Annals of Computer Science, 2021, vol 31 (1), pp. 23-29.
[9] Mathew G., Thomas S., PG Scholar. A novel multi-factor authentication system ensuring usability and security, The Journal arXiv of Computer Science, 2021.
[10] AlJanah, S., Zhang, N., & Tay, S. W. A Multifactor Multilevel and Interaction Based (M2I) AuthenticationFramework for Internet of Things (IoT) Applications. IEEE Access, 2022, vol 10, pp. 47965-47996.
[11] Ahmed S., Mahmood Q. An authentication based scheme for applications using JSON web token. International Conference on Computer and Information Sciences (ICCIS), 2021, pp. 1-6.
[12] Drakonakis K., Ioannidis S., Polakis J. The Cookie Hunter: Automated Black-box Auditing for Web Authentication and Authorization Flaws. ACM SIGSAC Conference on Computer and Communications Security (CCS '20), 2020, pp. 1953-1970.
[13] Ben Fredj, Cheikhrouhou O., Krichen M., Hamam H., Derhab A. An OWASP Top Ten Driven Survey on Web Application Protection Methods. International Conference on Cyber Security and Protection of Digital Services (CRiSIS), 2021, pp. 189-201.
[14] Erdodi L., Zennaro F. M. The Agent Web Model: modeling web hacking for reinforcement learning. International Journal of Information Security volume, 2022, vol 21, pp. 293-309.

TO THE ISSUE OF SECURE MULTIFACTOR AUTHENTICATIONIN WEB APPLICATIONS

The main segments of the smart city infrastructure using authentication in the security vector of Industry 4.0 technologies are considered. Approaches to secure authentication, in particular in WEB applications, are analyzed. A comparison of authentication methods in WEB applications by requirements and level of data security is made. Authentication threats, mechanisms and technologies of protection are analyzed and, on this basis, a system model of secure multifactor authentication in a WEB application based on the concept of "object – threat – protection" according to the structure "WEB page – WEB server – database" is created. An algorithmic and software implementation of a secure multi-factor authentication system in a WEB application based on the use of the SHA-1 cryptographic hash function and the AES symmetric message encryption algorithm using the JavaScript programming language is developed. The practical implementation of a step-by-step algorithm for multifactor authentication in WEB applications by factors such as login and password, fingerprint, and smartphone is presented.
Keywords: multifactor authentication, security, WEB application, system model, hash function, message encryption algorithm.

Дудикевич Валерій Богданович, д.т.н., професор, завідувач кафедри Національного університету «Львівська політехніка», Львів, Україна.
Valerii Dudykevych, Doctor of Technical Sciences, Professor, Head of Department of Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: vdudykev@gmail.com.
Orcid ID: 0000-0001-8827-9920.

Микитин Галина Василівна, д.т.н., професор, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.
Halyna Mykytyn, Doctor of Technical Sciences, Professor, Professor of Department of Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: cosmos-zirka@ukr.net.
Orcid ID: 0000-0003-4275-8285.

Насилевський Володимир Павлович, інженер-програміст компанії "SoftServe", Львів, Україна.
Volodymyr Nasylevskyi, Software Engineer at SoftServe, Lviv, Ukraine.
E-mail: bobbyf4de@gmail.com.
Orcid ID: 0009-0003-0203-4087.

Фігурняк Володимир Русланович, Магістрант, Національний університет «Львівська політехніка», Львів, Україна.
Volodymyr Fihurniak, Master's student, Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: volodymyr.fihurniak@gmail.com.
Orcid ID: 0009-0005-6695-0521.

DOI: 10.18372/2410-7840.25.17757
УДК 004.054

МЕТОД ФОРМУВАННЯ ЕТАЛОННОГО СУБДОВКІЛЛЯ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ URL-АДРЕС

Анна Корченко, Євгенія Іванченко, Сатибалдієва Феруза, Жумангалієва Назим

Збільшення та удосконалення кібератак на інформаційні системи зростає щорічно, а використання сучасних систем виявлення вторгнень дозволяє швидко реагувати на нові види кібератак та вдосконалювати існуючі

засоби захисту. Такі системи достатньо розвинуті, але для їх ефективної роботи необхідна інформація у режимі реального часу, з використанням якої можливо виявляти підозрілу активність неавторизованої сторони. Таку інформацію можна проаналізувати з використанням експертних підходів. Експертні методи можуть допомогти виявляти нові неочікувані кібератаки. Використання методів, моделей і систем на основі теорії нечітких множин при побудові засобів виявлення аномалій, породжених реалізацією нових кіберзагроз, дозволить удосконалити та зробити більш ефективними існуючі системи виявлення вторгнень. А розробка відповідних технічних рішень, що працюють в нечітких умовах, дозволить виявляти раніше не відомі та модифіковані види кібератак. Також є досить ефективні розробки, які використовуються для вирішення завдань виявлення кібератак, наприклад, низка методів формування еталонного субдовкілля для системи виявлення вторгнень, але вони не орієнтовані на фішингові підходи. Однак, як показує практика, при появі нових загроз та відповідних аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними, тому розробка методів, що дозволяють удосконалити процес отримання нового еталонного субдовкілля для системи виявлення вторгнень, є актуальним завданням. Одним із небезпечних засобів, який направлений на збір конфіденційної інформації, такої як логіни, паролі, фінансові реквізити та інші особисті дані є фішинг. Для цього розроблений метод формування еталонного субдовкілля для виявлення фішингових URL-адрес за рахунок сформованого набору параметрів: кількість країн за IP-адресою, вік домену та експертного оцінювання стану субдовкілля інформаційної системи дозволить формалізувати процес формування параметрів еталонного субдовкілля для вирішення задач, щодо виявлення фішингових URL-адрес.

Ключові слова: *атаки, кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, системи виявлення кібератак, виявлення аномалій в комп'ютерних мережах.*

ВСТУП

Розвиток сучасних систем виявлення вторгнень (СВВ) є надзвичайно актуальним, оскільки інтернет-злочинність стає все більшою проблемою для бізнесу та приватних користувачів. Кількість кібератак та вторгнень в інформаційні системи (ІС) зростає щорічно. Це призводить до значних втрат фінансових та матеріальних ресурсів, а також порушення базових характеристик безпеки ресурсів інформаційних систем.

Розвиток сучасних СВВ дозволяє вчасно виявляти та запобігати кібератакам, що зменшує ризик для компаній та приватних користувачів. Також ці системи дозволяють швидко реагувати на нові види кібератак та вдосконалювати заходи захисту, а також направлені на забезпечення безпеки в інтернет-довкіллі та зменшення ризиків від реалізації кібератак.

Також, функціональність сучасних систем виявлення та блокування вторгнень залежить від їх можливостей щодо виявлення нових кібератак у режимі реального часу, що наприклад, може включати такі елементи як:

1. Моніторинг системи – дає можливість виявити несправності та неочікувані поведінки в комп'ютерних системах. Це може включати аналіз змін у файловій системі, перехоплення мережевого трафіку та аналіз поведінки програм;

2. Виявлення уразливостей – дає можливість забезпечити вчасну реакцію на потенційну кібератаку. Для цього можна використовувати програмні засоби, які виявляють уразливості в операційній системі, веб-сайтах та програмних застосунках;

3. Системи виявлення вторгнень – дають можливість допомогти виявити незвичайну активність в мережі, яка може вказувати на кібератаку. Це може включати використання сигнатур, які описують відомі види атак, або аналіз поведінки в мережі;

4. Машинне навчання – дає можливість допомогти виявляти нові види кібератак, які не були відомі раніше. Для цього можуть використовуватись алгоритми, які навчаються на базі даних про відомі кібератаки та їх характеристики;

5. Аналіз журналів подій – дають можливість допомогти виявити незвичайну активність в комп'ютерній системі. Це може включати аналіз журналів подій операційних систем, веб-серверів та інших програмних застосунків тощо.

Такі сучасні системи достатньо розвинуті, але для їх ефективної роботи необхідна відповідна інформація у режимі реального часу, за допомогою якої можливо виявляти підозрілу активність неав-

торизованої сторони (НАС). Таку інформацію можна проаналізувати з використанням експертних підходів [1-2]. Експерти можуть дати оцінку можливим наслідкам конкретної кібератаки. Експертні методи використовуються для аналізу даних щодо стану кібербезпеки та виявлення тенденцій у злочинній діяльності НАС. Враховуючи швидкі темпи розвитку кіберзагроз та постійну зміну підходів НАС, експертні методи можуть допомогти виявляти нові неочікувані кібератаки, а також можуть бути корисні при розробці стратегій захисту та покращення загального стану кібербезпеки.

Використання методів, моделей і систем на основі теорії нечітких множин [1-2] при побудові засобів виявлення аномалій, породжених реалізацією нових кіберзагроз, дозволить удосконалити та зробити більш ефективними існуючі СВВ.

Зазначена теорія дозволяє враховувати певні нечіткості та невизначеності в стані системи, що може бути корисним при розробці засобів виявлення кібератак, які можуть мати нечіткий чи непередбачуваний характер.

Застосування методів теорії нечітких множин дозволяє покращити ефективність систем виявлення кібератак та зменшити кількість помилкових спрацювань. Наприклад, використання нечіткої логіки може дозволити виявляти аномальну поведінку користувачів, яка відповідає типовим шаблонам і може свідчити про можливу кібератаку.

Тобто, розробка відповідних технічних рішень, що працюють в нечітких умовах, дозволить виявляти раніше не відомі та модифіковані види кібератак.

На сьогодні, є досить ефективні розробки, які використовуються для вирішення завдань виявлення кібератак, наприклад, низка методів формування еталонних підсередовищ для СВВ [3-9], але вони не орієнтовані на фішингові підходи.

Однак, як показує практика, при появі нових загроз та відповідних аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними, тому розробка методів, що дозволяють удосконалити процес отримання нового еталонного субдовкілля для СВВ, є актуальним завданням.

Одним із небезпечних засобів, який направлений на збір конфіденційної інформації, такої як логіни, паролі, фінансові реквізити та інші особисті дані є фішинг. Фішингові кібератаки часто пов'язані зі створенням фальшивих веб-сайтів, розсилкою певних електронних листів або повідомлень, щоб неправомірним чином отримати інформацією від користувачів.

Зазвичай фішинг-кібератаки використовують маніпуляції та соціальну інженерію, щоб надихнути жертву на дії, які допоможуть НАС отримати доступ до конфіденційної інформації. Основна ознака фішингу полягає в тому, що НАС намагається ввести в оману жертву, вдаючись за правомірного власника інформації або використовуючи ім'я довіреного джерела, наприклад, банку або компанії.

ОСНОВНА ЧАСТИНА

Фішинг-кібератаки можуть бути спрямовані на користувачів електронної пошти, соціальних мереж, банківських систем та інше, а її цілі залежать від того, хто є НАС і що вона намагається отримати. Можемо виділити наступні цілі фішингу:

1. Отримання конфіденційних даних (НАС може створювати фальшиві веб-сайти, електронні листи або повідомлення, щоб збирати логіни, паролі, номери кредитних карток, ідентифікаційний номер);

2. Викрадення грошей (атаки можуть бути спрямовані на отримання фінансової інформації, щоб здійснити незаконний доступ до банківських рахунків або кредитних карток);

3. Злам систем безпеки (використання фішинг-кібератаки для отримання доступу до комп'ютерів або систем безпеки для заволодіння конфіденційною інформацією або встановлення шкідливого програмного забезпечення);

4. Розповсюдження шкідливого програмного забезпечення (НАС може поширювати віруси, троянські програми або інше шкідливе програмне забезпечення серед користувачів);

5. Ослаблення репутації (використання фішинг-кібератаки для поширення неправдивої або негативної інформації про певну компанію або особу) тощо [10].

Для виявлення фішингу можна скористатися низкою ознак (параметрів), наприклад:

1. Посилання на сайт (домен). Необхідно перевіряти URL-адресу сайту, на яку пропонується

перейти. Як правило, фішинг передбачає імітування легітимних сайтів, тому необхідно бути переконаним, що URL-адреса дійсно відповідає організації, з якої очікується отримати повідомлення. Вони можуть виглядати так само, як повідомлення від реальних компаній, але домен може відрізнятися від того, який використовується компанією. Наприклад, НАС може створювати сайти, що схожі на легітимні, але з частково зміненою URL-адресою, наприклад, замість «paypal.com» вони можуть створити «paypa1.com». У такому разі важливо перевіряти URL-адресу на правопис та використання правильного домену;

2. Запити до особистих даних (запит на конфіденційну інформацію). НАС може намагатися отри-мати певну інформацію, наприклад, фішери надсилають електронні листи або створюють сторінки, які запитують персональні дані та іншу конфіденційну інформацію, таку як ім'я, електронна пошта, номери кредитних карток, паролів тощо. Оскільки легітимні організації зазвичай не запитують особисті дані від користувачів у повідомленнях електронної пошти, то слід ігнорувати будь-які запити на надання конфіденційної інформації через пошту чи сторінки, які виглядають підозріло;

3. Недостовірні файли. Не слід відкривати недовірені файли, що приходять електронною поштою. Фішери часто здійснювати таку розсилку зі шкідливими програмами, які можуть пошкодити комп'ютер або викрасти особисті дані;

4. Зміст повідомлення (граматика та орфографія). Фішингові повідомлення можуть містити навмисні помилки в орфографії або граматиці, незвичайний тон чи спосіб форматування. Легітимні компанії зазвичай не роблять таких помилок. Фішери можуть також намагатися створити емоційну або психологічну обстановку, щоб змусити атаковану особу здійснити дії, що не відповідає її інтересам або потребам;

5. Джерело повідомлення. Слід бути повністю переконаним, щодо аутентичності відправника повідомлення, або що доменна адреса відповідає організації, з якої очікується отримати повідомлення;

6. Відсутність персоналізації. Фішингові повідомлення зазвичай не містять особистої інформації про отримувача. Якщо приходить повідомлення, яке не містить ідентифікаторів отримувача або іншої особистої інформації, то це може бути ознакою фішингу;

7. Відсутність відомостей про компанію. Якщо не вдається знайти інформацію про компанію, яка надіслала повідомлення, то це також може бути ознакою фішингу;

8. Неочікувані повідомлення. Якщо отримується повідомлення від джерела, з якого раніше не було контакту, то це теж може бути ознакою фішингу.

Для виявлення описаної кібератаки, далі, наприклад, за допомогою сервісів Phishtank – http://phishtank.org/ (використовується для виявлення фішингових сайтів), Whois – https://who.is (використовується для визначення інформації про доменне ім'я сайту) та GeoIP – https://www.maxmind.com/en / geoip-demo (використовується для визначення місцезнаходження веб-сайтів) зберемо інформацію про 150 чистих та фішингових URL-адрес за такими параметрами, як от «Кількість країн за IP-адресою» (за допомогою пінгового доменного імені отримаємо IP-адресу) та «Вік домену», який обчислюється за виразом ЗТД-СД=ТД, де ЗТД – дата закінчення терміну дії домену, СД – дата створення домену, ТД – термін дії домену. Отримані результати відповідних URL-адрес згрупуємо у таблицю 1.

На основі отриманих даних (з урахуванням [1] (див. п. 2.2) та [6]), для параметру «Вік домену» (Domain age – (DA)) візьмемо наступні інтервали, які наглядно показують діапазони мінімальних, середньо допустимих та максимальних значень для визначеної величини.

Виходячи з цього, найбільш коректним буде визначення максимального значення для параметра DA – 30.

Для параметра «Кількість країн за IP-адресою» (Number of countries – (NC)) доцільно використовувати п’ять термів з наступними інтервалами та максимальним значення параметра NC – 50.

Далі, з використанням цих значень створимо поточні (табл. 1-2) та частотні таблиці (табл. 3-8) для кожного параметра для чистих і фішингових URL-адрес.

Таблиця 1

Поточна таблиця легітимних URL-адрес

№	Легітимні URL-адреса	Термін дії домену (років)	Країна за IP-адресою
1	https://Taobao.com	21	China, Asia
2	https://www.name.com	26	US, North America
3	http://obozrevatel.com/	22	Ukraine, Europe
4	https://www.starlink.com/	29	US, North America
5	http://www.pitchforkmedia.com	24	US, North America
6	https://baidu.com	27	China, Asia
7	https://instagram.com	27	US, North America
8	https://twitter.com	23	US, North America
9	https://yahoo.com	28	US, North America
10	https://amazon.com	30	US, North America
11	https://netflix.com	26	US, North America
12	http://gismeteo.ua/	18	Ukraine, Europe
13	https://ebay.com	28	US, North America
14	https://bing.com	27	US, North America
15	https://linkedin.com	22	US, North America
16	https://whatsapp.com	23	US, North America
17	https://aliexpress.com	18	China, Asia
18	https://sogou.com	30	China, Asia
19	https://pinterest.com	15	US, North America
20	https://office.com	24	US, North America
21	https://msn.com	29	US, North America
22	https://naver.com	26	South Korea, Asia
23	https://twitch.tv	15	US, North America
24	https://paypal.com	24	US, North America
25	https://craigslist.org	27	US, North America
26	https://github.com	17	US, North America
27	https://www.aicc.org/	27	US, North America
28	https://Reddit.com	19	US, North America
29	http://www.aerofiles.com/	24	US, North America
30	https://rozetka.com.ua	26	Ukraine, Europe
31	https://olx.ua	10	India, Asia
32	https://prom.ua	15	Canada
33	https://privatbank.ua	23	India, Asia
34	https://ukr.net	28	US
35	https://telegram.org	28	US, North America
36	https://sinoptik.ua	14	China, Asia
37	https://epicentrk.ua	8	Australia, Oceania
38	https://allo.ua	11	Canada
39	https://work.ua	11	Cyprus, Europe
40	https://tabletki.ua	19	Canada
…	…	…	…
150	https://www.bilibili.com	27	China, Asia

Таблиця 2

Поточна таблиця фішингових URL-адрес

№	Фішингові URL-адреса	Термін дії домену (років)	Країна за IP-адресою
1	https://joktauninvest.pro	1	Texas, US, North America
2	https://defi-aa-vev3.co/#/	1	US, North America
3	https://caring-jay.cloudvent.net/	1	US, North America
4	http://andriyivsky.space/	3	Ukraine, Europe
5	https://x2y2nft.pro/	1	US, North America
6	https://raydium-io.ex-change/	1	US, North America
7	https://tonhold.com/	1	US, North America
8	https://apple-wallet-up-date-uk.com/	1	Malaysia, Asia
9	http://auth-webs.com	1	Nairobi, Nairobi Province, Kenya, Africa

10	https://mkbhu-login.com/	1	US, North America
11	http://metamaska.cc/	1	Hong Kong, Asia
12	https://dbs-myverifications-sg.com/	1	Ashburn, Virginia, US
13	https://leboncoinssl.com/	1	US, North America
14	http://tv-magazineluiza.com	1	Campinas, Sao Paulo, Brazil, South America
15	http://auth-webs.com	1	Nairobi, Nairobi Province, Kenya, Africa
16	https://magicedeni.io/	1	North Charleston, South Carolina, US, North America
17	https://magic-eben.com/	1	US, North America
18	https://magicedeni.io/	1	North Charleston, South Carolina, US, North America
19	https://dbs-myverifications-sg.com/	1	US, North America
20	https://leboncoinssl.com/	1	US, North America
21	https://leboncoinssl.com/	1	US, North America
22	https://www.camenergy.org	8	Malaysia, Asia
23	https://www.poocoinappd.info/	1	Belize, North America
24	http://www.rodhaninvesting.pro	1	US, North America
25	https://www.rodhaninvesting.pro/	1	US, North America
26	https://photoresis.com/	1	russia, Europe
27	https://www.marklokdinvest.pro/	1	US, North America
28	https://opensea.tv/	3	Singapore, Asia
29	https://www.hordasinvest.pro/	1	Malaysia, Asia
30	https://wfi290jvkas.club/	1	US, North America
31	https://rodhaninvesting.pro	1	Texas, US, North America
32	https://marklokdinvest.pro	1	Texas, US, North America
33	https://hordasinvest.pro	1	Texas, US, North America
34	https://joktauninvest.pro	1	US, North America
35	https://unismoveis.com	1	Rio de Janeiro, Brazil, South America
36	http://rodhaninvesting.pro/	1	Texas, US, North America
37	https://marklokdinvest.pro/	1	Texas, US, North America
38	https://rodhaninvesting.pro	1	Texas, US, North America
39	https://hordasinvest.pro	1	Texas, US, North America
40	https://marklokdinvest.pro	1	Texas, US, North America
…	…	…	…
150	https://joktauninvest.pro	1	Texas, US, North America

Таблиця 3

Термін дії домену (чисті сайти)

Інтервал	Частота
1-10	12
11-20	42
21 30	96

Таблиця 4

Кількість країн (чисті сайти)

Країна	Кількість країн
Australia	18
Asia	23
Canada	13
Europe	7
Ukraine, Europe	32
US, North America	48
US, South America	9

Таблиця 5

Країна реєстратор (чисті сайти)

Інтервал	Частота
1-10	2
11-20	2
21-30	1
31-40	1
41-50	1

Таблиця 6

Термін дії домену (фішингові сайти)

Інтервал	Частота
1-10	146
11-20	3
21 30	1

Таблиця 7

Кількість країн (фішингові сайти)

Країна	Кількість країн
Africa	8
Asia	18
Europe	14
North Charleston, North America	21
Texas, North America	30
US, North America	50
US, South America	9

Таблиця 8

Країна реєстратор (фішингові сайти)

Інтервал	Частота
1-10	2
11-20	2
21-30	2
31-40	0
41-50	1

Виходячи з цього, метою роботи є розробка методу формування еталонного субдовкілля для виявлення фішингових URL-адрес (МФЕФ). Це дозволить формалізувати процес отримання еталонів параметрів для конкретних лінгвістичних змінних визначеного довкілля (середовища оточення) при ви-рішенні задач щодо виявлення фішингових кібератак. Для розробки МФЕФ скористаємося відомим МФЕС, який заснований на теорії нечітких множин та експертних підходах [6, 11].

З урахуванням цього, сформуємо підмножину ідентифікаторів (ІД) суджень експертів при $n=1$ для кібератаки («Фішинг» – Phishing (Ph)) з ІД $CA_1 = CA_{Ph} = Ph$ $(m_1 = 2,\ r_1 = 5,\ r_2 = 3)$ відповідно до етапу 1 виразу (2.30) (див. п. 2.2) в [1] та [3, 6]:

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

$$\{\{LE_{PhNC1},\ LE_{PhNC2},\ LE_{PhNC3},\ LE_{PhNC4},\ LE_{PhNC5}\},$$

$$\{LE_{PhDA1},\ LE_{PhDA2},\ LE_{PhDA3}\}\} =$$

$$\{\{"ДМ",\ "М",\ "С",\ "В",\ "ДВ"\},$$

$$\{"МЛ",\ "СР",\ "СТ"\}\},$$

де:

- $LE_{PhNC1} = "ДМ"$ – «ДУЖЕ МАЛЕ (ДМ)»;
- $LE_{PhNC2} = "М"$ – «МАЛЕ (М)»;
- $LE_{PhNC3} = "С"$ – «СРЕДНЕ (С)»;
- $LE_{PhNC4} = "В"$ – «ВЕЛИКЕ (В)»;
- $LE_{PhNC5} = "ДВ"$ – «ДУЖЕ ВЕЛИКЕ (ДВ)»;
- $LE_{PhDA1} = "МЛ"$ – «МОЛОДИЙ (МЛ)»;
- $LE_{PhDA2} = "СР"$ – «СЕРЕДНІЙ (СР)»;
- $LE_{PhDA3} = "СТ"$ – «СТАРИЙ (СТ)».

Відповідно є ІД лінгвістичних оцінок експерта, які відображають стан параметрів $P_{PhNC} = NC$ («Кількість країн за IP-адресою» – Number of countries (NC)) та $P_{PhDA} = DA$ («Вік домену» – Domain age (DA)) в *2*-вимірному параметричному субдовкіллі ($\mathbf{P_i = P_{Ph}}$) [1, 12-14].

Наступним, відповідно до етапу 2 (див. п. 2.2 в [1]) необхідно сформувати базову матрицю частот.

Для цього побудуємо підмножину ІД інтервалів $\mathbf{N_{ij}}$ $(j = \overline{1,m_i})$ (див. (2.35) в [1]), що характеризують кібератаку з ІД $CA_1 = CA_{Ph} = Ph$, на області визначення яких експерт здійснює лінгвістичну оцінку відносно значень параметрів P_{PhNC} та P_{PhDA} (див. п. 2.1 в [1]).

При $n=1,\ m_1=2,\ r_1=5,\ r_2=3$ отримаємо:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}}\mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{1}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{N_{ij}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{k_j} N_{ijk}\}\}\} =$$

$$\{\{N_{PhNC1},\ N_{PhNC2},\ N_{PhNC3},\ N_{PhNC4},\ N_{PhNC5}\},$$

$$\{N_{PhDA1},\ N_{PhDA2},\ N_{PhDA3}\}\}.$$

З урахування елементів підмножин $\mathbf{LE_{ij}}$ та $\mathbf{N_{ij}}$ на основі узагальнювальної матриці (див. табл. 2.1 в [1]) побудуємо поточні оцінки (див. табл. 9-10) за елементами підмножин LE_{PhNCk} $(r_1 = 5,\ k = \overline{1,5})$, N_{PhNCk}, тобто:

- $N_{PhNC1} = [N^{min}_{PhNC1}; N^{max}_{PhNC1}] \Leftrightarrow [0;10]$;
- $N_{PhNC2} = [N^{min}_{PhNC2}; N^{max}_{PhNC2}] \Leftrightarrow [11;20]$;

- $N_{PhNC3} = [N^{min}_{PhNC3}; N^{max}_{PhNC3}] \Leftrightarrow [21;30];$
- $N_{PhNC4} = [N^{min}_{PhNC4}; N^{max}_{PhNC4}] \Leftrightarrow [31;40];$
- $N_{PhNC5} = [N^{min}_{PhNC5}; N^{max}_{PhNC5}] \Leftrightarrow [41;50];$
- LE_{PhDAk} $(r_2 = 3,\ k = \overline{1,3}),\ N_{PhDAk}$.

З цього:

- $N_{PhDA1} = [N^{min}_{PhDA1}; N^{max}_{PhDA1}] \Leftrightarrow [0;10];$
- $N_{PhDA2} = [N^{min}_{PhDA2}; N^{max}_{PhDA2}] \Leftrightarrow [11;20];$
- $N_{PhDA3} = [N^{min}_{PhDA3}; N^{max}_{PhDA3}] \Leftrightarrow [21;30]$.

Таблиця 9

Поточна таблиця оцінок за $\mathbf{LE_{PhNC}}$

$\mathbf{LE_{PhNC}}$	$\mathbf{N_{PhNC}}$				
	N_{PhNC1}	N_{PhNC2}	N_{PhNC3}	N_{PhNC4}	N_{PhNC5}
“ДМ”	5	2	0	0	0
“М”	2	4	1	0	0
“С”	0	2	3	3	0
“В”	0	0	2	5	2
“ДВ”	0	0	0	3	4

Таблиця 10

Поточна таблиця оцінок за $\mathbf{LE_{PhDA}}$

$\mathbf{LE_{PhDA}}$	$\mathbf{N_{PhDA}}$		
	N_{PhDA1}	N_{PhDA2}	N_{PhDA3}
“МЛ”	8	2	2
“СР”	1	3	2
“СТ”	0	1	3

Далі, з урахуванням даних таблиць 9-10, а також виразу (2.36) в [1], сформуємо матриці частот (при $n=1,\ m_1=2,\ s,q=\overline{1,r_1},\ s,q=\overline{1,r_2}$):

$$F_{11} = F_{PhNC} = \left\| f_{11sq} \right\| =$$

$$\left\| \begin{matrix} f_{1111} & f_{1112} & f_{1113} & f_{1114} & f_{1115} \\ f_{1121} & f_{1122} & f_{1123} & f_{1124} & f_{1125} \\ f_{1131} & f_{1132} & f_{1133} & f_{1134} & f_{1135} \\ f_{1141} & f_{1142} & f_{1143} & f_{1144} & f_{1145} \\ f_{1151} & f_{1152} & f_{1153} & f_{1154} & f_{1155} \end{matrix} \right\| = \left\| \begin{matrix} 5 & 2 & 0 & 0 & 0 \\ 2 & 4 & 1 & 0 & 0 \\ 0 & 2 & 3 & 3 & 0 \\ 0 & 0 & 2 & 5 & 2 \\ 0 & 0 & 0 & 3 & 4 \end{matrix} \right\|,$$

$$F_{12} = F_{PhDA} = \left\| f_{12sq} \right\| = \left\| \begin{matrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{matrix} \right\| = \left\| \begin{matrix} 8 & 2 & 2 \\ 1 & 3 & 2 \\ 0 & 1 & 3 \end{matrix} \right\|.$$

Наступним, для формування похідної матриці частот (при $n=1,\ m_1=2$) побудуємо, за відповідними стовпцями матриць F_{PhNC} і F_{PhDA} з урахуванням виразу (2.38) в [1], вектори сум:

$$VS_{PhNC} = \left\| vs_{PhNCq} \right\| =$$

$$\left\| vs_{PhNC1}, vs_{PhNC2}, vs_{PhNC3}, vs_{PhNC4}, vs_{PhNC5} \right\| =$$

$$\left\| \bigcup_{q=1}^{5} \sum_{s=1}^{5} f_{PhNCsq} \right\| = \left\| 7,8,6,11,6 \right\|,\ (q = \overline{1,5}),$$

$$VS_{PhDA} = \left\| vs_{PhDAq} \right\| = \left\| vs_{PhDA1}, vs_{PhDA2}, vs_{PhDA3} \right\| =$$

$$\left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{PhDAsq} \right\| = \left\| 9,6,7 \right\|,\ (q = \overline{1,3}).$$

З урахуванням (2.39) в [1] з VS_{PhNC} і VS_{PhDA} визначимо максимальний елемент:

$$vsm_{PhNC} = \bigvee_{q=1}^{5} vs_{PhNCq} =$$

$$vs_{PhNC1} \vee vs_{PhNC2} \vee vs_{PhNC3} \vee vs_{PhNC4} \vee vs_{PhNC5} =$$

$$7 \vee 8 \vee 6 \vee 11 \vee 6 = vsm_{PhNC} = 11,$$

$$vsm_{PhDA} = \bigvee_{q=1}^{3} vs_{PhDAq} = vs_{PhDA1} \vee vs_{PhDA2} \vee vs_{PhDA3} =$$

$$9 \vee 6 \vee 7 = vsm_{PhDA} = 9.$$

Відповідно до (2.40) в [1] отримаємо похідну матрицю частот:

$$F'_{PhNC} = (vsm_{PhNC} / vsm_{PhNCq}) F_{PhNC} =$$

$$\left\| \begin{matrix} 7,9 & 2,8 & 0 & 0 & 0 \\ 3,1 & 5,5 & 1,8 & 0 & 0 \\ 0 & 2,8 & 5,5 & 3 & 0 \\ 0 & 0 & 3,7 & 5 & 3,7 \\ 0 & 0 & 0 & 3 & 7,3 \end{matrix} \right\|,$$

$$F'_{PhDA} = (vsm_{PhDA} / vsm_{PhDAq}) F_{PhDA} = \left\| \begin{matrix} 8 & 3 & 2,6 \\ 1 & 4,5 & 2,6 \\ 0 & 1,5 & 3,9 \end{matrix} \right\|.$$

Далі, з урахуванням (2.45) в [1] сформуємо підмножину нечітких термів $\mathbf{T_{PhNC}}$, $\mathbf{T_{PhDA}}$, що відображають певні стани параметрів P_{PhNC} та P_{PhDA} в *2*-вимірному параметричному субдовкіллі ($\mathbf{P_i} = \mathbf{P_{Ph}}$), а також при $n=1$ (для кібератак з ІД $CA_1 = CA_{Ph} = Ph$), $m_1 = 2,\ r_1 = 5,\ r_2 = 3$:

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

$$\{\{\underset{\sim}{T}_{PhNC1}, \underset{\sim}{T}_{PhNC2}, \underset{\sim}{T}_{PhNC3}, \underset{\sim}{T}_{PhNC4}, \underset{\sim}{T}_{PhNC5}\},$$

$$\{\underset{\sim}{T}_{PhDA1}, \underset{\sim}{T}_{PhDA2}, \underset{\sim}{T}_{PhDA3}\}\} =$$

$$\{\{\underset{\sim}{ДМ}_{PhNC}, \underset{\sim}{М}_{PhNC}, \underset{\sim}{С}_{PhNC}, \underset{\sim}{В}_{PhNC}, \underset{\sim}{ДВ}_{PhNC}\},$$

$$\{\underset{\sim}{МЛ}_{PhDA}, \underset{\sim}{СР}_{PhDA}, \underset{\sim}{СТ}_{PhDA}\}\},$$

де:

- $\underset{\sim}{T}_{PhNC1} = \underset{\sim}{ДМ}_{PhNC}$, $\underset{\sim}{T}_{PhNC2} = \underset{\sim}{М}_{PhNC}$, $\underset{\sim}{T}_{PhNC3} = \underset{\sim}{С}_{PhNC}$, $\underset{\sim}{T}_{PhNC4} = \underset{\sim}{В}_{PhNC}$ та $\underset{\sim}{T}_{PhNC5} = \underset{\sim}{ДВ}_{PhNC}$ відповідно є НЧ $\underset{\sim}{ДМ}_{PhNC}$, $\underset{\sim}{М}_{PhNC}$, $\underset{\sim}{С}_{PhNC}$, $\underset{\sim}{В}_{PhNC}$, $\underset{\sim}{ДВ}_{PhNC}$, які інтерпретують висловлювання експерта, що відображаються за допомогою LE_{PhNC1}="ДМ", LE_{PhNC2} = "М", LE_{PhNC3} = "С", LE_{PhNC4} = "В" та LE_{PhNC5} = "ДВ";

- $\underset{\sim}{T}_{PhDA1} = \underset{\sim}{МЛ}_{PhDA}$, $\underset{\sim}{T}_{PhDA2} = \underset{\sim}{СР}_{PhDA}$ і $\underset{\sim}{T}_{PhDA3} = \underset{\sim}{СТ}_{PhDA}$ відповідно є НЧ $\underset{\sim}{МЛ}_{PhDA}$, $\underset{\sim}{СР}_{PhDA}$, $\underset{\sim}{СТ}_{PhDA}$, що інтерпретують висловлювання експерта, які відображаються за допомогою LE_{PhDA1} = "МЛ", LE_{PhDA2} = "СР" і LE_{PhDA3} = "СТ".

З урахуванням (2.46) в [1] за відповідними рядками F'_{PhNC} та F'_{PhDA} побудуємо вектори максимумів:

$$FM_{PhNC} = \| fm_{PhNCs} \| =$$

$$\| fm_{PhNC1}, fm_{PhNC2}, fm_{PhNC3}, fm_{PhNC4}, fm_{PhNC5} \| =$$

$$\|7{,}9;\ 5{,}5;\ 5{,}5;\ 5;\ 7{,}3\|,$$

$$FM_{PhDA} = \| fm_{PhDAs} \| = \| fm_{PhDA1}, fm_{PhDA2}, fm_{PhDA3} \| =$$

$$\|8;\ 4{,}5;\ 3{,}9\|.$$

На основі FM_{PhNC} та FM_{PhDA} за виразом (2.47) в [1] сформуємо матриці функцій належності:

$$M_{PhNC} = \|\mu_{PhNCsq}\| = \begin{Vmatrix} 1 & 0{,}5 & 0 & 0 & 0 \\ 0{,}4 & 1 & 0{,}3 & 0 & 0 \\ 0 & 0{,}5 & 1 & 0{,}6 & 0 \\ 0 & 0 & 0{,}7 & 1 & 0{,}5 \\ 0 & 0 & 0 & 0{,}6 & 1 \end{Vmatrix},$$

$$M_{PhDA} = \|\mu_{PhDAsq}\| = \begin{Vmatrix} 1 & 0{,}7 & 0{,}7 \\ 0{,}1 & 1 & 0{,}7 \\ 0 & 0{,}3 & 1 \end{Vmatrix},$$

де:

- $\mu_{PhNCsq} = f'_{PhNCsq} / fm_{PhNCs}$, $(s,q = \overline{1,5})$,
- $\mu_{PhDAsq} = f'_{PhDAsq} / fm_{PhDAs}$, $(s,q = \overline{1,3})$.

На основі отриманих даних μ_{PhNCsq}, μ_{PhDAsq} та обчислених за виразом (2.49) в [1] x_{PhNCsq}, x_{PhDAsq} визначимо низки нечітких термів відповідно до (2.48) в [1]:

$$\underset{\sim}{T}_{PhNCs} = \{\mu_{PhNCs1} / x_{PhNCs1},\ \mu_{PhNCs2} / x_{PhNCs2},$$

$$\mu_{PhNCs3} / x_{PhNCs3},\ \mu_{PhNCs4} / x_{PhNCs4},\ \mu_{PhNCs5} / x_{PhNCs5}\},$$

$$(s,q = \overline{1,5}),$$

де, з урахуванням (2.49) в [1]:

$$X_{PhNCsq} = N^{max}_{PhNCq} / N^{max}_{PhNCr},\ (q = \overline{1,5})$$ або

$$\{\bigcup_{q=1}^{5} X_{PhNCsq}\} = \{0{,}2;0{,}4;0{,}6;0{,}8;1\}.$$

Далі, аналогічно, визначимо:

$$\underset{\sim}{T}_{PhDAs} =$$

$$\{\mu_{PhDAs1} / x_{PhDAs1},\ \mu_{PhDAs2} / x_{PhDAs2},\ \mu_{PhDAs3} / x_{PhDAs3}\},$$

$$(s,q = \overline{1,3}),$$

де $X_{PhDAsq} = N^{max}_{PhDAq} / N^{max}_{PhDAr}$, $(q = \overline{1,3})$ або $\{\bigcup_{q=1}^{3} X_{PhDAsq}\} =$ $\{0{,}3;0{,}7;1\}$.

Таким чином, отримані члени підмножини T_{PhNC}, T_{PhDA} (числова форма) відповідно є відображенням членів підмножини LE_{PhNC}, LE_{PhDA} (лінгвістична форма) та представляються у наступному вигляді:

$$-\underset{\sim}{T}_{PhNC1} = \underset{\sim}{ДМ}_{PhNC} = \{1 / 0{,}2; 0{,}5 / 0{,}4; 0 / 0{,}6; 0 / 0{,}8; 0 / 1\};$$

$$-\underset{\sim}{T}_{PhNC2} = \underset{\sim}{М}_{PhNC} = \{0{,}4 / 0{,}2; 1 / 0{,}4; 0{,}3 / 0{,}6; 0 / 0{,}8; 0 / 1\};$$

$$-\underset{\sim}{T}_{PhNC3} = \underset{\sim}{С}_{PhNC} = \{0 / 0{,}2; 0{,}5 / 0{,}4; 1 / 0{,}6; 0{,}6 / 0{,}8; 0 / 1\};$$

$-\underset{\sim}{T}_{PhNC4} = \underset{\sim}{B}_{PhNC} = \{0/0,2; 0/0,4; 0,7/0,6; 1/0,8; 0,5/1\};$

$-\underset{\sim}{T}_{PhNC5} = \underset{\sim}{ДВ}_{PhNC} = \{0/0,2; 0/0,4; 0/0,6; 0,6/0,8; 1/1\};$

$-\underset{\sim}{T}_{PhDA1} = \underset{\sim}{МЛ}_{PhDA} = \{1/0,3; 0,7/0,7; 0,7/1\};$

$-\underset{\sim}{T}_{PhDA2} = \underset{\sim}{СР}_{PhDA} = \{0,1/0,3; 1/0,7; 0,7/1\};$

$-\underset{\sim}{T}_{PhDA3} = \underset{\sim}{СТ}_{PhDA} = \{0/0,3; 0,3/0,7; 1/1\}.$

Далі, відповідно до етапу 5 виразу (2.52) в [1] сформуємо НЧ $\mathbf{T^e_{PhNC} \subseteq T^e}$, $\mathbf{T^e_{PhDA} \subseteq T^e}$ еталонного субдовкілля ($\mathbf{T^e_i = T^e_{Ph}}$):

$$T^e_{PhNC} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^e_{PhNCs}\} =$$

$$\{\underset{\sim}{T}^e_{PhNC1}, \underset{\sim}{T}^e_{PhNC2}, \underset{\sim}{T}^e_{PhNC3}, \underset{\sim}{T}^e_{PhNC4}, \underset{\sim}{T}^e_{PhNC5}\} =$$

$$\{\underset{\sim}{ДМ}^e_{PhsNC}, \underset{\sim}{М}^e_{PhsNC}, \underset{\sim}{С}^e_{PhsNC}, \underset{\sim}{В}^e_{PhsNC}, \underset{\sim}{ДВ}^e_{PhsNC}\},$$

$$(s = \overline{1,5}),$$

$$T^e_{PhDA} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{PhDAs}\} = \{\underset{\sim}{T}^e_{PhDA1}, \underset{\sim}{T}^e_{PhDA2}, \underset{\sim}{T}^e_{PhDA3}\} =$$

$$\{\underset{\sim}{МЛ}^e_{PhsDA}, \underset{\sim}{СР}^e_{PhsDA}, \underset{\sim}{СТ}^e_{PhsDA}\}, \ (s = \overline{1,3}),$$

де члени підмножини:

- $T^e_{PhNC} - \underset{\sim}{ДМ}^e_{PhNC}, \underset{\sim}{М}^e_{PhNC}, \underset{\sim}{С}^e_{PhNC}, \underset{\sim}{В}^e_{PhNC}, \underset{\sim}{ДВ}^e_{PhNC}$,
- $T^e_{PhDA} - \underset{\sim}{МЛ}^e_{PhDA}, \underset{\sim}{СР}^e_{PhDA}, \underset{\sim}{СТ}^e_{PhDA}$,

є НЧ, що складають основу еталонного субдовкілля ($\mathbf{T^e_i = T^e_{Ph}}$).

Далі, перетворимо нечіткі терми $\underset{\sim}{ДМ}_{PhNC}$, $\underset{\sim}{М}_{PhNC}$, $\underset{\sim}{С}_{PhNC}$, $\underset{\sim}{В}_{PhNC}$, $\underset{\sim}{ДВ}_{PhNC}$ та $\underset{\sim}{МЛ}_{PhDA}$, $\underset{\sim}{СР}_{PhDA}$, $\underset{\sim}{СТ}_{PhDA}$ таким чином, щоб для всіх $\underset{\sim}{T}_{PhNCs}$ та $\underset{\sim}{T}_{PhDAs}$ було справедливо відношення порядку, тобто:

- $\forall x_{PhNCsq} : x_{PhNCsq} < x_{PhNCsq+1}, \ (q = \overline{1,5})$,
- $\forall x_{PhDAsq} : x_{PhDAsq} < x_{PhDAsq+1} \ (q = \overline{1,3})$,

(відповідно до кроку 1, етапу 5 (див. п. 2.2)).

Якщо за компоненти таких термів використовувати конкретні значення, отримані у вище описаному прикладі, то для них таке відношення буде істинним. Так, наприклад, для $\underset{\sim}{ДМ}_{PhNC}$ це $x_{PhNC11} < x_{PhNC12} < x_{PhNC13} < x_{PhNC14} < x_{PhNC15} = 0,2 < 0,4 < 0,6 < 0,8 < 1.$

Також, аналогічно, буде істинним відношення для $\underset{\sim}{МЛ}_{PhDA}$, тобто $x_{PhDA11} < x_{PhDA12} < x_{PhDA13} = 0,3 < 0,7 < 1$.

Далі, відповідно до кроку 2 етапу 5 (див. п. 2.2) для кожного $\underset{\sim}{T}_{PhNCs}$ реалізуємо процедуру поглинання.

Для $\underset{\sim}{ДМ}_{PhNC}$ (де мода $x_{PhNC1M} = x_{PhNC11} = 0,2$, а її порядковий номер $M = 1$) при умові U_2 (тобто $\mu_{PhNC13} = \mu_{PhNC14} = \mu_{PhNC15} = 0$) здійснюється поглинання одним компонентом $0 / x^{max}_{PhNC1}$ низку інших відповідно до виразу $x^{max}_{PhNC1} = x_{PhNC13} \wedge x_{PhNC14} \wedge x_{PhNC15} = 0,6 \wedge 0,8 \wedge 1 = 0,6, (q = \overline{1,5})$.

Отже, $\mu_{PhNC13} / x_{PhNC13} = 0/0,6$, $\mu_{PhNC14} / x_{PhNC14} = 0/0,8$, $\mu_{PhNC15} / x_{PhNC15} = 0/1$ поглинаються компонентом $\mu_{PhNC13} / x_{PhNC13} = 0/0,6$.

Аналогічно, для $\underset{\sim}{М}_{PhNC}$ (де мода $x_{PhNC2M} = x_{PhNC21} = 0,4$, а її порядковий номер $M = 2$) при умові U_2 (тобто $\mu_{PhNC24} = \mu_{PhNC25} = 0$) здійснюється поглинання одним компонентом $0 / x^{max}_{PhNC2} = \mu_{PhNC24} / x_{PhNC24} = 0/0,8$ відповідно до виразу $x^{max}_{PhNC2} = x_{PhNC24} \wedge x_{PhNC25} = 0,8 \wedge 1 = 0,8$.

Таким чином, $\mu_{PhNC24} / x_{PhNC24} = 0/0,8$ та $\mu_{PhNC25} / x_{PhNC25} = 0/1$ поглинаються компонентом $\mu_{PhNC24} / x_{PhNC24} = 0/0,8$. Далі видно, що для НЧ $\underset{\sim}{С}_{PhNC}$ умови U_1 та U_2 не виконуються і тому операція поглинання не здійснюється. Для $\underset{\sim}{В}_{PhNC}$ (де мода $x_{PhNC4M} = x_{PhNC41} = 0,8$, а її порядковий номер $M = 4$) при умові U_1 (тобто $\mu_{PhNC41} = \mu_{PhNC42} = 0$) компонент $0 / x^{min}_{PhNC4} = \mu_{PhNC42} / x_{PhNC42} = 0/0,4$ відповідно до виразу $x^{min}_{PhNC4} = x_{PhNC41} \vee x_{PhNC42} = 0,2 \vee 0,4 = 0,4$, а отримане значення $\mu_{PhNC41} / x_{PhNC42} = 0/0,2$ та $\mu_{PhNC42} / x_{PhNC42} = 0/0,4$ поглинається компонентом $\mu_{PhNC41} / x_{PhNC42} = 0/0,4$.

Аналогічно, для $\underset{\sim}{ДВ}_{PhNC}$ ($x_{PhNC5M} = x_{PhNC55} = 1$, а її порядковий номер $M = 5$) при умові U_1 (тобто $\mu_{PhNC51} = \mu_{PhNC52} = \mu_{PhNC53} = 0$) здійснюється поглинання одним компонентом $0 / x^{min}_{PhNC5}$ низки інших

відповідно до виразу $x^{min}_{PhNC5} = x_{PhNC51} \vee x_{PhNC52} \vee x_{PhNC53} = 0,2 \vee 0,4 \vee 0,6 = 0,6.$ Отже, $\mu_{PhNC51} / x_{PhNC51} = 0 / 0,2$, $\mu_{PhNC52} / x_{PhNC52} = 0 / 0,4$, $\mu_{PhNC53} / x_{PhNC53} = 0 / 0,6$ поглинаються компонентом $\mu_{PhNC53} / x_{PhNC53} = 0 / 0,6.$

Далі, для кожного $\underset{\sim}{МЛ}_{PhDA}$, $\underset{\sim}{СР}_{PhDA}$, $\underset{\sim}{СТ}_{PhDA}$ умова U_1 та U_2 не виконуються і тому операція поглинання не здійснюється.

З урахуванням описаних перетворень, а також виразу (2.51) в [1], визначимо проміжні терми у вигляді: $\underset{\sim}{T}'_{PhNC1} = \underset{\sim}{ДМ}'_{PhNC} = \{1 / 0,2; 0,5 / 0,4; 0 / 0,6\};$ $\underset{\sim}{T}'_{PhNC2} = \underset{\sim}{М}'_{PhNC} = \{0,4 / 0,2; 1 / 0,4; 0,3 / 0,6; 0 / 0,8\};$ $\underset{\sim}{T}'_{PhNC3} = \underset{\sim}{С}'_{PhNC} = \{0 / 0,2; 0,5 / 0,4; 1 / 0,6; 0,6 / 0,8; 0 / 1\};$ $\underset{\sim}{T}'_{PhNC4} = \underset{\sim}{В}'_{PhNC} = \{0 / 0,4; 0,7 / 0,6; 1 / 0,8; 0,5 / 1\};$ $\underset{\sim}{T}'_{PhNC5} = \underset{\sim}{ДВ}'_{PhNC} = \{0 / 0,6; 0,6 / 0,8; 1 / 1\}$ та $\underset{\sim}{T}'_{PhDA1} = \underset{\sim}{МЛ}'_{PhDA} = \{1 / 0,3; 0,7 / 0,7; 0,7 / 1\};$ $\underset{\sim}{T}'_{PhDA2} = \underset{\sim}{СР}'_{PhDA} = \{0,1 / 0,3; 1 / 0,7; 0,7 / 1\};$ $\underset{\sim}{T}'_{PhDA3} = \underset{\sim}{СТ}'_{PhDA} = \{0 / 0,3; 0,3 / 0,7; 1 / 1\}.$

Відповідно до кроку 3 етапу 5 (див. п. 2.2), при реалізації другого кроку у формулі (2.51) в [1] для низки проміжних термів $\underset{\sim}{ДМ}'_{PhNC}$ та $\underset{\sim}{М}'_{PhNC}$ $\exists \underset{\sim}{T}'_{PhNC1} : \{0 / x^{min}_{PhNC1}\} \in \varnothing$ та $\exists \underset{\sim}{T}'_{PhNC2} : \{0 / x^{min}_{PhNC2}\} \in \varnothing$ (тобто $\mu_{PhNC11} = 1 \neq 0$ і $\mu_{PhNC21} = 0,2 \neq 0$), а для $\underset{\sim}{В}'_{PhNC}$ та $\underset{\sim}{ДВ}'_{PhNC}$ $\exists \underset{\sim}{T}'_{PhNC4} : \{0 / x^{max}_{PhNC4}\} \in \varnothing$ та $\exists \underset{\sim}{T}'_{PhNC5} : \{0 / x^{max}_{PhNC5}\} \in \varnothing$ (тобто $\mu_{PhNC45} = 0,5 \neq 0$ і $\mu_{PhNC55} = 1 \neq 0$), то формування підмножин $\underset{\sim}{T}^{e}_{PhNC1}$, $\underset{\sim}{T}^{e}_{PhNC2}$ та $\underset{\sim}{T}^{e}_{PhNC4}$, $\underset{\sim}{T}^{e}_{PhNC5}$ здійснимо за рахунок розширення $\underset{\sim}{T}'_{PhNC1}$, $\underset{\sim}{T}'_{PhNC2}$ та $\underset{\sim}{T}'_{PhNC4}$, $\underset{\sim}{T}'_{PhNC5}$ (див. (2.51) в [1]) шляхом введення додаткових $\mu_{PhNC1\beta-1} / x_{PhNC1\beta-1} = 0 / 0,2$, $\mu_{PhNC2\beta-1} / x_{PhNC2\beta-1} = 0 / 0,2$ та $\mu_{PhNC4r_j-\gamma+2} / x_{PhNC4r_j-\gamma+2} = 0 / 1$, $\mu_{PhNC5r_j-\gamma+2} / x_{PhNC5r_j-\gamma+2} = 0 / 1$ і відповідно, після чого в НЧ здійснюється переіндексація компонент починаючи з першої.

З урахування цього, набір проміжних термів для $\underset{\sim}{ДМ}'_{PhNC}$ буде мати наступний вигляд $\underset{\sim}{T}'_{PhNC1} = \underset{\sim}{ДМ}'_{PhNC} = \{\mu_{PhNC11} / x_{PhNC11}, \mu_{PhNC12} / x_{PhNC12}, \mu_{PhNC13} / x_{PhNC13}, \mu_{PhNC14} / x_{PhNC14}\} = \{0 / 0,2; 1 / 0,2; 0,5 / 0,4; 0 / 0,6\}$, де $\mu_{PhNC1\beta-1} = 0.$

Аналогічним чином, отримуємо проміжні терми для $\underset{\sim}{М}'_{PhNC}$, $\underset{\sim}{В}'_{PhNC}$ та $\underset{\sim}{ДВ}'_{PhNC}$, де $\mu_{PhNC2\beta-1} = \mu_{PhNC4r_j-\gamma+2} = \mu_{PhNC5r_j-\gamma+2} = 0.$ Таким чином, компоненти підмножини еталонів $\underset{\sim}{T}^{e}_{PhNC1}$ відповідно до (2.52) в [1] будуть визначатися як $\mu^{e}_{PhNC11} / x^{e}_{PhNC11} = 0 / 0,2$, $\mu^{e}_{PhNC12} / x^{e}_{PhNC12} = 1 / 0,2$, $\mu^{e}_{PhNC13} / x^{e}_{PhNC13} = 0,5 / 0,4$, $\mu^{e}_{PhNC14} / x^{e}_{PhNC14} = 0 / 0,6$ та, аналогічним чином, для $\underset{\sim}{T}^{e}_{PhNC2}$, $\underset{\sim}{T}^{e}_{PhNC4}$, $\underset{\sim}{T}^{e}_{PhNC5}$.

Далі, відповідно до (2.52) в [1], для $\underset{\sim}{ДМ}'_{PhNC}$, $\underset{\sim}{М}'_{PhNC}$, $\underset{\sim}{В}'_{PhNC}$, $\underset{\sim}{ДВ}'_{PhNC}$ сформуємо еталонні значення, тобто: $\underset{\sim}{T}^{e}_{PhNC1} = \underset{\sim}{ДМ}^{e}_{PhNC} = \{0 / 0,2; 1 / 0,2; 0,5 / 0,4; 0 / 0,6\};$ $\underset{\sim}{T}^{e}_{PhNC2} = \underset{\sim}{М}^{e}_{PhNC} = \{0 / 0,2; 0,4 / 0,2; 1 / 0,4; 0,3 / 0,6; 0 / 0,8\};$ $\underset{\sim}{T}^{e}_{PhNC3} = \underset{\sim}{С}^{e}_{PhNC} = \{0 / 0,2; 0,5 / 0,4; 1 / 0,6; 0,6 / 0,8; 0 / 1\};$ $\underset{\sim}{T}^{e}_{PhNC4} = \underset{\sim}{В}^{e}_{PhNC} = \{0 / 0,4; 0,7 / 0,6; 1 / 0,8; 0,5 / 1; 0 / 1\};$ $\underset{\sim}{T}^{e}_{PhNC5} = \underset{\sim}{ДВ}^{e}_{PhNC} = \{0 / 0,6; 0,6 / 0,8; 1 / 1; 0 / 1\}.$

Також, за аналогією формуються і наступні еталонні значення:

$-\underset{\sim}{T}^{e}_{PhDA1} = \underset{\sim}{МЛ}^{e}_{PhDA} = \{0 / 0,3; 1 / 0,3; 0,7 / 0,7; 0,7 / 1; 0 / 1\};$

$-\underset{\sim}{T}^{e}_{PhDA2} = \underset{\sim}{СР}^{e}_{PhDA} = \{0 / 0,3; 0,1 / 0,3; 1 / 0,7; 0,7 / 1; 0 / 1\};$

$-\underset{\sim}{T}^{e}_{PhDA3} = \underset{\sim}{СТ}^{e}_{PhDA} = \{0 / 0,3; 0,3 / 0,7; 1 / 1; 0 / 1\}.$

Далі, з урахуванням етапу 6 (див. п. 2.2 в [1]) для підмножини еталонів $\mathbf{T^{e}_{PhNC}}$ і $\mathbf{T^{e}_{PhDA}}$ з використанням отриманих конкретних значень можна здійснити їх графічну інтерпретацію, скориставшись необхідними НЧ еталонного субдовкілля ($\mathbf{T^{e}_{i} = T^{e}_{Ph}}$), будуються п'ять (див. рис. 1) та три (див. рис. 2) ламані відповідно.

ВИСНОВКИ

Запропонований в роботі МФЕФ, який за рахунок сформованого набору параметрів NC, DA та експертного оцінювання стану субдовкілля

інформаційної системи дозволить формалізувати процес формування параметрів еталонного субдовкілля для вирішення задач щодо виявлення фішингових URL-адрес в ІС.

Запропонований метод може бути використаний для підвищення ефективності засобів захисту інформації, що спрямовані на протидію фішингу в ІС.

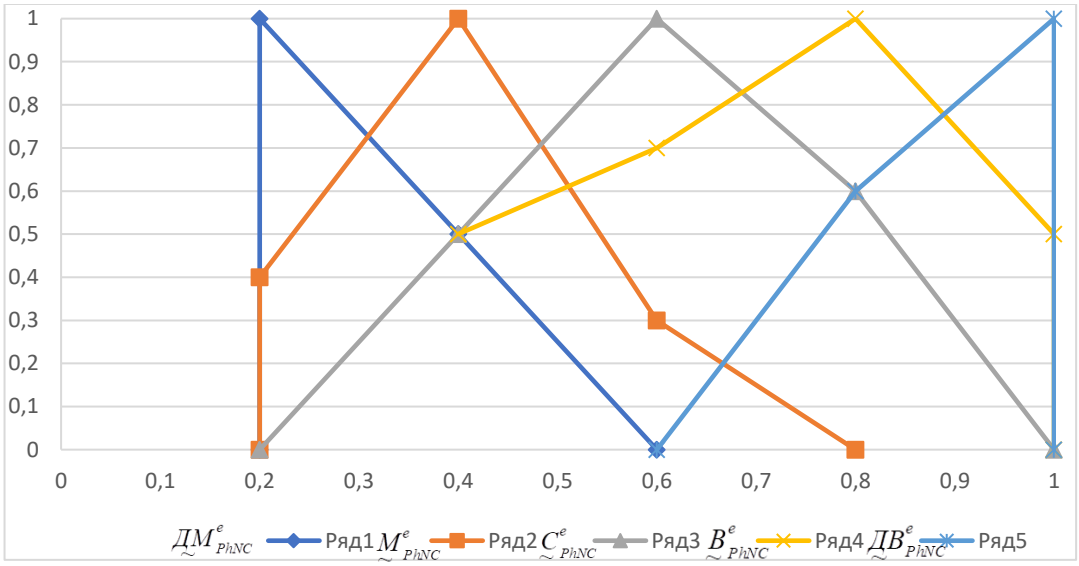

Рис. 1. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{PhNC}$

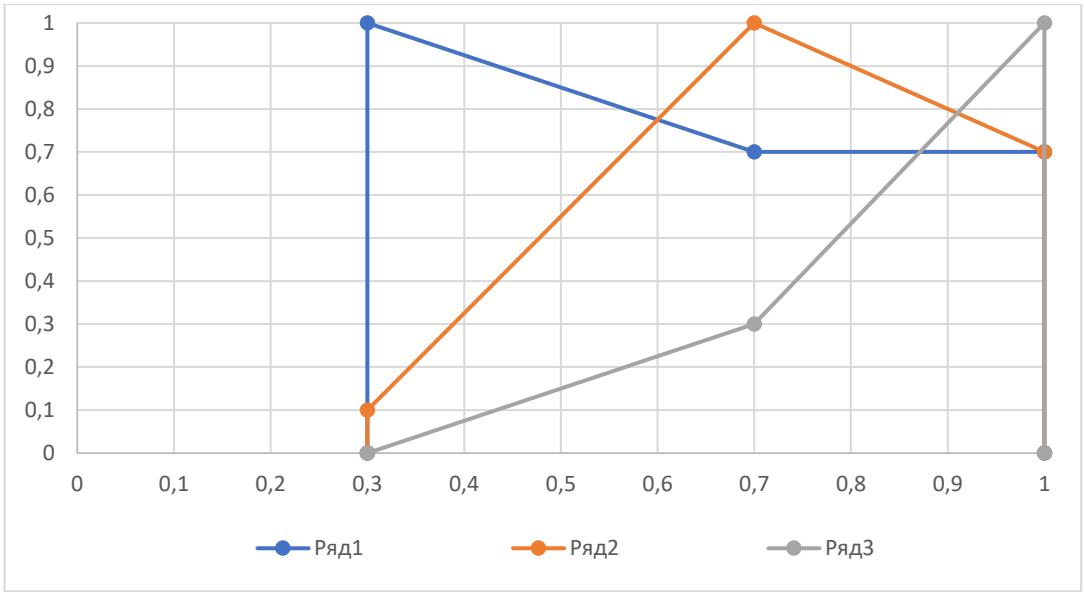

Рис. 2. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{PhDA}$

Запропонований в роботі МФЕФ, який за рахунок сформованого набору параметрів NC, DA та експертного оцінювання стану субдовкілля інформаційної системи дозволить формалізувати процес формування параметрів еталонного субдовкілля для вирішення задач щодо виявлення фішингових URL-адрес в ІС. Запропонований метод може бути використаний для підвищення ефективності засобів захисту інформації, що спрямовані на протидію фішингу в ІС.

В подальшому, для застосування МФЕФ необхідно розробити метод, що дає змогу формалізувати процес перетворення поточних значень нечітких параметрів, утворюючих mi-вимірне пара-

метричне субдовкілля, з метою його подальшого застосування для виявлення аномального стану, який викликаний фішинг-атаками.

ЛІТЕРАТУРА

[1] Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019. 361 с.

[2] Корченко О.Г. Побудова систем захисту інформації на нечітких множинах: теорія та практичні рішення / О.Г. Корченко. К.: МК-Прес, 2006. 320 с.

[3] Akhemetov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym / 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.

[4] Nazym Zhumangaliyeva, Anna Korchenko, Aliya Doszhanova, Aigul Shaikhanova, Shangytbayeva Gulmira Avkurova Zhadyra / Detection environment formation method for anomaly detection systems // Journal of Theoretical and Applied Information Technology, 2019. Vol.97. №.16. pp. 4239-4250.

[5] A. Korchenko, V. Breslavskyi, S. Yevseiev, N Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk / Development of a method for constructing linguistic standards for multi-criterial assessment of honeypot efficiency // Eastern-European Journal of Enterprise Technologies, 2021. Vol.109. №.1/2. pp. 14-23.

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

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

[8] M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conference on, 2017. pp. 258-264.

[9] І. Терейковський, А. Корченко, П. Вікулов, І. Ірейфідж, «Моделі еталонів лінгвістичних змінних для систем виявлення email спуфінг-атак», Безпека інформації. Т.24, №2, С. 99-109, 2018.

[10] Zawoad, S., Hasan, R., & Hasan, M.A. The evolution of phishing attacks: patterns, trends, and future directions. ACM Computing Surveys (CSUR), 2019. Vol. 52(6), pp. 1-40.

[11] Anna Korchenko, «Formation of linguistic standards for of intrusion detection systems», Безопасность в авиации и космические технологии: VIII Всемирный конгресс «Авиация в XXI столетии», Киев, 2018. С. 3.2.1.-3.2.6.

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

[13] A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on, 2015. pp. 478-483.

[14] А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф., Київ, 2015. С. 274-275.

METHOD OF FORMING A REFERENCE SUBENVIRONMENT FOR DETECTING PHISHING URLS

Increasing and improving the effectiveness of cyber-attacks to detect disease detection systems annually, and the use of modern intrusion detection systems allows you to quickly respond to new types of cyber-attacks and detect cases of infection with protective equipment. Such systems are quite advanced, but their significant operation requires real-time information, which can be used to determine the suspicious activity of an unauthorized party. Such information can be determined using expert approaches. Expert methods can help detect new cyber-attacks. The use of methods, models and systems based on the theory of fuzzy sets in the construction of anomaly detection tools generated by the implementation of new cyber threats is likely to have a trial and detection of an intrusion detection system. The development of computational solutions, calculations in fuzzy conditions, are likely to be identified by previously improbable and modified types of cyber-attacks. There are also enough developments that are used to solve cyber-attack detection problems, for example, a number of methods for creating a reference subenvironment for an intrusion detection system, but they are not focused on phishing approaches. However, as practice shows, when new symptoms and anomalies appear, generated by attacking actions with unspecified or unclearly targeted actions, in relation to media that do not always require effective work, therefore, methods that allow obtaining results in the process of a new reference subsystem for an intrusion detection system

are relevant tasks. Phishing is one of the standard means aimed at collecting confidential information, such as logins, passwords, financial details and other personal data. For this developed model of the formation of a reference subenvironment for determining phishing URLs due to the generated set: the number of country parameters by IP address, the age of the domain and expert assessment of the state of the subenvironment of the disclosed system, the formalization of the process of generating the parameters of the reference subenvironment for solving the problems of determining phishing URLs is determined.

Keywords: attacks, cyberattacks, anomalies, intrusion detection systems, anomaly detection systems, intrusion detection systems, cyberattack detection systems, anomaly detection in computer networks.

Корченко Анна Олександрівна, доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Anna Korchenko, doctor of technical sciences, professor, professor of the department of information security and telecommunications, National Technical University Dnipro Polytechnic, Professor of the Department of Information Technology Security, National Aviation University.
E-mail: annakor@ukr.net.
Orcid ID: 0000-0003-0016-1966.

Іванченко Євгенія Вікторівна, кандидат технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Yevheniya Ivanchenko, Candidate of Technical Sciences, Professor, Professor of the Department of Information Technology Security, National Aviation University.
E-mail: evivancenko@gmail.com.
Orcid ID: 0000-0003-3017-5752.

Сатибалдієва Феруза Аубакирівна, магістр, завідувач кафедри комп'ютерних технологій Казахської національної академії мистецтв імені Темірбека Жургенова (Алмати, Казахстан).

Feruza Satybaldiyeva, Master, Head of the Department of Computer Technology of the Kazakh National Academy of Arts named after Temirbek Zhurgenov (Almaty, Kazakhstan).
E-mail: feruza201200@gmail.com.
Orcid ID: 0000-0003-4107-7568.

Жумангалієва Назим Кенжегаліївна, магістр, старший викладач кафедри комп'ютерних технологій Казахської національної академії мистецтв імені Темірбека Жургенова (Алмати, Казахстан).

Nazym Zhumangaliyeva, Master, Senior Lecturer of the Department of Computer Technology, Temirbek Zhurgenov Kazakh National Academy of Arts (Almaty, Kazakhstan).
E-mail: nazym_k.81@mail.ru.
Orcid ID: 0000-0003-1130-3405.