В доповіді пропонується фільтр генератор псевдовипадкових послідовностей на основі хеш функцій з гарантованою довжиною періоду. Структурна схема запропонованого ГПВП представлена на рисунку 2.

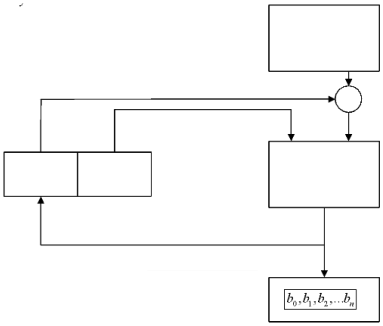

Рис.2. Структурна схема запропонованого фільтр ГПВП на основі хеш функції HMAC

В якості функції *f* можливо використання операцій *xor* або *mod* 2^n. Використання регістра зсуву з лінійним зворотнім (РЗЗЗЗ) зв'язком дає можливість формувати псевдовипадкові послідовності гарантованого періоду, а завдяки хеш-функції (наприклад, SHA-256) запропонований ГПВП забезпечує високу непередбачуваність та легко реалізовується на програмному та апаратному рівні.

1. NIST SP 800-90A Rev.1. URL: https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

Теоретико-множинний підхід до класифікації сучасних методів соціотехнічних атак

УДК 004.056.53(045)

Анна Корченко[1], Кирило Давиденко[2]
[1,2]*Національний технічний університет «Дніпровська політехніка», Україна,*
[1]annakor@ukr.net, [2]kirilldavy@gmail.com,

Постійний розвиток інформаційних технологій і цифрових послуг породжує нові кіберзагрози, зокрема соціотехнічні атаки. Зловмисники застосовують психологічні маніпуляції для отримання несанкціонованого доступу до інформаційних ресурсів, що становить загрозу конфіденційності, цілісності та доступності даних. Особливу небезпеку такі атаки становлять для об'єктів критичної інформаційної інфраструктури (КІІ) та кіберфізичних систем, де наслідки можуть виходити за межі віртуального простору й впливати на реальні технологічні процеси, безпеку життєдіяльності й національну безпеку в цілому.

Відсутність систематизованої класифікації актуальних підходів та відповідних методів реалізації таких атак ускладнює розробку ефективних

заходів протидії, особливо в контексті захисту КІІ. З огляду на це, аналіз, класифікація і розробка сучасних підходів та методів виявлення соціотехнічних атак є важливим і актуальним науковим завданням.

Соціальна інженерія – це метод маніпулювання людьми з метою отримання доступу до конфіденційної інформації або ресурсів. Такі атаки спрямовані на людський фактор, використовуючи довіру, неуважність та недостатню обізнаність користувачів, що особливо критично в умовах, коли ціллю зловмисника є персонал або адміністратори об'єктів КІІ.

Аналізуючи дані провідних досліджень, можна виділити певні методи, які використовуються соціотехніками. Водночас у наявних публікаціях не в повному обсязі сформовані множини ознак, які характеризують підходи до реалізації відповідних атак, що дасть можливість з системних позицій формалізувати процес їх класифікації.

Крім того, соціотехнічні атаки постійно еволюціонують, що зумовлює необхідність їх комплексного аналізу та створення адаптивних методів захисту, що є ключовим для проектування механізмів захисту кіберфізичних об'єктів критичної інфраструктури. Ефективна протидія має базуватися не лише на технологічних рішеннях, а й на підвищенні обізнаності користувачів, впровадженні процедурного контролю та зміцненні організаційних і політичних аспектів кібербезпеки.

Метою роботи є розробка методу побудови моделі класифікації сучасних підходів реалізації соціотехнічних атак для систематизації та інтеграції існуючих класифікацій відповідних підходів [1, 2] з можливістю розширення новими ознаковими характеристиками. Це, в першу чергу, дасть можливість з системних позицій навчити персонал протистояти соціотехнічним загрозам. Для досягнення поставленої мети необхідно на основі теоретико-множинного підходу розробити метод побудови моделі класифікації соціотехнічних атак.

Для цього, з урахуванням запропонованих ознак, критеріїв та підкритеріїв [3] класифікації сучасних підходів до реалізації соціотехнічних атак було розроблено відповідну модель, метод формування якої реалізується в три етапи:

Етап 1 – визначення множини ідентифікаторів ознак ($\mathbf{S}$) класифікації підходів до реалізації соціотехнічних атак $\mathbf{S} = \{\boxtimes_{i=1}^{n} \mathbf{S_i}\} = \{\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n}\}$, $(i = \overline{1,n})$. Де $\mathbf{S_i}$ i-й ідентифікатор ознак класифікації підходів реалізації соціотехнічних атак, а n – їх кількість.

Етап 2 – визначення множини критеріїв щодо класифікації підходів до реалізації соціотехнічних атак $\mathbf{S_i} = \{\boxtimes_{j=1}^{m_i} \mathbf{C_{ij}}\} = \{\mathbf{C_{i1}}, \mathbf{C_{i2}}, ..., \mathbf{C_{im_i}}\}$, $(j = \overline{1,m_i})$. Де $\mathbf{C_{ij}} \subseteq \mathbf{S_i}$ множина набору критеріїв ($\mathbf{C}$) i-го ідентифікатора j-го критерія класифікації підходів до реалізації соціотехнічних атак, а m_i – їх кількість.

Етап 3 – визначення множини підкритеріїв класифікації підходів реалізації соціотехнічних атак $\mathbf{C_{ij}} = \{\bigotimes_{k=1}^{r_j} \mathbf{SC_{ijk}}\} = \{\mathbf{SC_{ij1}}, \mathbf{SC_{ij2}}, ..., \mathbf{SC_{ijr_j}}\}$, $(k = \overline{1, r_j})$. Де $\mathbf{SC_{ijk}}$ k-й ідентифікатор підкритеріїв j-го критерія i-го ідентифікатора ознак класифікації підходів реалізації соціотехнічних атак, а r_j – їх кількість.

Таким чином, запропоновано метод побудови моделі класифікації соціотехнічних атак в якому за рахунок етапів визначення множин: ідентифікаторів ознак, критеріїв та підкритеріїв класифікації підходів до реалізації соціотехнічних атак, дозволило розробити узагальнену модель теоретико-множинної інтерпретації класифікації сучасних підходів реалізації соціотехнічних атак.

1. Класифікація методів соціального інжинірингу / О.Г. Корченко, Є.В. Паціра, Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.

2. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, «Розширена класифікація методів соціального інжинірингу», Безпека інформації, т. 20, № 2, с. 197-205, 2014.

3. Корченко А. Сучасні методи соціотехнічних атак. Корченко А., Давиденко К. ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, с. 123-125.

Аналіз існуючих підходів, методів та моделей оцінки захищеності систем захисту інформації в корпоративній мережі

УДК 004.056.5:004.08

Віталій Котелянець[1], Денис Трухан[2]

Державний університет інформаційно-комунікаційних технологій,

[1]v.kotelianets@duikt.edu.ua, [2] trukhan@stud.duikt.edu.ua

У сучасному бізнес-середовищі корпоративні мережі є основою для функціонування компаній. Вони зберігають, обробляють та передають величезні обсяги цінної інформації – від фінансових даних та інтелектуальної власності до персональних даних клієнтів та співробітників. Забезпечення безпеки цих мереж є критично важливим завданням, оскільки будь-який інцидент може призвести до значних фінансових збитків, репутаційної шкоди та юридичних наслідків.

У сучасному світі динамічного розвитку інформаційних технологій захист комп'ютерних мереж стає ключовим завданням для забезпечення кібербезпеки.Особливу увагу слід приділяти захисту від атак в різних секторах країни, які можуть паралізувати критично важливу інфраструктуру та фінансовий сектор на тривалий час [1].

Крім того, поява нових фінансових інструментів, таких як альтернативні валюти, стимулює злочинців до подальшої розробки шкідливого програмного забезпечення (ШПЗ) з метою отримання прибутку. При цьому шкідливе програмне забезпечення використовує обчислювальні потужності не тільки