У ракетних військах стратегічного призначення інформаційно-психологічне протиборство здійснюють командири, штаби, служби та органи виховної роботи. Особлива роль в цьому належить службі захисту державної таємниці ракетних військ стратегічного призначення, органам військової контррозвідки і обчислювальним відділам. Органи виховної роботи здійснюють інформаційно-виховну та психологічну роботу, беруть участь спільно з медичною службою в захисті особового складу від інформаційно-психологічного впливу противника і психологічної реабілітації військовослужбовців.

Як видно з аналізу функцій, цілей і завдань, інформаційно-психологічне протиборство по своїй суті всеохоплююче. Воно ведеться в мирний і воєнний час, на всіх рівнях і напрямках. Інформація в ньому виступає в якості зброї, ресурсу та цілі, а психологічний компонент як свого роду спосіб або засіб доставки цієї інформації. Ефективність і результативність інформаційно-психологічного протиборства залежить в кінцевому рахунку від обох цих складових. Тому в сучасних умовах надзвичайно важливо, щоб країна не залишилася осторонь від сучасних інформаційних технологій і в той же час зберегла свою унікальну самобутність, свої традиції, свій світогляд, своє емоційно-психологічну своєрідність.

Список використаних джерел

1. Панарин И. СМИ, пропаганда и информационные войны [Електронний ресурс] / И. Панарин. – Режим доступа: https://propagandahistory.ru/books/Igor-Panarin_SMI--propaganda-i-informatsionnye-voyny/28

2. Оров А.М. Основні прийоми ведення інформаційних війн в політичній сфері [Електронний ресурс] / А.М.Оров. – Режим доступа: https://ukrbukva.net/page,5,78344-Osnovnye-priemy-vedeniya-informacionnyh-voiyn-v-politicheskoiy-sfere.html

3. Сафіна С.О. Інформаційні війни сучасності [Електронний ресурс] / С.О. Сафіна. – Режим доступа: http://ukrefs.com.ua/page,2,98886-Informacionnye-voiyny-sovremennosti.html

---

УДК 004.455.1:004.056

АНАЛІЗ РОБОТИ АНТИФІШИНГОВОГО БРАУЗЕРА НА ОСНОВІ «RANDOM FOREST» І ПРАВИЛА «EXTRACTION FRAMEWORK»

Желіба Д. В., здобувач вищої освіти, гр. МКБп-201
Науковий керівник: **Ткач Ю. М.**, д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Фішинг - це техніка атаки у соціальній інженерії, яка найбільш широко використовується для отримання конфіденційної інформації користувача, наприклад облікових даних для входу, інформації про кредитні та дебетові картки тощо[3]. Для захисту веб-користувачів від цих атак розробляються різні методи боротьби з фішингом, але вони не можуть захистити користувача від цих атак різними способами. У цій роботі ми пропонуємо нову техніку для ідентифікації фішингових веб-сайтів без особливих зусиль зі сторони клієнта, пропонуючи нову архітектуру браузера. У цій системі ми використовуємо правило аналізу властивостей або функцій веб-сайту, використовуючи лише URL-адресу.

Виявлення та блокування фішингової атаки надзвичайно важливо для збереження безпеки та конфіденційності користувача Інтернету. Вчені запропонували різні підходи для вирішення цієї визначної проблеми. Існує кілька алгоритмів, розроблених для виявлення фішингових сайтів. Але ними може користуватися лише спеціаліст.

Головною метою цієї роботи є аналіз технології, яка може бути легко використана кожною особою для точного виявлення нелегальних веб-сайтів у режимі реального часу. Процес виявлення здійснюється на стороні клієнта. Новизна підходу EPDB - це нещодавно

розроблена архітектура браузера з новим модулем під назвою «Intelligent Engine», який відповідає за легке виявлення фішингових веб-сайтів у реальному часі. Використовується 30 різних функцій для аналізу URL-адреси, введеної користувачем. Цей аналіз використовується алгоритмом класифікації для визначення достовірності адреси. Модель класифікації створена базою даних, що складається з 11 055 незаконних URL-адрес. «Intelligent Engine» аналізує кожен веб-сайт, завантажений браузером. «Intelligent Engine» та «Rendering Engine» розроблені таким чином, щоб працювати паралельно, мінімізуючи час.

Зловмисники використовують фішинг-атаки для викрадення облікових даних користувача для отримання доступу до приватних даних користувача. Згідно з доповіддю Федерального бюро розслідувань (ФБР) [1], загальна кількість виявлених фішингових шахрайських операцій у 2017 році становить 25 344, що спричиняє загальну втрату близько 29 703 421 доларів.

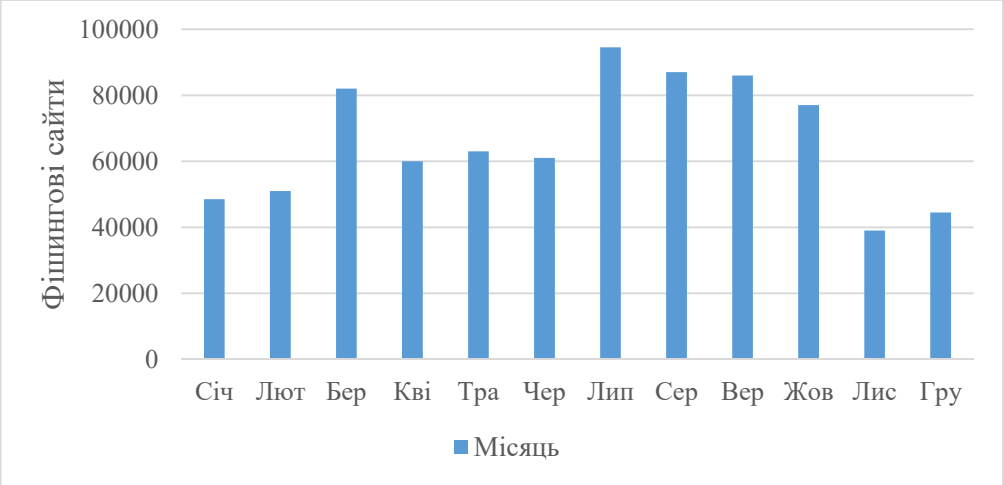

Рисунок 1 - Загальна кількість щомісячного фішингу сайтів у 2019 році

Беручи до уваги статистичні дані, ми зобразили загальну кількість щомісячного фішингу сайтів у 2019 році на рис.1. За даними APWG [2], найбільш «цікавими» для фішингу секторами у 2019 році є SAAS/Webmail-34%, Payment-23%, фінансові установи-18%, (рис. 2).

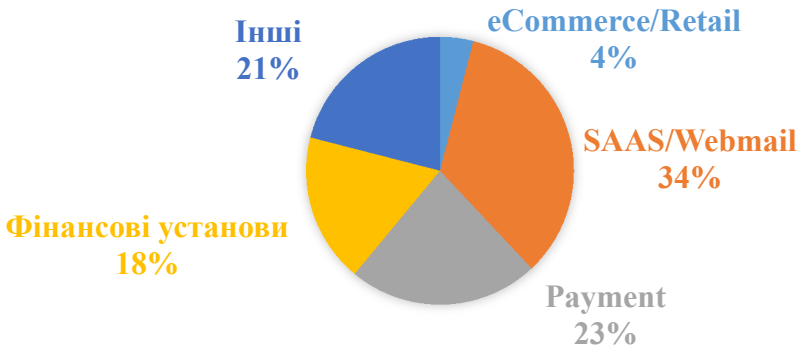

Рисунок 2 – розподіл секторів для фішингу

Запропонована системна архітектура EPDB показана на рис.3. Вона розроблена для виконання всіх операцій, необхідних браузеру, поряд із цим введено новий модуль під назвою «Intelligent Engine» для виконання операцій з виявлення фішингових веб-сайтів під час серфінгу Інтернет.

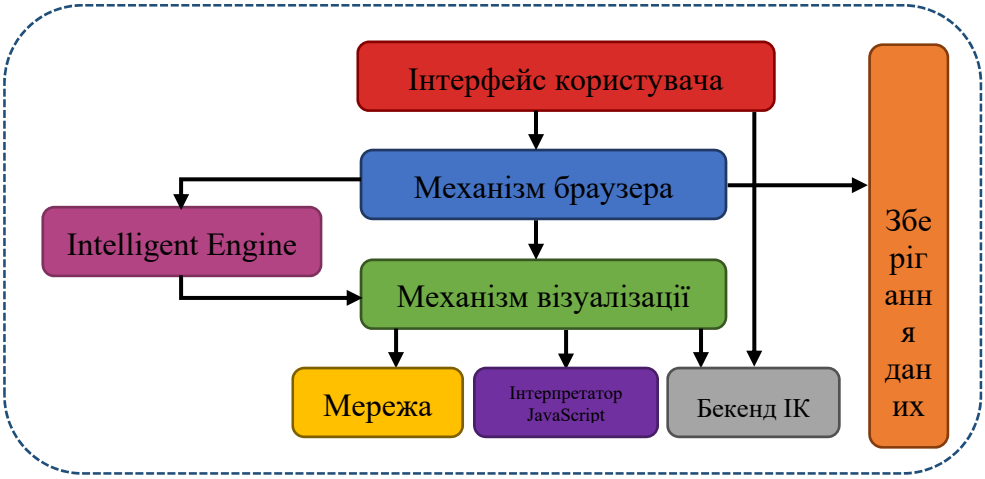

Рисунок 3 - Модель системи

Основними компонентами браузера є наступні:
• користувацький інтерфейс;
• механізм браузера;
• механізм візуалізації;
• мережа;
• інтерпретатор JavaScript;
• бекенд інтерфейсу користувача;
• зберігання даних;
• «Intelligent Engine».

Запропонована схема EPDB

Огляд набору даних

База складається з 11 055 записів [4,5], що містять як законні, так і незаконні веб-сайти. Точний підрахунок обох категорій, наявних у наборі даних, показаний на рис. 4. Кожен кортеж у наборі даних має 30 різних характеристик, які буде мати веб-сайт. Ці характеристики будуть розглядатися як незалежні змінні для навчання моделі. На основі цих особливостей визначається одна залежна змінна або цільова функція, яка визначає справжність веб-сайту. Набір даних обмежений 11 055 кортежами, щоб зменшити вплив переобладнання на продуктивність моделі.

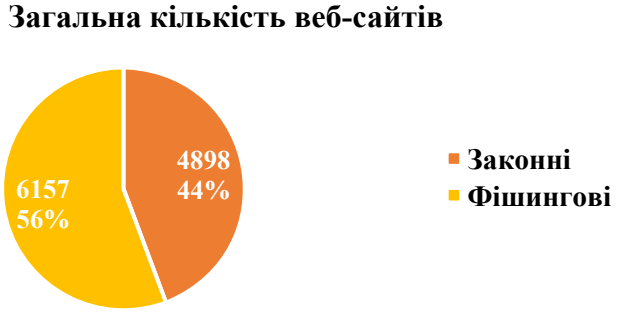

Рисунок 4 – Загальна кількість веб-сайтів

Правило визначення. Веб-сторінки мають найрізноманітніші властивості. Для переліку властивостей веб-сайту використовується правило Framework Extraction. Цей алгоритм сприймає URL-адресу як вхідну інформацію та аналізує 30 різних особливостей веб-сторінки, які потрібні для визначення її справжності. Ці результати перераховані та передані в модель класифікатора для подальшої обробки.

Модель «Random forest». «Random forest» грунтується на базі даних, що складається з 11 055 кортежів. Для створення більш ефективної моделі ми використали GridSearchCV для пошуку оптимальних параметрів для моделі. Модель працює за допомогою техніки перевірки K-кратності

Ефективність моделі аналізується за допомогою матриці, виробленої під час тестування та прогнозованих значень. Більш детальна інформація про матрицю на рис. 5 для кращого та легшого аналізу.

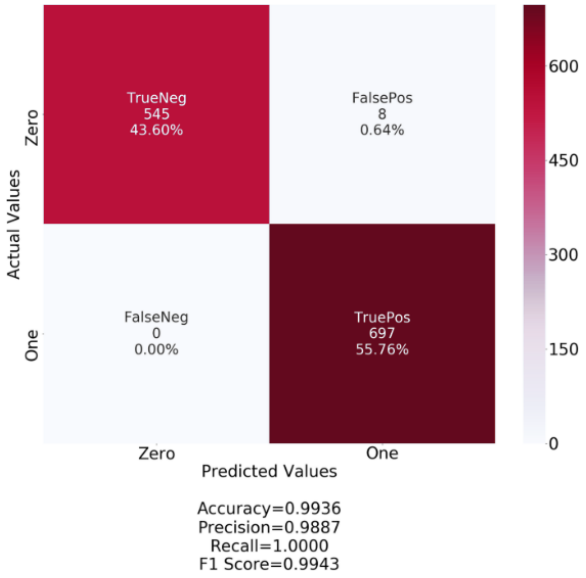

Рисунок 5 - Матриця, вироблена під час тестування та прогнозованих значень

Архітектура системи EPDB. Модель працює з набором даних за допомогою методу k-перехресної перевірки. Коли користувач вводить назву веб-сайту, URL-адреса паралельно надсилається до Intelligent Engine для перевірки. Цей механізм визначає усі 30 характеристик веб-сайту. Потім ці 30 функцій надсилаються до алгоритму «Random forest» для прогнозування. Приймається рішення щодо справжності отриманої URL-адреси та результат передається до механізму візуалізації. Механізм візуалізації спочатку отримає повідомлення від інтелектуального механізму, потім він отримує дані з браузерного механізму. Якщо отриманий результат є негативним, тоді механізм візуалізації відображатиме веб-сторінку. Якщо результат - фішинг, тоді механізм візуалізації заморозить візуалізацію веб-сторінки та з'явиться попереджувальне повідомлення про це. Користувача може продовжити, або повернутися назад. Такої функції немає у звичайних браузерах.

Основними перевагами запропонованої архітектури EPDB є:

• виявлення фішингового веб-сайту в режимі реального часу з точністю 99,36%;

• «Intelligent Engine» і «Browser Engine» працюють паралельно;

• веб-сайт зависає, якщо це фішинг;

•«Intelligent Engine» використовує значно менше пам'яті та часу на виконання опрецій;

У цій роботі ми провели аналіз технології роботи захищеного веб-браузера з використанням нових архітектур браузера. Він захищає користувача під час веб-серфінгу, забезпечуючи кращий захист від фішингових атак у режимі реального часу, забезпечує швидкий, надійний та безпечний перегляд користувачів та дозволяє їм отримати значні переваги безпеки.

Список використаних джерел

1. 2017 Internet Crime Report. https://pdf.ic3.gov/2017_IC3Report.pdf.
2. APWG trends report q4 2019. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf.

3. Armano G, Marchal S, Asokan N (2016) Real-time client-side phishing prevention add-on. In: 2016 IEEE 36th international conference on distributed computing systems (ICDCS), pp 777–778. https://doi.org/10.1109/icdcs.2016.44

4. Phishing scams and spoof emails at MillerSmiles.co.uk. http://www.millersmiles.co.uk/.

5. Join the fight against phishing. https://www.phishtank.com/.

6. Hawanna VR, Kulkarni VY, Rane RA (2016) A novel algorithm to detect phishing URLs. In: 2016 international conference on automatic control and dynamic optimization techniques (ICACDOT), pp 548–552. https://doi.org/10.1109/icacdot.2016.7877645

7. Hu J, Zhang X, Ji Y, Yan H, Ding L, Li J, Meng H (2016) Detecting phishing websites based on the study of the financial industry webserver logs. In: 2016 3rd international conference on information science and control engineering (ICISCE), pp 325–328. https://doi.org/10.1109/icisce.2016.79

8. Mei C, Leng C, Dayang H, Abang I, Nah S (2016) Feature-based phishing detection technique. J Theor Appl Inf Technol:101–106 Retrieved from https://ir.unimas.my/id/eprint/13943/

9. Phishing Trends & Intelligence Report 2018. https://info.phishlabs.com/hubfs/ 2018PTIReport/ PhishLabsTrendReport_2018-digital.pdf.

УДК 004.056.55

СХЕМА РОЗПОДІЛУ СЕКРЕТУ НА ОСНОВІ КИТАЙСЬКОЇ ТЕОРЕМИ ПРО ОСТАЧІ

Іллюшко Б. О., здобувач вищої освіти гр. КБ-181
Науковий керівник: **Синенко М. А.,** к.ф.м.-н., доцент
Національний університет «Чернігівська політехніка»

Схема розподілу секрету – криптографічний метод, суть якого полягає у розподіленому зберіганні секрентої інформації (наприклад, секретних ключів, паролів) з метою запобігання шахрайству. Секрет розподіляється серед учасників таким чином, що тільки їх коаліція в змозі його відновити. Ймовірність злочинної змови усіх учасників групи, що мають доступ до зберінання частин секрету вважається неймовірно малою. Серед поширених схем розподілу секрету слід відмітити схему Блеклі, яка була створена у 1979 році і базується на твердженні, що система k лінійних лінійно незалежних конгруенцій по простому модулю має один розв'язок, схему Шаміра, яка побудована на ідеї інтерполяції многочлена $(k-1)$-го степеня k точками.

У даній роботі буде розглянуто схему розподілу секрету, ідея побудови якої базується на китайській теоремі про остачі. Доведена близько 100 років до н.е. у наш час ця теорема широко застосовується у криптографії.

Сформулюємо китайську теорему про остачі.

Якщо $m_1, m_2, \dots, m_k$ попарно взаємно прості числа, $(m_i, m_j) = 1, i \neq j$, $a_1, a_2, \dots, a_k$ – довільні цілі числа, то система конгруенцій виду

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x \equiv a_k (mod\ m_k) \end{cases}$$

має єдиний розв'язок $x \equiv a (mod\ M)$, де

$M = m_1 m_2 \dots m_k,\ a = \sum_{i=1}^{k} a_i M_i \mu_i,\ M_i = \frac{M}{m_i},\ \ \mu_i = M_i^{-1} (mod\ m_i).$

Розглянемо схему розподілу секрету. Нехай N – секрет. Вибирають попарно різні прості числа $p_1, p_2, \dots, p_k$ і для кожного простого числа p_i знаходять $x_i \equiv N (mod\ m_i)$. Числа x_i –