services are Google AppEngine, VMWare Pivotal Cloud Foundry, Red Hat's OpenShift, Heroku and more.

Finally, the closest type of service to system administrators is IaaS. Infrastructure as a service in its facilities and characteristics is closest to owning your own «hardware» and virtualization. In the case of IaaS, you get cloud processors, memory, disks, and networks, from which you later create virtual routers and configure the network topology as you need.

The logic of choosing the right type of cloud service is to find a balance between setup speed and system flexibility. It is unlikely to sharpen SaaS exactly for your business processes, but it is also almost impossible to build a ready-made solution based on IaaS in a couple of hours. It is also worth noting the need to build multi-vendor solutions, which in the case of SaaS and PaaS can be very difficult.

And it’s necessary to mention one more of the cloud models, without which the review would not be complete, namely VPS and Dedicated servers. Formally, this service also falls into the IaaS class, but has significant differences. The essence of the service consists in the provision by the customer of virtual or dedicated physical servers for rent at very low prices.

Література:

1 Виды облаков и облачных услуг [Електронний ресурс] – Режим доступу до ресурсу: https://www.datafort.ru/blog/the-types-of-clouds.html.

2 Виды облачных сервисов: IaaS, PaaS, SaaS и другие модели [Електронний ресурс] – Режим доступу до ресурсу: https://oblako.kz/iaas-blog/samye-populjarnye-oblachnye-servisy-v-mire.

Думчиков С.А., *студент 6 курсу, факультет інформаційних технологій та комп’ютерної інженерії, кафедра захисту інформації, Вінницький національний технічний університет, м. Вінниця;*

Лукічов В.В., *к.т.н., старший викладач, факультет інформаційних технологій та комп’ютерної інженерії, кафедра захисту інформації, Вінницький національний технічний університет, м. Вінниця*

ВИЯВЛЕННЯ ФІШИНГОВИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Фішинг – це популярна форма атаки соціальної інженерії, при якій зловмисник обманює жертву, видаючи себе за іншу особу або ресурс. Електронні листи і повідомлення зі шкідливими вкладеннями або скомпрометованими URL-адресами, що перенаправляють на шкідливі веб-сайти, є одними з найпоширеніших векторів атак, які використовуються при фішингу. Технологічний прогрес надав фішерам більш досконалі інструменти для запуску небезпечних і витончених атак. У звіті Phishlabs про тенденції в області фішингу за 2018 рік [1] згадується, що цілі фішингових атак перемістилися з приватних осіб на підприємства. Що ще гірше, у фішерів тепер є доступ до безкоштовних SSL-сертифікатів. Майже половина всіх фішингових

веб-сайтів в даний час використовує протокол HTTPS, який був одним з основних індикаторів легітимності веб-сайтів [2]. В іншому звіті, опублікованому APWG в першому кварталі 2019 року, говориться, що кількість фішингових атак збільшилася на 30% в порівнянні з попереднім кварталом і що основними цілями були служби «Програмне забезпечення як послуга» і веб-пошта [3].

За останнє десятиліття дослідники ідентифікували і класифікували особливості, що проявляються з векторів фішингових атак різними способами. В деяких статтях ознаки класифікуються з точки зору типу атаки, деякі класифікуються на основі того, як і де вони з'являються у векторі атаки [4], [5]. Однак, наскільки відомо, ніхто не дав систематичної класифікації, яка незалежна від підходів до виявлення і охоплює всі можливі особливості, які можуть бути добуті з векторів атак. Вектори фішингу, наприклад веб-сайти, URL-адреси, представляють собою спеціалізовані стрічки. Тому, такі категорії мови чи логіки як синтаксис, семантика і прагматика можуть бути ефективно використані для класифікації їх атрибутів. Побудова класифікації потребує детального огляду інформаційних джерел, розуміння потенційних проблем та можливостей, а також систематичного і детального підходу. Класифікація, що представлена на рисунку 1, має основні компоненти веб-сторінки в якості других рівнів. Кожний компонент далі розбивається на такі групи: синтаксис, семантика і прагматика.

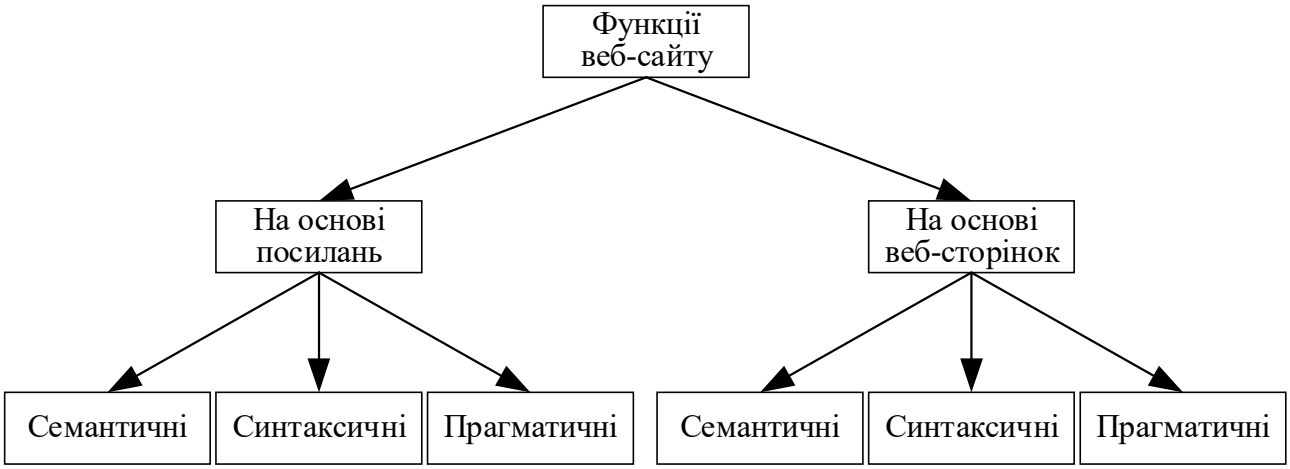

Рисунок 1 – Вигляд класифікації сайтів на основі посилань та веб-сторінок

Синтаксичні функції вектору залежать від формату і синтаксичної коректності вектору URL-адреси чи веб-сайту. Наприклад, у правильно побудованій URL-адресі домен верхнього рівня (.com, .net, .ua) з'являється лише один раз. Однак це не завжди так у випадку шкідливої URL-адреси. Ця проблема зв'язана з синтаксисом URL-адрес, тому розглядаємо позицію домену верхнього рівня як синтаксичну особливість. Досліджуючи вміст веб-сайту,

можемо підрахувати усі теги, що являється ще одною синтаксичною особливістю.

Семантичні функції зосереджені на значенні та інтерпритації текстового вмісту в URL-адресах та веб-сайтах. Прикладом семантичної функції для веб-сайту може бути значення елементів HTML, наприклад кількість прихованих об’єктів.

Прагматичні функції не мають прямого відношення до синтаксису чи семантиці URL-адреси чи веб-сайту. Наприклад, відключення натискання правої кнопки миші на веб-сайтах – це метод, що використовується зловмисниками для попередження перегляду і збереження вихідного коду користувачами. Це не має відношення ні до синтаксису вмісту HTML, ні до його семантики. Таким чином, це відноситься до категорії прагматичних функцій. Іншими прикладами прагматичних функцій є відомості про реєстрацію веб-сайту, термін дії веб-сайту і т.д.

Представлено класифікацію сайтів для виявлення фішингового вмісту. На відміну від поділу фішингового ресурсу за вектором та типом фішингової атаки, дана класифікація охоплює особливості, які можуть бути добуті з вектору атаки. Майбутня робота включає пошук способів визначення будь-якого типу фішингових сайтів якнайшвидше.

Література:

1. The 2018 Phishing Trends & Intelligence Report. URL: https://info.phishlabs.com/2018_phishing_trends_and_-intelligence_report-0.
2. Patrick Nohe. HTTPS Phishing: 49% of Phishing Websites Now Sport The Green Padlock. URL: https://www.thesslstore.com/blog/https-phishing-green-padlock/.
3. A.-P. W. Group. Phishing Activity Trends Report-1st Quarter 2019. URL: https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf.
4. M. Vijayalakshmi, S. Mercy Shaline, Ming Hour Yang, Raja Meenakshi U. Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions. URL: https://doi.org/10.1049/iet-net.2020.0078.
5. J. Mao, W. Tian, P. Li, T. Wei and Z. Liang. «Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity» in IEEE Access, vol. 5, pp. 17020-17030, 2017, doi: 10.1109/ACCESS.2017.2743528. URL: https://ieeexplore.ieee.org/abstract/document/8015116.