБ11} / x^{e}_{ESPKCБ11} = 0/0,25$, $\mu^{e}_{ESPKCБ12} / x^{e}_{ESPKCБ12} = 1/0,25$, $\mu^{e}_{ESPKCБ13} / x^{e}_{ESPKCБ13} = 0,25/0,5$, $\mu^{e}_{ESPKCБ14} / x^{e}_{ESPKCБ14} = 0/0,75$ та аналогічно для $\underset{\sim}{T}^{e}_{ESPKCБ2}$, $\underset{\sim}{T}^{e}_{ESPKCБ3}$, $\underset{\sim}{T}^{e}_{ESPKCБ4}$.

Далі, згідно (29), в [8] для $\underset{\sim}{M}'_{ESPKCБ1}$, $\underset{\sim}{C}'_{ESPKCБ1}$, $\underset{\sim}{B}'_{ESPKCБ1}$, $\underset{\sim}{ДВ}'_{ESPKCБ1}$ сформуємо еталонні значення, тобто:

$\underset{\sim}{T}^{e}_{ESPKCБ1} = \underset{\sim}{M}^{e}_{ESPKCБ1} = \{0/0,25, 1/0,25; 0,25/0,5; 0/0,75; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCБ2} = \underset{\sim}{C}^{e}_{ESPKCБ2} = \{0/0,25; 0,5/0,25; 1/0,5; 0,5/0,75; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCБ3} = \underset{\sim}{B}^{e}_{ESPKCБ3} = \{0/0,25; 0,25/0,5; 1/0,75; 0,3/1; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCБ4} = \underset{\sim}{ДВ}^{e}_{ESPKCБ4} = \{0/0,5; 0,24/0,75; 1/1; 0/1\}$,

Також аналогічно формуються і наступні еталонні значення:

$\underset{\sim}{T}^{e}_{ESPKCT1} = \underset{\sim}{H}^{e}_{ESPKCT1} = \{0/0,2; 1/0,2; 0,5/0,5; 1/1; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCT2} = \underset{\sim}{C}^{e}_{ESPKCT2} = \{0/0,2; 0,3/0,2; 1/0,5; 0,5/1; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCT3} = \underset{\sim}{B}^{e}_{ESPKCT3} = \{0/0,2; 0,5/0,5; 1/1; 0/1\}$ та

$\underset{\sim}{T}^{e}_{ESPKCП1} = \underset{\sim}{H}^{e}_{ESPKCП1} = \{0/0,3; 1/0,3; 0,3/0,6; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPTKCП2} = \underset{\sim}{C}^{e}_{ESPKCП2} = \{0/0,3; 0,5/0,3; 1/0,6; 0,6/1; 0/1\}$;

$\underset{\sim}{T}^{e}_{ESPKCП3} = \underset{\sim}{B}^{e}_{ESPKCП3} = \{0/0,3; 0,8/0,6; 1/1; 0/1\}$;

Для підмножини еталонів $\mathbf{T}^{e}_{ESPKCБ}$, $\mathbf{T}^{e}_{ESPKCT}$ та $\mathbf{T}^{e}_{ESPKCП}$ з урахуванням отриманих конкретних значень є можливість реалізувати їх графічну інтерпретацію (див. рис. 12-14), скориставшись відповідними еталонами НЧ.

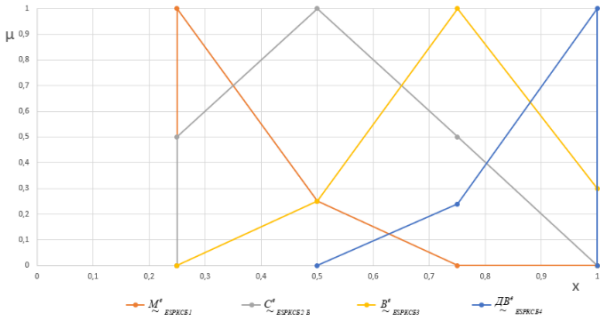


Рис.12 Лінгвістичні еталони для $\mathbf{T}^{e}_{ESPKCБ}$.

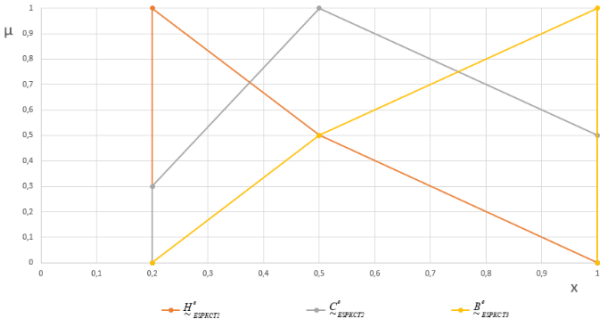


Рис.13 Лінгвістичні еталони для $\mathbf{T}^{e}_{ESPKCT}$

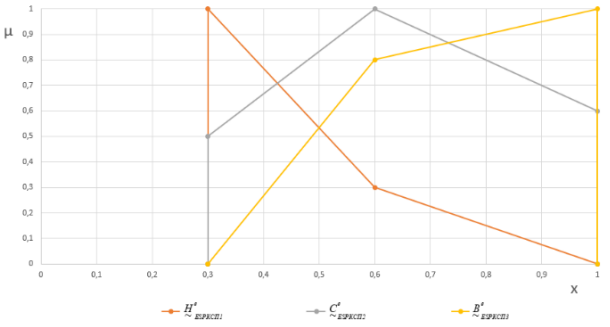


Рис.14 Лінгвістичні еталони для $\mathbf{T}^{e}_{ESPKCП}$

На основі визначених параметрів КСБ, КСТ і КСП та їх сформованих еталонних значень, а також з

урахуванням [15-18, 22] є можливість у подальшому будувати підмножини базових детекційних правил, що використовуватимуться для виявлення email-спуфінг атак.

Запропоновані в роботі моделі, які з використанням експертної оцінки стану інформаційної системи і реалізованого процесу формування еталонів параметрів КСБ, КСТ та КСП, дозволяють формалізувати процес отримання еталонних значень певних величин, що дає можливість побудувати детекційні правила для виявлення email-спуфінг атак.

Подібні моделі можуть бути використані для підвищення ефективності засобів захисту інформації, що спрямовані на протидію email-спуфінг атакам в інформаційних системах.

Література

[1] Новое время. Крупнейшие кибератаки против Украины с 2014 года. Инфографика. URL: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-goda-infografika-1438924.html.

[2] Сегодня. В СБУ рассказали, сколько раз российские спецслужбы атаковали Украину в сети. URL: https://www.segodnya.ua/ukraine/v-sburasskazali-skolko-raz-rossiyskie-specsluzhby-atakovali-ukrainu-v-seti-1152136.html.

[3] А.Г. Корченко. «Построение систем защиты информации на нечетких множествах. Теория и практические решения». К.: МК-Пресс, 2006. 320 с.

[4] А.А. Корченко. «Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах». *Захист інформації.* № 4 (57). 2012. С. 112-118.

[5] А.И. Стасюк, А.А. Корченко. «Базовая модель параметров для построения систем выявления атак». *Захист інформації*. № 2 (55). 2012. С. 47-51.

[6] М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А Охрименко. «Модели эталонов лингвистических переменных для систем выявления атак». *Захист інформації*. № 2 (55). 2012. С. 71-78.

[7] А. Стасюк, А. Корченко. «Метод выявления аномалий порожденных кибератаками в компьютерных сетях». *Захист інформації*. №4 (57). 2012. С. 129-134.

[8] А.А. Корченко. «Метод формирования лингвистических эталонов для систем выявления вторжений».*Захист інформації.* Т.16, №1. 2014. С. 5-12.

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

[10] А.А. Корченко. «Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений». *Захист інформації*. Т.16, №4. 2014. С. 292-304.

[11] А.А. Корченко. «Метод определения идентифицирующих термов для систем обнаружения вторжений». *Безпека інформації*. Т.20, № 3. 2014. С. 217-223.

[12] А.А. Корченко. «Система выявления аномального состояния в компьютерных сетях». *Безпека інформації*. 2012. № 2 (18). С. 80-84.

[13] А.А. Корченко. «Система формирования нечетких эталонов сетевых параметров». *Захист інформації*. 2013. Т.15, №3. С. 240-246.

[14] А.А. Корченко. «Система формирования эвристических правил для оценивания сетевой активности». *Захист інформації*. 2013. №4. Т.15. С. 353-359.

[15] А.А. Корченко. «Кортежная модель формирования набора базовых компонент для выявления кибератак». *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2014. В.2 (28). С. 29-36.

[16] A. Korchenko. K. Warwas, A. Kłos-Witkowska. «The Tupel Model of Basic Components' Set Formation for Cyberattacks». *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015)*, Warsaw, Poland. September 24-26, 2015. Vol. 1. PP. 478-483.

[17] . М. Карпинский, А. Корченко, С. Ахметова. «Метод формирования базовых детекционных правил для систем обнаружения вторжений». *Захист інформації*. 2015. №4. Т.17. С. 312-324.

[18] A. Korchenko. K. Warwas, A. Kłos-Witkowska. «The Tupel Model of Basic Components' Set Formation for Cyberattacks». *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015).* Warsaw, Poland. September 24-26, 2015. Vol. 1. PP. 478-483.

[19] А. Корченко, В. Щербина, Н. Вишневская. «Методология построения систем выявления аномалий порожденных кибератаками». *Захист інформації*. 2016. №1. Т.18. С. 30-38.

[20] B. Akhmetova, A. Korchenko, S. Akhmetova, N. Zhumangalieva. «Improved method for the formation of linguistic standards for of intrusion detection systems». *Journal of Theoretical and Applied Information Technology*, 2016. Vol.87. №.2. PP. 221-232.

[21] А. Корченко, Н. Жумангалиева, П. Викулов. «Построение лингвистических эталонов для выявления сниффинг атак». Актуальні питання забезпечення кібербезпеки та захисту інформації. ІІІ міжнар. наук.-практ. конф. Тези доп. Київ, 22-25 лютого 2017 р. С. 93-97.

[22] M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan. «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection». *Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017*), Romania, Bucharest. September 21-23, 2017: Vol. 1. PP. 258-264.

[23] B. Akhmetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva. «Improved method for the formation of linguistic standards for of intrusion detection systems». *Journal of Theoretical and Applied Information Technology*. 2016. Vol.87. No.2. PP. 221-232.

[24] И. Терейковский, А. Корченко, П. Викулов, А. Шаховал. «Модели эталонов лингвистических переменных для обнаружения сниффинг-атак». *Захист інформації*. 2017. №3. Т.19. С. 228-242.

[25] MX Tool Box SuperTool 7 Network Tools. URL: https://mxtoolbox.com/SuperTool.aspx.

[26] Local News: Subject Line tool. URL: http://www.localnews.biz/subjectLine/ValidateSubjectLine.asp.

УДК 004.056.53(045)

Терейковский И.А., Корченко А.А., Викулов П.А., Ирейфидж Имад Исса Джамиль. Модели эталонов лингвистических переменных для систем обнаружения email-спуфинг-атак

Аннотация. *Развитие информационных систем в современном мире неразрывно связано с совершенствованием деструктивного программного обеспечения, которое направлено на различные ресурсы информационных систем. Среди различных способов воздействия на пользователя особенно опасны те, что с помощью маскировки под реально существующее программное обеспечение или web-сервис пытаются получить доступ к персональным данным пользователя, использовать его ресурсы или программное обеспечение в мошеннических целях. Активизация подобных атак требует создания специализированных средств обнаружения и противодействия, которые будут одинаково эффективны как против имеющихся, так и будущих киберугроз с неустановленными или нечетко определенными свойствами. То есть подобные средства могут функционировать в нечеткой, слабоформализованной среде. Современные методы, модели и системы, основанные на нечетких множествах могут быть использованы для построения и совершенствования имеющихся средств обнаружения вторжений и аномалий в информационных системах, возникающих в результате реализации киберугроз. Есть ряд разработок, используемых при их обнаружении, одной из которых является метод формирования лингвистических эталонов для систем обнаружения вторжений. В описанном методе не раскрыт механизм процесса формирования эталонов параметров для email-спуфинг-атак. С учетом этого, разработана модель эталонов лингвистических переменных для выявления email-спуфинг-атак, которая позволит формализовать процесс получения эталонов параметров (количество выявленных IP-адресов в спам-базах, количество спам-слов в теме, количество спам-слов в сообщении) для заданных лингвистических переменных определенной среды окружения при решении задач выявления атак. Подобные модели могут быть использованы для повышения эффективности средств защиты информации, направленных на противодействие email-спуфинг атакам в информационных системах.*

Ключевые слова: *атаки, кибератаки, аномалии, методы формирования лингвистических эталонов, системы обнаружения вторжений, системы обнаружения атак, выявление аномалий в информационных системах.*

Tereykovsky I., Korchenko A., Vikulov P., Ireifej Imad Issa Jamil. Etalons models of linguistic variables for email-spoofing-attack detection systems

Abstract. *The development of information systems in the modern world is inextricably linked with the improvement of destructive software, which is aimed at the various resources of information systems. Among the various ways to influence the user, the most dangerous are those that masking by under the really existing software or web service and are trying to access the personal data of the user, or use its resources or software for fraudulent purposes. The activation of such attacks requires the creation of specialized means of detection and counteraction, which will be equally effective against both present and future cyber threats with unidentified or unclearly defined properties. That is, similar means can function in a fuzzy, poorly formalized environment. Modern methods, models and systems based on fuzzy sets can be used to construct and improve existing tools for detecting intrusions and anomalies in information systems that arise as a result of the implementation of cyber threats. There are a number of developments that are used when they are detected, one of which is the method of forming linguistic etalons for intrusion detection systems. In the described method, the mechanism of the process of forming parameters etalons for email spoofing attacks is not disclosed. With this in mind, a model of linguistic variables etalons was developed for detecting email spoofing attacks, which would formalize the process of obtaining parameter benchmarks. (the number of detected IP addresses in spam bases, the number of spam words in the topic, the number of spam messages in the message) for given linguistic variables of the selected environment when solving problems, in relation to detection of attacks. Similar models can be used to increase the effectiveness of information security measures aimed at countering email spoofing attacks in information systems.*

Key words: *attacks, cyber attacks, anomalies, methods of forming linguistic etalons, intrusion detection systems, attack detection systems, detection of anomalies in information systems.*

Отримано 16 *червня 2018 року*, затверджено редколегією *30 червня 2018 року*